МЕЖДИСЦИПЛИНАРНЫЕ ИССЛЕДОВАНИЯ

Д. С. Лобов[1]
МГИМО МИД РФ / СПбГУ (Москва, Санкт-Петербург, Россия)

УДК: 338.012
doi: 10.55959/MSU0130-0105-6-60-6-11

ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ЦЕННОСТНОГО ПРЕДЛОЖЕНИЯ КВАНТОВЫХ КОММУНИКАЦИЙ И ПОСТКВАНТОВОЙ КРИПТОГРАФИИ С ТОЧКИ ЗРЕНИЯ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ НА ПРИМЕРЕ ФИНАНСОВОЙ ОТРАСЛИ

Работа посвящена исследованию экономических аспектов внедрения квантовых коммуникаций и постквантовой криптографии – двух передовых инструментов защиты связи в условиях появления квантового компьютера. Цель исследования – прогнозирование условий, при которых внедрение будет является экономически обоснованным для конечных пользователей в финансовой отрасли. Гипотеза заключалась в том, что применение квантовых коммуникаций и постквантовой криптографии как инструментов информационной безопасности представляет интерес для финансовых организаций, являющихся владельцами критической информационной инфраструктуры, в связи со снижением рисков экономических потерь от последствий киберпреступлений. Для доказательства данной гипотезы автор исследовал место и роль квантовых коммуникаций и постквантовой криптографии в системе информационной безопасности банка, оценил объем затрат на трансформацию инфраструктуры с применением квантового компонента, дал экономическую оценку рисков, связанных с отсутствием квантового уровня безопасности сети. Исследование основано на вводных по стоимости компонентов от участников рынка, а также на финансовых данных по результатам деятельности банка из открытых источников. В результате проведения сравнительного анализа потенциальных затрат и рисков, автор приходит к выводу о том, что отсутствие массового спроса на услуги пилотирования квантовых коммуникаций может быть связано с ожиданием недостаточных экономических эффектов на текущей стадии технологической готовности. Повышение спроса возможно с применением маркетинговых и финансовых инструментов отложенного платежа. Рекомендуется обратить внимание на сценарии применения оборудования квантового распределения ключей в ключевых узлах передачи данных. Полученные выводы могут представлять интерес для специалистов, работающих в области развития и коммерциализации новой отрасли квантовых коммуникаций в Российской Федерации.

[1] Лобов Даниил Сергеевич — к.э.н., старший преподаватель, МГИМО МИД РФ, научный сотрудник, СПбГУ; e-mail: d.lobov96@yandex.ru, ORCID: 0000-0002-9548-2502.

Ключевые слова: квантовые коммуникации, квантовое распределение ключей, постквантовая криптография, критическая информационная инфраструктура, экономика инноваций.

Цитировать статью: Лобов, Д. С. (2025). Экономические аспекты ценностного предложения квантовых коммуникаций и постквантовой криптографии с точки зрения конечного пользователя на примере финансовой отрасли. *Вестник Московского университета. Серия 6. Экономика,* 60*(6),* 257–276. https://doi.org/10.55959/MSU0130-0105-6-60-6-11.

D. S. Lobov
MGIMO, SPbGU (Moscow, Saint-Petersburg, Russia)
JEL: O31

ECONOMIC ASPECTS OF THE VALUE PROPOSITION OF QUANTUM COMMUNICATIONS AND POST-QUANTUM CRYPTOGRAPHY FROM THE END-USER PERSPECTIVE: CASE STUDY IN THE FINANCIAL INDUSTRY

This paper examines the economic aspects of implementing quantum communications and post-quantum cryptography — two advanced tools for securing communications in the context of the advent of quantum computers. The aim of the study is to predict the conditions under which their implementation will be economically feasible for end users in the financial sector. The hypothesis is that the use of quantum communications and post-quantum cryptography as information security tools is of interest to financial institutions that own critical information infrastructure due to the potential to reduce the risk of economic losses from cybercrime. To prove this hypothesis, the author examined the place and role of quantum communications and post-quantum cryptography in a bank's information security system, estimated the costs of transforming the infrastructure using a quantum component, and provided an economic assessment of the risks associated with the lack of a quantum-level network security. The study is based on input data on component costs from market participants, as well as financial data on bank's performance from open sources. Drawing on the comparative analysis of potential costs and risks, the author concludes that the lack of massive demand for quantum communications piloting services may be due to anticipated insufficient economic impact at the current stage of technological readiness. Demand could be increased through the use of deferred payment marketing and financial instruments. The author recommends to pay attention to scenarios for using quantum key distribution equipment in key data transmission nodes. These findings may be of interest to specialists working in the development and commercialization of emerging quantum communications industry in the Russian Federation.

Keywords: quantum communications, quantum key distribution, postquantum cryptography, critical information infrastructure, innovation economics.

To cite this document: Lobov, D. S. (2025). Economic aspects of the value proposition of quantum communications and post-quantum cryptography from the end-user perspective: case study in the financial industry. *Lomonosov Economics Journal*, 60*(6),* 257–276. https://doi.org/10.55959/MSU0130-0105-6-60-6-11

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. Функциональное преимущество квантового распределения ключей заключается в снижении риска компрометации ключевых носителей благодаря автоматической загрузки ключа в СКЗИ (James, 2023) по протоколу ProtoQa без участия курьера или администратора, а также невозможности перехвата ключа с применением методов прослушивания оптоволоконного канала (Lee, 2022). Кроме того, информация, зашифрованная симметричным квантовым ключом, более устойчива к кибератакам с применением квантового компьютера, чем текущие ассиметричные алгоритмы RSA, ГОСТ 34.10.2012 (Sharma, 2021). Таким образом, квантовые коммуникации позволят снизить как текущие, так и будущие риски в области информационной безопасности.

Конкурирующим решением, направленным прежде всего на обеспечение устойчивости шифрования критической информационной инфраструктуры в условиях функционирования квантового компьютера, является постквантовая криптография. Преимущества постквантовых алгоритмов заключаются в отсутствии необходимости закупки дорогостоящих устройств квантового распределения ключей (Satrya, 2023; Ahn, 2022), а также в возможности защиты беспроводных сетей при отсутствии доступа к воздушным каналам (Fakhruldeen, 2023). Но 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 продвинутых квантовых компьютеров в долгосрочной перспективе.

Финансовая отрасль является одним из ключевых направлений применения квантовых коммуникаций и постквантовой криптографии. Исследователи отмечают перспективные кейсы: информационная защита онлайн-транзакций (Madje, 2024; Dixit, 2020; Turjya, 2024), банкоматов (Ahmad, 2024), внутренних и межбанковских коммуникаций в целях защиты коммерческих и персональных данных (Williams, 2024; Lee, 2025).

Международный практический опыт дает развитие исследовательским гипотезам:

1. 2017 г., Китай: около 150 организаций, среди которых десятки крупных китайских банков, подключили офисы к магистральной квантовой сети (Quantum-Info, 2017).
2. 2022 г., Швейцария: компания по управлению финансовыми активами защитила канал передачи данных с применением устройств КРК между основным офисом и центром обработки данных. Помимо квантового оборудования установлены 10G Ethernet-шифраторы (AES-256) и сервер управления квантовыми ключами (ID Quantique, 2022).
3. 2024 г., Южная Корея: Toshiba, KT и Shinhan Bank успешно продемонстрировали гибридную систему защищённой связи (квантовые коммуникации и постквантовые алгоритмы) для защиты связи между двумя офисами банка в Сеуле (Toshiba, 2024).
4. 2024 г., США: J. P. Morgan заявила об успешном тестировании КРК для защиты канала между ЦОД и офисом компании с применением высокоскоростного шифровального оборудования (J. P. Morgan, 2024).

Несмотря на большую распространенность и медийное освещение отдельных опытов пилотирования квантовых коммуникаций, фактически уже сегодня осуществляется масштабирование практики защиты информации с помощью постквантовых алгоритмов. В США NIST завершил стандартизацию постквантового шифрования и NSA обязало провести переход на новые алгоритмы владельцев критической информационной инфраструктуры в течение пяти лет. Аналогичная дорожная карта была опубликована регуляторами ЕС в июне 2025 г.

Действия регулятора представляют интерес с точки зрения теории инновационного менеджмента: в соответствии с выводами Тайгелера Х., исследовавшего на примере облачных сервисов специфику действий регуляторов, ответственных за сертификацию (Teigeler, 2019), 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 (Hötte, 2023). Низкая активность регулятора в области квантовых коммуникаций, в отличие от сферы поствантовых алгоритмов, может свидетельствовать о недостаточной силе «рыночного притяжения», ожиданиях слабого экономического эффекта от внедрения устройств квантового распределения ключей со стороны потребителей.

Учитывая международный опыт регулирования сферы квантового шифрования, а также опыт пилотирования инноваций, автор работы выдвигает гипотезу о том, что внедрение квантовых коммуникаций и постквантовой криптографии как инструментов информационной безопасности представляет интерес для финансовых организаций, являющихся владельцами критической информационной инфраструктуры, при этом внедрение постквантовых алгоритмов может представлять большую ценность для конечных клиентов, чем квантовые коммуникации. Для доказательства данной гипотезы автор провел исследование места и роли квантовых коммуникаций и постквантовых алгоритмов в системе информационной безопасности финансовой организации, оценил объем затрат на трансформацию ИТ-инфраструктуры с применением квантового компонента, дал экономическую оценку рисков, связанных с отсутствием квантового уровня безопасности сети в долгосрочной перспективе.

Квантовые коммуникации в системе информационной безопасности финансовых компаний

Финансовая отрасль, концентрирующая объекты критической инфраструктуры, играет важную роль в стабильности экономики Российской Федерации. В 2024 г. финансовый сектор оказался в тройке самых атакуемых хакерами. По данным RED Security, на него пришлось около 17% кибератак — совокупно это более 20 000 инцидентов (Forbes, 2025).

Функционал устройств квантового распределения ключей в теории позволяет решать ряд задач в области информационной безопасности, связанных не только с существующими киберугрозами, но и потенциальными, например, рисками снижения устойчивости шифрования при успешном применении потенциальным противником квантового компьютера (табл. 1). Однако необходимо определить, насколько данный функционал актуален с учетом действительных угроз.

Таблица 1

Функциональные преимущества устройств квантового распределения ключей

Вид угрозы	Угроза	Функционал устройств
Текущая	Man-in-the-middle attack	Физические свойства фотона не позволяют осуществлять манипуляции с каналом третьими лицами
Текущая	Компрометация ключевого носителя	Ключ автоматически загружается в СКЗИ из устройства КРК, что снижает риски человеческого фактора при работе с ключевыми носителями
Потенциальная	Снижение устойчивости алгоритмов, преимущественно RSA	Шифрование информации с применением симметричных квантовых ключей снижает вероятность успеха дешифрования сообщения потенциальным противником с применением квантового компьютера

Источник: составлено автором на основе (Jawad, 2023; Dervisevic, 2024; Sharma, 2021).

Изучение источников, посвященных статистике инцидентов на объектах финансовой инфраструктуры, показывает (Alkhdour, 2024), что наиболее результативные атаки хакеров связаны с методами фишинга и социальной инженерии. Однако также выявлены исторические случаи специфичных атак, когда неблагонадежные сотрудники банка осуществляли кражу средств со счетов клиентов, обладая доступом к ключам шифрования (CBonds, 2024). Квантовые коммуникации действительно позволили бы автоматизировать процесс работы с ключевыми носителями и значительно снизить риск кражи средств (табл. 2).

Таблица 2

Экономические риски успешной квантовой атаки

Риск	**Горизонт**	**Потери**	**Квантовые коммуникации**	**Постквантовое шифрование**
Доступ администратора к ключевому носителю	Текущий риск	Осуществление несанкционированных транзакций	Снижают риск за счет автоматизации работы с ключами	Не снижает риск
Взлом асимметричного шифрования, подделка цифровых подписей с применением квантового компьютера	Будущий риск	Осуществление несанкционированных транзакций	Снижают риск за счет шифрования коммуникаций симметричными квантовыми ключами	Снижает риск за счет повышения сложности вычислений, недоступных квантовым компьютерам
		Кража персональных данных		
		Падение капитализации компании в результате снижения доверия клиентов		

Источник: составлено автором.

Устройства квантового распределения ключей и постквантовые алгоритмы исключают риск атаки с применением квантового компьютера. Ключевые угрозы, связанные с квантовым компьютером, заключаются прежде всего в возможном получении доступа к данным, зашифрованным асимметричным ключом RSA (Sharma, 2021), в то время как, например, алгоритм симметричного шифрования AES останется устойчивым даже в новых условиях (Bonnetain, 2019). Таким образом, функциональное применение инновационных решений сужается до процессов, реализуемых с применением асимметричного шифрования. Действительно, асимметричные методы широко распространены в финансах:

1. Безопасная передача данных (TLS/SSL): асимметричное шифрование используется для установления защищенных HTTPS-соединений в протоколах TLS. Банки применяют TLS для защи-

ты коммуникаций на порталах онлайн-банкинга, API и внутренних сервисах.

2. Межбанковские системы связи и расчетов: асимметричное шифрование встроено в такие системы, как SWIFT, SEPA и RTGS, которые используют зашифрованные цифровые подписи для обеспечения целостности транзакций.

Потенциальные угрозы успешной квантовой атаки включают: подделка цифровых подписей с возможностью осуществления несанкционированных транзакций, подделки документов, кражи персональных данных.

Оценка экономических эффектов от внедрения квантовых коммуникаций и постквантовой криптографии в финансовой организации

Оценим кейс внедрения квантовых коммуникаций и постквантовой криптографии на примере ПАО «Сбербанк». Данные для проведения анализа взяты из открытых источников. Предположим, что руководство компании примет решение внедрить квантовые коммуникации по следующим сценариям:

1. Защита наиболее критичных объектов Среднерусского банка. Для защиты 164 объектов потребуется установка 16 устройств приема сигнала и 164 передатчика (предположим, наиболее критичные объекты составляют 10% от общего количества).
2. Защита всех каналов Среднерусского банка. Для защиты всех 1645 объектов потребуется установка 160 устройств приема сигнала и 1645 передатчиков.
3. Защита наиболее критичных каналов Сбербанка. Потребуется установка 100 устройств приема сигнала и 1,1 тыс. передатчиков (1,1 тыс. объектов, предположим, что наиболее критичные объекты составляют 10% от общего количества).
4. Защита всех каналов Сбербанка (CBonds, 2024), потребуется установка 1 тыс. устройств приема сигнала и 11 тыс. передатчиков.

Оценка рисков квантовой атаки основана на следующей гипотезе: злоумышленник, используя квантовый компьютер, подделывает цифровую подпись и отправляет запрос, переводя 10% от общего оборота средств на офшорный счет для постепенного вывода. Перевод выглядит законным, так как подпись действительна, и система подтверждает его подлинность. Мошенничество обнаруживается через 4 часа, после чего применяются меры, ограничивающие возможности злоумышленника.

В случае квантовых коммуникаций также учитывается возможность реализации текущего риска компрометации ключей шифрования администратором, осуществляющим несанкционированные транзакции.

Потери от снижения капитализации компании на биржевом рынке предлагается не учитывать в связи со значительным влиянием спекулятивных сделок (риски в области информационной безопасности зачастую не оказывают долгосрочного влияния на рыночную стоимость компаний).

В случае если установка устройств квантового распределения ключей окажется значительно дороже, чем риски потерь от киберугроз, предлагается оценить стоимость внедрения постквантовых алгоритмов.

Оценка затрат на внедрение квантового оборудования производится по формуле:

$$QTc = \left(A \cdot P_1\right) + \left(B \cdot P_2\right) + \left(C \cdot P_3\right) + \left(S \cdot P_4\right) + \\ + \left(PN \cdot P_5\right) + \left(L \cdot P_6\right) + \left(C \cdot P_7\right), \quad (1)$$

где QTc — 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.

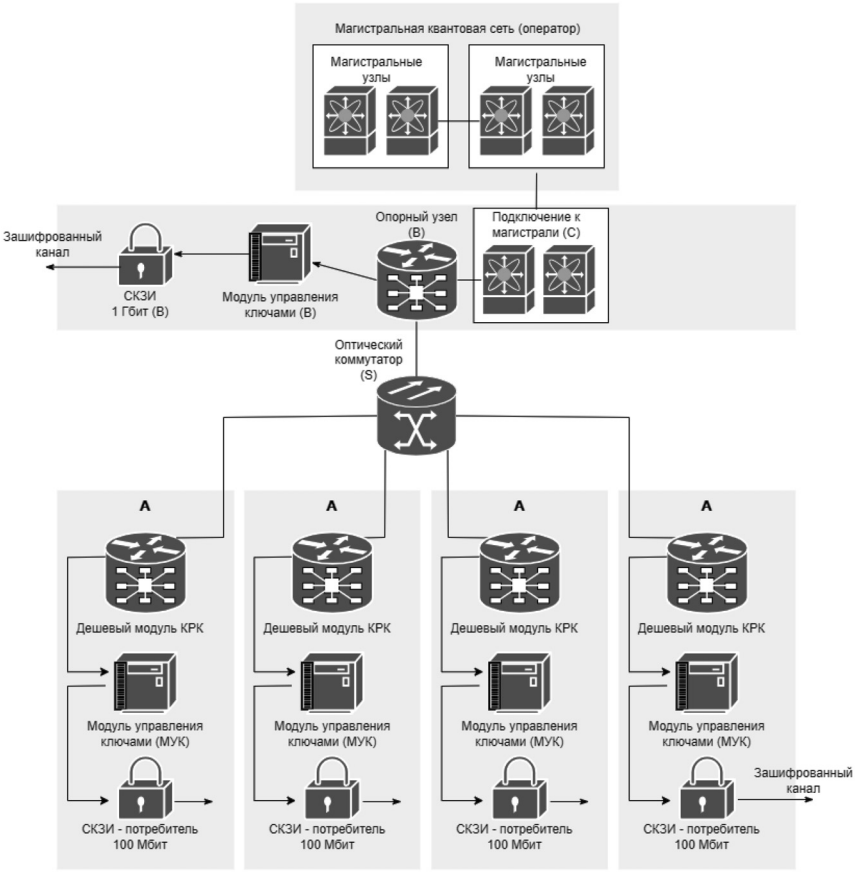

Рис. 1. Схема компонентов локальной квантовой сети

Источник: составлено автором.

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

$$ER = \left(QR \cdot AL\right) + (CR \cdot CL), \tag{2}$$

где ER — экономическая оценка рисков отказа от внедрения КРК и постквантовых алгоритмов;

QR — вероятность реализации риска применения квантового компьютера;

AL — ожидаемые потери в результате успешной квантовой кибератаки;

CR — вероятность реализации традиционных угроз в области информационной безопасности (например, компрометации ключевого носителя администратором сети);

CL — ожидаемые потери от реализации традиционных угроз в области информационной безопасности (например, компрометации ключевого носителя администратором сети.)

При оценке ER в контексте внедрения постквантовых алгоритмов исключается расчет $CR \cdot CL$, так как постквантовые алгоритмы не актуальны для снижения риска реализации традиционных угроз. Произведение $QR \cdot AL$ можно обозначить условным термином «квантовый риск», а произведение $CR \cdot CL$ — «традиционный риск». Схематичное изображение данных рисков представлено на рис. 2.

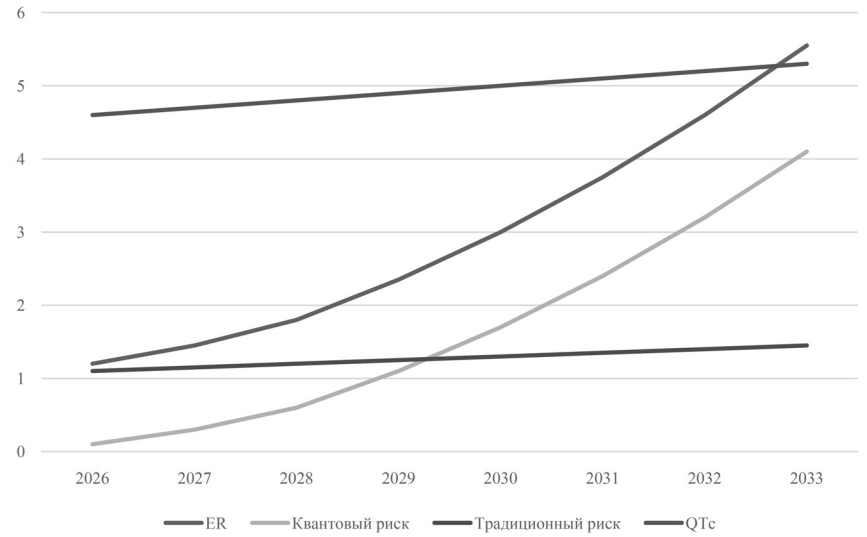

Рис. 2. Схематичное представление квантового и традиционного рисков, затрат на осуществление квантовой трансформации, условные единицы

Риск применения квантового компьютера определяется в соответствии с данными ведущих аналитических агентств, публикующих прогнозы создания квантового компьютера, способного снизить устойчивость асимметричных алгоритмов. Ожидаемые потери в результате успешной квантовой кибератаки (на примере финансовой организации) рассчитываются по следующей формуле:

$$AL = F \cdot T, \tag{3}$$

где AL — ожидаемые потери в результате успешной квантовой кибератаки, руб.;
F — оборот денежных средств в финансовой организации в течение 1 часа, руб.;
T — вероятная продолжительность квантовой атаки, 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, т.е. 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 алгоритмов можно оценить с применением метода бенчмаркинга по формуле:

$$PQ = ITB \cdot \alpha, \tag{4}$$

где PQ — затраты на постквантовую трансформацию;
α — 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 три года (требование к сроку амортизации средств криптографической защиты информации):

$$QTtco = QTc + \left(QTqc \cdot \partial \cdot t\right) + \left(C \cdot P_7 \cdot t\right), \tag{5}$$

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);
∂ — 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 ($C \cdot P_7 \cdot t$) 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:

$$ERc = \sum_{i=1}^{n} ER_i, \tag{6}$$

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.

Результаты

Результаты предварительных расчетов приведены в табл. 3. 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 два года функционирования оборудования плюс один год внедрения. Итоговые результаты анализа учитывают инфляционные ожидания и представлены в динамике до 2040 г.

Таблица 3

Оценка затрат на внедрение оборудования квантового распределения ключей в соответствии со сценариями на момент 2025 г.

Показатель	Сценарий 1	Сценарий 2	Сценарий 3	Сценарий 4
A, ед.	164	1645	1100	11 000
P_1, млн руб.	6	6	6	6
$A \cdot P_1$, млн руб.	984	9870	6600	66 000
B, ед.	16	165	100	1000
P_2, млн руб.	40	40	40	40
$B \cdot P_2$, млн руб.	640	6600	4000	40 000
C, ед.	16	165	100	1000
P_3, млн руб.	33	33	33	33

Окончание табл. 3

Показатель	Сценарий 1	Сценарий 2	Сценарий 3	Сценарий 4
$C \cdot P_3$, млн руб.	528	5445	3300	33 000
S, ед.	16	165	100	1000
P_4, млн руб.	1	1	1	1
$S \cdot P_4$, млн руб.	16	165	100	1000
PN; L	Отсутствуют в упрощенном расчете			
P_7, млн руб.	1,5	1,5	1,5	1,5
$C \cdot P_7$, млн руб.	24	248	150	1500
QTc, млн руб.	2192	22 328	14 150	141 500
$QTqc$, млн руб.	2168	22 000	14 000	140 000
∂, %	20	20	20	20
T, лет	2	2	2	2
$(QTqc \cdot \partial \cdot t)$, млн руб.	867,2	8800	5600	56 000
$(C \cdot P_7 \cdot t)$, млн руб.	48	496	300	3000
QT_{uco}, млн руб.	3 107	31 624	20 050	200 500

Источник: составлено автором.

Оценим риски атак, как квантовой, так и традиционной, с участием злоумышленника — сотрудника компании:

1. Объем переводов по системе SberPay (TBank, 2024) за 4 месяца составляет около 1 трлн руб. (347 222 222 руб. в час). Всего за 4 часа в зону риска попадает около 1 388 888 888 руб. Предположим, что целью мошенников является 10% всех переводов — 416 млн руб. Таким образом, за 4 часа квантовой атаки злоумышленники могут вывести 416 млн руб. в масштабах деятельности Сбербанка (сценарии 3–4).

Количество клиентов Среднерусского банка составляет 36% (41 млн счетов/ 113,2 млн активных физических и юридических лиц). Учитывая это, предположим, что в сценариях 1–2 под угрозу действий злоумышленников попадает 150 млн руб. (CBonds, 2024; SberBank, 2024).

2. Вероятность успешного создания квантового компьютера основана на опросах экспертов квантовой индустрии (в основу оценки вероятности создания лег отчет McKinsey (McKinsey, 2024), применяется понижающий индикативный коэффициент x2, учитывающий консервативные прогнозы создания функционирующего квантового компьютера (Introtoquantum. Timelines), а также заявления лидеров индустрии (Observer, 2025), она уве-

личивается с 5% в 2025 г. до 69% в 2040 г., с неравномерными темпами роста в периодах 2025–2030 гг. и 2031–2040 гг.

3. Для оценки рисков компрометации ключевого носителя также применим метод бенчмаркинга: известно, что в декабре 2018 г. группа недобросовестных сотрудников южноафриканского банка PostBank похитила мастер ключ, используемый для генерации ключей шифрования организации. Сотрудники использовали его для прямого доступа к банковским счетам клиентов, совершив 25 000 мошеннических транзакций и похитив 3,2 млн долл. В результате утечки PostBank пришлось заменить 12 млн карт клиентов, затратив 60 млн долл. (ImmersiveLabs, 2020). Итого потери для банка составили 63,2 млн долл., или 5029 млн руб.

4. Вероятность реализации данного риска незначительна. Внутренние атаки с применением несанкционированного доступа составляют около 5% (Shehab, 2024) от всех видов атак, компрометация ключа встречаются еще реже, так как потенциальные нарушители осведомлены о высокой вероятности выявления подобных действий. В связи с этим предлагается индикативно оценить возможность риска в 0,5%.

Оценка потенциальных рисков в результате отсутствия проекта внедрения квантового оборудования, учитывающая данные вводные, представлена в табл. 4.

Таблица 4

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

Показатель	Сценарий 1	Сценарий 2	Сценарий 3	Сценарий 4
AL, млн руб.	150	150	416	416
QR, %	5	5	5	5
CL, млн руб.	1810	1810	5029	5029
CR, %	0,5	0,5	0,5	0,5
ER, млн руб.	7,5 + 9,06 = 16,55	7,5 + 9,06 = 16,55	20,8 + 25,15 = 45,95	20,8 + 25,15 = 45,95

Источник: составлено автором.

Предварительный анализ собранных материалов показал, что внедрение квантовых коммуникаций на объектах ПАО «Сбер» не является экономически обоснованным решением в краткосрочной перспективе ни в одном из сценариев (табл. 5).

Таблица 5

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

	Сценарий 1	Сценарий 2	Сценарий 3	Сценарий 4
ER, млн руб.	16	16	46	46
QTc, млн руб.	2192	22 328	14 150	141 500

Источник: составлено автором.

Экономическая эффективность потенциальных проектов квантовой трансформации функции информационной безопасности увеличивается при точечной защите ключевых объектов критической информационной инфраструктуры. Например, речь может идти о защите центров обработки данных и головных офисов компании. Покрытие многочисленных офисов с незначительным оборотом денежных средств считается избыточным.

Далее предлагается рассмотреть экономическую привлекательность проекта в динамике. Прогноз показателей до 2040 г. по сценариям 1 и 3 с представлен на рис. 3 и 4.

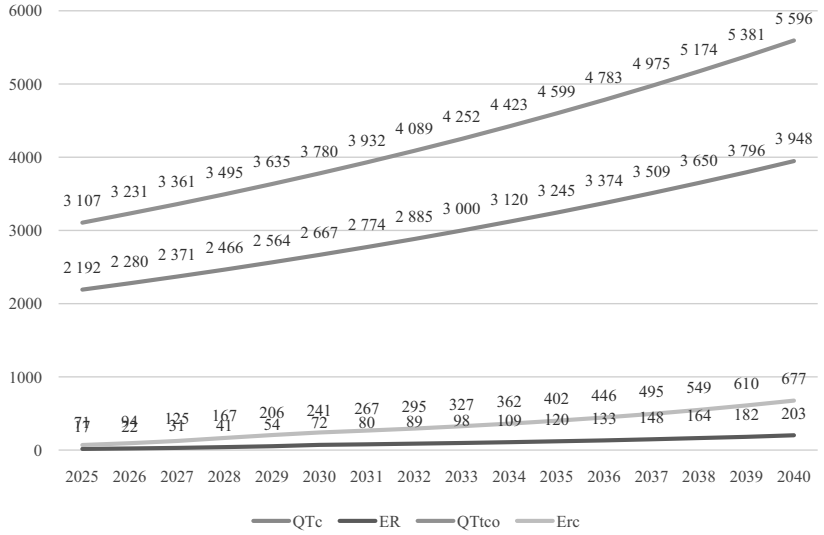

Рис. 3. Сравнение стоимости рисков экономических потерь и проведения квантовой трансформации функции информационной безопасности, сценарий 1, млн руб.
Источник: составлено автором.

Проведение расчета показало, что внедрение квантового оборудования по сценариям 1 и 3 (наиболее благоприятным с точки капитальных

затрат, так как предполагается покрытие 10% наиболее критичных объектов инфраструктуры) не представляет экономического интереса: риски потери средств значительно ниже, чем стоимость проведения квантовой трансформации. Даже в случае попадания 100% оборота SberPay в течение 4 часов под угрозу вывода злоумышленниками, затраты на оборудование квантового распределения ключей не окупаются.

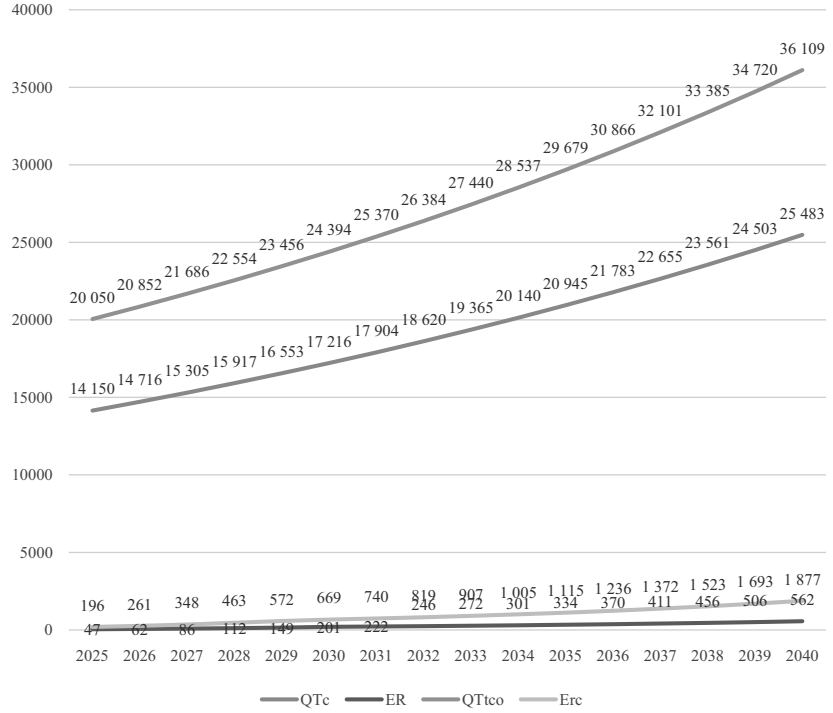

Рис. 4. Сравнение стоимости рисков экономических потерь и проведения квантовой трансформации функции информационной безопасности, сценарий 3, млн руб.
Источник: составлено автором.

Далее оценим стоимость внедрения постквантовых алгоритмов как альтернативного инструмента защиты от квантовой угрозы для сценариев 3–4. Для оценки стоимости внедрения постквантовых алгоритмов применяется метод бенчмаркинга: бюджет ИТ «Сбер» составляет, как минимум, 450 млрд руб. за три года или 150 млрд руб. в год (Fontanka, 2023). Бенчмарк равен 10%, так как Правительство США планирует выделить 7,1 млрд долл. на внедрение постквантовых алгоритмов (Quantum Insider, 2024), что равняется примерно 10% годового бюджета 2024 г. (The White House, 2024).

Таким образом, затраты на постквантовую трансформацию (*PQ*) ПАО «Сбер» могут составить от 15 млрд руб.

Хотя стоимость внедрения постквантовых алгоритмов все же выше, чем затраты компании в результате реализации рисков, в случае частого повторения квантовых атак инновационное решение может представлять и экономический интерес. В свою очередь сравнительный анализ квантовых коммуникаций и постквантовых алгоритмов показал, что вторая технология является более привлекательной с учетом экономической эффективности.

Стоит отметить, что повысить спрос на инфраструктурные решения в области квантовых коммуникаций могут маркетинговые инструменты, учитывающие прогноз риска применения квантового компьютера, что продемонстрировано на рис. 5 (схематичное изображение). В том случае, если расчет, проведенный по представленной в данной работе методологии, показывает вероятность пересечения *ER* и *QTc* в период 2028–2032 гг., возможно ускорение коммерциализации решений со сдвигом потенциального проекта на начало 2026 г. Для этого необходимо рассмотреть возможность бесплатного лизинга оборудования потенциальному клиенту на первые несколько лет (период низкого риска применения квантового компьютера). Предполагается, что риск вырастет к 2030–2035 гг., в период, когда возможно более обоснованное повышение цен для конечных клиентов.

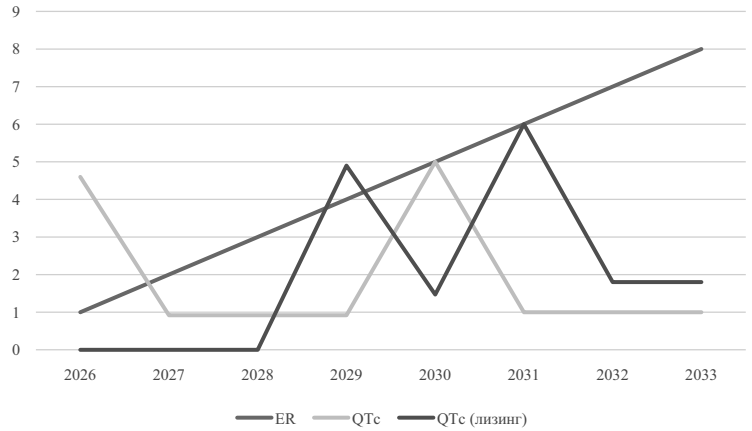

Рис. 5. Схематичное представление роли маркетинговых инструментов в сфере продвижения продуктов квантовых коммуникаций (бесплатный лизинг оборудования первые три года), условные единицы

Любое пересечение *QTc* на рис. 4 говорит о снижении вероятности успешной сделки по внедрению квантовых коммуникаций на объекте клиента. График показывает, что применение инструментов отложенного платежа повышает вероятность сделки.

Заключение

Гипотеза о наличии ценностного предложения квантовых коммуникаций и постквантовой криптографии, основанного на экономических эффектах, подтвердилась только частично: внедрение квантовых коммуникаций и постквантовых алгоритмов приведет к значительным капитальным затратам компаний. При стоимости проекта в размере от 15 до 200 млрд руб. и ограниченных рисках финансовых потерь, масштабное осуществление квантовой трансформации не может быть рекомендовано к реализации.

При снижении стоимости проекта, внедрение квантовых коммуникаций может представлять интерес прежде всего на ключевых узлах передачи информации, например, для защиты центров обработки данных. Постквантовые алгоритмы применяются в сценариях защиты беспроводных каналов. Повышение экономической привлекательности решений возможно благодаря маркетинговым и финансовым инструментам отложенного платежа.

Но для подготовки окончательных выводов требуется проведение более глубокого анализа, аудита ИБ-инфраструктуры потенциального заказчика. Необходимо ответить на следующие вопросы: можно ли ограничиться исключительно защитой наиболее критичных объектов для сокращения проектных затрат при сохранении функциональной эффективности решения? Обладает ли компания традиционными инструментами ограничения действий злоумышленников в случае квантовой атаки, или же инструменты отсутствуют, атака может привести к более масштабным потерям, чем указано в индикативном расчете исследования?

Проведенный анализ может представлять интерес для специалистов, связанных с развитием и коммерциализацией новой отрасли квантовых коммуникаций. Рекомендуется обратить внимание на действительную актуальность функционала предлагаемого оборудования, количественную оценку рисков потенциальных клиентов при работе с ценообразованием услуг квантового распределения ключей, а также на «фактор страха» и ожидания по созданию функционирующего квантового компьютера при анализе перспектив коммерциализации.

Результаты исследования могут лечь в основу прогнозирования спроса на услуги квантовых коммуникаций в экономической модели развития данного направления в Российской Федерации.

Список литературы

Ahmad, F., Kanta, K., Shiaeles, S., Naeem, A., Khalid, Z., & Mahboob, K. (2024). Enhancing ATM security management in the post-quantum era with quantum key distribution. *In 2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, 329–334. https://doi.org/10.1109/CSR61664.2024.10679471.

Ahn, J., Kwon, H. Y., Ahn, B., Park, K., Kim, T., Lee, M. K., & Chung, J. (2022). Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography

(pqc) and quantum key distribution (qkd). *Energies*, *15*(3), 714. https://doi.org/10.3390/en15030714.

Alkhdour, T., AlWadi, B. M., & Alrawad, M. (2024). Assessment of cybersecurity risks and threats on banking and financial services. *Journal of Internet Services and Information Security*, *14*(3), 167–190. https://doi.org/10.58346/JISIS.2024.I3.010.

Bonnetain, X., Naya-Plasencia, M., & Schrottenloher, A. (2019). Quantum Security Analysis of AES. *IACR Transactions on Symmetric Cryptology*, *2*, 55–93. https://doi.org/10.13154/tosc.v2019.i2.55-93.

CBonds. (2024). Филиалы действующих кредитных организаций на территории РФ. ПАО Сбербанк. Дата обращения 30.07.2025, https://cbonds.ru/indexes/161017/

Dervisevic, E., Tankovic, A., Fazel, E., Kompella, R., Fazio, P., Voznak, M., & Mehic, M. (2025). Quantum Key Distribution Networks--Key Management: A Survey. *ACM Computing Surveys*, *10*(57), 1–36. https://dl.acm.org/doi/10.1145/3730575.

Dixit, S. (2020). The Impact of Quantum Supremacy on Cryptography: Implications for Secure Financial Transactions. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *6*(4), 611–637. https://doi.org/10.58346/JISIS.2024.I3.010.

Fakhruldeen, H. F., Al-Kaabi, R. A., Jabbar, F. I., Al-Kharsan, I. H., & Shoja, S. J. (2023). Post-quantum Techniques in Wireless Network Security: An Overview. *Malaysian Journal of Fundamental and Applied Sciences*, *19*(3), 337–344. https://doi.org/10.11113/mjfas.v19n3.2905.

Fontanka. (2023). Сбер вложит 450 млрд рублей в IT и нейросети. Крупнейший банк страны рассказал, какими будут следующие три года для всех нас. Дата обращения 30.07.2025, https://www.fontanka.ru/2023/12/06/72990440/?ysclid=mdop3x3xuj971318719.

Forbes. (2025). Эксперты назвали главные киберугрозы для банков. Дата обращения 30.07.2025, https://www.forbes.ru/finansy/528907-eksperty-nazvali-glavnye-kiberugrozy-dla-bankov-i-ih-klientov-v-2025-godu?ysclid=mdoi1ovn8p653847810.

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

ID Quantique. (2022). Securing Network for Disaster Recovery. Дата обращения 30.07.2025, https://marketing.idquantique.com/acton/attachment/11868/f-0211/1/-/-/-/- /Financial%20Services_DRC%20QKD%20Use%20Case.pdf.

Immersive Labs. (2020). Inside job responding to threats from within. Дата обращения 30.07.2025, https://www.immersivelabs.com/resources/blog/inside-job-responding-to-threats-from-within.

Introtoquantum. Timelines: When can we expect a useful quantum computer? Дата обращения 30.07.2025, https://introtoquantum.org/essentials/timelines/.

J. P. Morgan. (2024). JPMorgan Chase establishes quantum-secured crypto-agile network. Дата обращения: 30.07.2025, https://www.jpmorgan.com/technology/news/firm-establishes-quantum-secured-crypto-agile-network.

James, P., Laschet, S., Ramacher, S., & Torresetti, L. (2023). Key management systems for large-scale quantum key distribution networks. *In Proceedings of the 18th International Conference on Availability, Reliability and Security*, *126*, 1–9. https://doi.org/10.1145/3600160.3605050.

Jawad, T. A., Mahmood, A. N., & Hameed, A. N. (2023). Detecting man-in-the-middle attacks via hybrid quantum-classical protocol in software-defined networks. *Indonesian Journal of Electrical Engineering and Computer Science*, *31*(1), 205–211.

Lee, C., Sohn, I., & Lee, W. (2022). Eavesdropping detection in BB84 quantum key distribution protocols. *IEEE Transactions on Network and Service Management*, *19*(3), 2689–2701. https://doi.org/10.1109/TNSM.2022.3165202.

Lee, Y. S., & Tso, R. (2025). Post-Quantum Cryptography (PQC) Migration Guide for Financial Institutions. *Communications of the CCISA*, *31*(1), 45–55.

Madje, U. P., & Pande, M. B. (2024). A Conceptual Model of Quantum Cryptography Techniques used to Provide Online Banking Transactions Security. *In 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies*, 1–5. https://doi.org/10.1109/TQCEBT59414.2024.10545237.

McKinsey. (2024). Enabling the next frontier of quantum computing. Дата обращения 30.07.2025, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/enabling-the-next-frontier-of-quantum-computing.

Observer. (2025). Is Nvidia's Jensen Huang Right About Quantum Computing? Дата обращения: 30.07.2025, https://observer.com/2025/01/is-nvidias-jensen-huang-right-about-quantum-computing/.

Quantum-Info. (2017). The World's First Quantum Communication Backbone was Launched and the First-ever Intercontinental Quantum Communication was Realized. Дата обращения: 30.07.2025, https://www.quantum-info.com/English/News/progress/2017/1007/392.html (дата обращения: 30.07.2025)

Quantum Insider. (2024). White House Report: U. S. Federal Agencies Brace for $7.1 Billion Post-Quantum Cryptography Migration. Дата обращения 30.07.2025, https://thequantuminsider.com/2024/08/12/white-house-report-u-s-federal-agencies-brace-for-7-1-billion-post-quantum-cryptography-migration/.

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

SberBank. (2024). Пресс-релиз. Дата обращения 30.07.2025, https://www.sberbank.com/common/img/uploaded/files/info/results_q4_qx5ln89k_2024.pdf.

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

TBank. (2024). Пульс. Дата обращения 30.07.2025, https://www.tbank.ru/invest/social/profile/Violette/aa65debf-c6d7-4d59-a685-a46e035fe5b5/.

Teigeler, H., & Lins, S., & Sunyaev, A. (2019). Technology-Push or Market-Pull — What Drives Certification Authorities to Perform Continuous Service Certification? *Conference: European Conference on Information Systems 2019 (ECIS)At*. Stockholm, Sweden.

The White House. (2024). Budget of the U. S. Government FISCAL YEAR 2024. https://www.whitehouse.gov/wp-content/uploads/2023/03/budget_fy2024.pdf.

Toshiba. (2024). Hybrid Quantum Secure Communications with South Korea's Shinhan Bank. Дата обращения 30.07.2025, https://www.global.toshiba/ww/news/digitalsolution/2024/04/news-20240419-01.html.

Turjya, S. M., Singh, R., Sarkar, P., Swain, S., & Bandyopadhyay, A. (2024). Quantum-based QKD and sugar-salt encryption approach in cloud-fog computing to strengthen protection of online banking data. *In 2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS)*, 1–7. https://doi.org/10.1109/ICITEICS61368.2024.10624984.

Williams, S., Martin, D., & Green, J. (2024). Quantum Cryptography to Secure Financial Data. *Journal of Tecnologia Quantica*, *1*(6), 312–321. https://doi.org/10.70177/quantica.v1i6.1702.