Технологии информационного общества

ПРОГНОЗ СПРОСА НА УСЛУГИ КВАНТОВЫХ КОММУНИКАЦИЙ В НЕФТЕГАЗОВОЙ ОТРАСЛИ С УЧЕТОМ ЦЕННОСТНОГО ПРЕДЛОЖЕНИЯ

Статья рекомендована к публикации членом редакционного совета А. А. Стрельцовым 23.12.2024

Лобов Даниил Сергеевич

Кандидат экономических наук
МГИМО МИД РФ
АО «Кэпт», помощник менеджера
Москва, Российская Федерация
d.lobov@odin.mgimo.ru

Аннотация

Работа посвящена исследованию экономических аспектов внедрения технологий квантовых коммуникаций. Цель исследования – прогнозирование условий, при которых внедрение данной инновации будет представлять экономический интерес для конечных пользователей на примере нефтегазовой отрасли. Гипотеза заключалась в том, что внедрение квантовых коммуникаций как инструмента информационной безопасности представляет интерес для нефтегазовых компаний, являющихся владельцами критической информационной инфраструктуры, в целях снижения рисков экономических потерь от последствий киберпреступлений. 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, дал экономическую оценку рисков, связанных с отсутствием квантового уровня безопасности сети. 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 недостаточными экономическими эффектами на текущей стадии технологического прогресса, но успехи потенциального противника в разработке квантовых компьютеров повысят спрос на квантовые коммуникации в долгосрочном горизонте 2030-2038 гг. Полученные выводы могут представлять интерес для специалистов, работающих в области развития и коммерциализации новой отрасли квантовых коммуникаций в Российской Федерации.

Ключевые слова

квантовые коммуникации, квантовое распределение ключей, постквантовая криптография, критическая информационная инфраструктура, экономика инноваций

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. Функциональные преимущества квантового распределения ключей заключаются в повышении устойчивости систем в условиях растущих рисков информационной безопасности.

Большинство работ, посвященных вопросам экономики квантовых коммуникаций, рассматривает факторы развития рынка устройств квантового распределения ключей. Барьеры

© Лобов Д. С, 2025

Производство и хостинг журнала «Информационное общество» осуществляется Институтом развития информационного общества.

Данная статья распространяется на условиях международной лицензии Creative Commons «С указанием авторства - С сохранением условий версии 4.0 Международная» (Creative Commons Attribution – ShareAlike 4.0 International; CC BY-SA 4.0). См. https://creativecommons.org/licenses/by-sa/4.0/legalcode.ru
https://doi.org/10.52605/16059921_2025_04_108

коммерциализации, выявленные в 2014-2015 гг., включали недостаточность сертификации и стандартизации оборудования и технологий, низкое качество послепродажного обслуживания, отсутствие необходимой телекоммуникационной инфраструктуры [9]. До сих пор нерешенной задачей остается создание «квантового повторителя», позволяющего транслировать состояние фотона на протяженные расстояния [11, 13]. При этом авторы отмечают позитивную динамику развития отрасли с 2023 года: осуществляется переход исследований с этапа НИР на ОКР, что свидетельствует о росте уровня технологической готовности решений [4], в создании квантовой инфраструктуры принимают участие такие крупные технологические компании, как Toshiba, Huawei, наблюдается определенный прогресс в области стандартизации [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 [4], прогнозируется рост объема международного рынка до 36 млрд долл. в 2040 г. [26].

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 [3], важность технологии для транспортной [6], энергетической [7] отраслей. Подчеркиваются возможности применения квантовых коммуникаций в целях защиты каналов центров обработки данных [11].

При этом 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., исследовавшего на примере облачных сервисов специфику действий регуляторов, ответственных за сертификацию [32], 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 [17]. Таким образом, недостаточная активность регулятора в области квантовых коммуникаций может свидетельствовать о недостаточной силе «рыночного притяжения», ожиданиях слабого экономического эффекта от внедрения устройств квантового распределения ключей со стороны потребителей.

Автор данной работы предполагает, что внедрение квантовых коммуникаций как инструмента информационной безопасности должно представлять интерес для компаний-владельцев объектов критической информационной инфраструктуры в связи со снижением экономических рисков, связанных с потенциальными последствиями кибер-преступлений. 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, дал экономическую оценку рисков, связанных с отсутствием квантового уровня безопасности сети в долгосрочной перспективе.

1 Квантовые коммуникации в системе информационной безопасности энергетических компаний

Определение места и роли квантовых коммуникаций в системе информационной безопасности промышленных организаций требует базового понимания сущности текущих вызовов и угроз, технологического функционала устройств квантового распределения ключей. В качестве примера предлагается взять энергетическую отрасль, концентрирующую объекты критической инфраструктуры, играющие важную роль в стабильности экономики Российской Федерации.

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

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 [12, 19, 30].

Изучение источников, посвященных статистике инцидентов на объектах энергетической инфраструктуры, показывает (таблица 2), что наиболее результативные атаки хакеров связаны с недостаточной подготовкой персонала и подрывными действиями сотрудников самих организаций. Борьба с наиболее актуальными угрозами лежит прежде всего в периметре административной работы: своевременное обновление патчей и программного обеспечения сотрудниками ИТ, обучение персонала, а также сегментация сетей. Функционал устройств квантового распределения ключей может оказаться излишним в текущих условиях.

Таблица 2. Ключевые кибер-атаки на критическую информационную инфраструктуру в области энергетики

Направление	Характер атаки	Источник
Нефтегазовая отрасль (upstream, midstream, downstream)	Фишинговые атаки, загрузка вирусов, в том числе сотрудниками компаний.	Stergiopoulos, 2020. Cyber-attacks on the Oil & Gas sector: A survey on incident assessment and attack patterns
Энергетика, нефтегазовая отрасль	Программы вымогатели, уязвимость нулевого дня.	Лаборатория Касперского (2023). Первое полугодие 2023 года — краткий обзор основных инцидентов промышленной кибербезопасности
	Фишинг, программы вымогатели, использование уязвимостей в открытом для интернета хосте или системе для первоначального доступа к сети.	Security Intelligence (2022). Industry threat recap: Energy

Источник: составлено автором на основе [20, 29, 31].

Необходимо ли применение квантовых коммуникаций для защиты от потенциальных угроз, например, квантового компьютера? Ключевые риски, связанные с квантовым компьютером, заключаются прежде всего в возможном получении доступа к данным, зашифрованным ассиметричным ключом RSA [30], в то время как, например, алгоритм симметричного шифрования AES останется устойчивым даже в новых условиях [10]. 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 её информационной безопасности подробно исследуются экспертами. Опыт прошлых

кибератак показывает [18], что компрометация систем SCADA может привести к экономическому и в некоторых случаях физическому ущербу для населения. Кроме того, исследование текущих вызовов и угроз, связанных с применением SCADA, показывает наличие рисков реализации man-in-the-middle атак [15], что обуславливает актуальность применения квантовых коммуникаций для защиты этих систем, особенно в условиях применения квантового компьютера потенциальным противником.

Ряд авторов приходит к аналогичным выводам, предлагая подходы к обеспечению защиты SCADA как с применением квантового распределения ключей, так и математических постквантовых алгоритмов, не требующих дополнительных затрат на установку квантовой инфраструктуры [19, 28, 22, 24]. В рамках данного исследования автор предлагает ввести ограничение, предполагающее необходимость применения синергии технологий квантового распределения ключей и постквантовых математических алгоритмов для гарантированной защиты инфраструктуры, ссылаясь на технические обоснования предыдущих работ экспертов в области безопасности SCADA [19].

Таким образом, оценка потенциальных экономических эффектов от внедрения квантовых коммуникаций на объектах нефтегазовой отрасли будет основываться на следующих гипотезах:

1. Квантовый компьютер будет создан;
2. Создание квантового компьютера несет риски снижения устойчивости SCADA, повышает успешность кибер-атак типа ransomware, приводящим к значительным простоям оборудования;
3. Синергия технологий квантового распределения ключей и математических постквантовых алгоритмов позволяет ликвидировать новые риски и угрозы для систем SCADA, связанные с квантовым компьютером.

2 Оценка экономических эффектов от внедрения квантовых коммуникаций на объектах нефтегазовой отрасли

Устойчивость нефтегазовой отрасли в условиях растущих кибер-угроз является одним из залогов стабильного функционирования экономики [21, 31]. В связи с этим предлагается провести оценку экономических эффектов от внедрения квантовых коммуникаций на примере одной из ведущих нефтегазовых компаний России: ПАО «НК «Роснефть».

Ограничение расчета будет заключаться в следующем сценарии: ПАО «НК «Роснефть» выделяет бюджет на защиту 10 объектов нефтепереработки решениями в области квантовых коммуникаций и постквантовой криптографии: Комсомольского НПЗ, Ангарской нефтехимической компании, Ачинского НПЗ, Туапсинского НПЗ, Куйбышевского НПЗ, Новокуйбышевского НПЗ, Сызранского НПЗ, Саратовского НПЗ, Рязанской нефтеперерабатывающей компании, Ярославского НПЗ.

Предположим, что защита внутреннего периметра каждого из предприятий осуществляется с применением топологии точка-многоточка, в соответствии с которой необходимо установить 1 дорогостоящее квантовое устройство и 3 дешевых клиента, стоимостью 30 и 3 млн руб. соответственно.

Защита внешнего периметра осуществляется за счет подключения к магистральной квантовой сети, годовая стоимость подключения в данном исследовании определяется в размере 1.5 млн руб. в год за подключение одного модуля. Стоимость модуля внешней связи равна 3 млн руб. Каждая организация приравнивается одному подключению.

Таким образом, затраты ПАО «НК «Роснефть» в 2025 году на подключение устройств квантового распределения ключей будут рассчитаны по (1)[1].

$$QKDc = \sum_{i=1}^{n}(A_i * P_1) + (B_i * P_2) + (T_i * P_3) + (T_i * TP), \quad (1)$$

где А – количество модулей «Алиса», Р1 – стоимость оборудования и монтажа модуля «Алиса», В – количество модулей «Боб», Р2 – стоимость оборудования и монтажа модуля «Боб», Т – количество модулей, закупаемых для подключения к внешней сети, Р3 – стоимость оборудования и монтажа модулей подключения к внешней сети, ТР – стоимость подключения модуля к сети в год.

[1] Данный подход к расчету является индикативным, более подробная методология представлена в монографии автора

Стоимость внедрения постквантовых алгоритмов шифрования осуществляется с применением бенчмаркинга. В то время как российские разработчики заявляют об отсутствии необходимости выделения значительного бюджета на постквантовую трансформацию, автор предлагает не пренебрегать данным показателем в расчётах, так как зарубежная практика доказывает наличие существенных затрат на обновление традиционной ИТ-инфраструктуры, обучение персонала. С 2025 по 2035 гг. Правительство США планирует выделить 7.1 млрд долларов на внедрение постквантовых алгоритмов [27], что равняется примерно 10% годового бюджета 2024 г. [33]. Расчет итоговой стоимости на внедрение мер защиты от квантовой угрозы представлен в (2).

$$QQT = QKDc + (ITc * \alpha)\,, \quad (2)$$

где QKDc – затраты на внедрение устройств квантового распределения ключей с учетом годового тарифа на обслуживание внешних сетей, ITc – затраты на ИТ организации, a – бенчмарк стоимости постквантовой трансформации.

Так как информация в открытых источниках о бюджетах ИТ 12 отобранных промышленных объектах Роснефти отсутствует, их оценка была также получена с применением бенчмарка: отношение бюджета ИТ энергетических компаний к выручке [14]. Совокупная выручка 12 объектов была получена за 2020 г. на основании открытых данных бухгалтерской отчетности [1] и проиндексирована в соответствии с инфляцией, после чего был применен бенчмарк, в соответствии с которым бюджет ИТ составляет 1.5% от выручки. Индикативная совокупная оценка бюджета ИТ (план) за 2025 год составила 3.234 млрд руб. Соответственно, бюджет на внедрение постквантовых алгоритмов в 2025 г. равен 0.323 млрд руб. Совокупные затраты на трансформацию информационной безопасности составляют 0.75 млрд руб. Ежегодная ожидаемая стоимость внедрения индексируется в соответствии с прогнозируемой инфляцией 4.5-4% [2]. Вероятные затраты на внедрение представлены на рисунке 1.

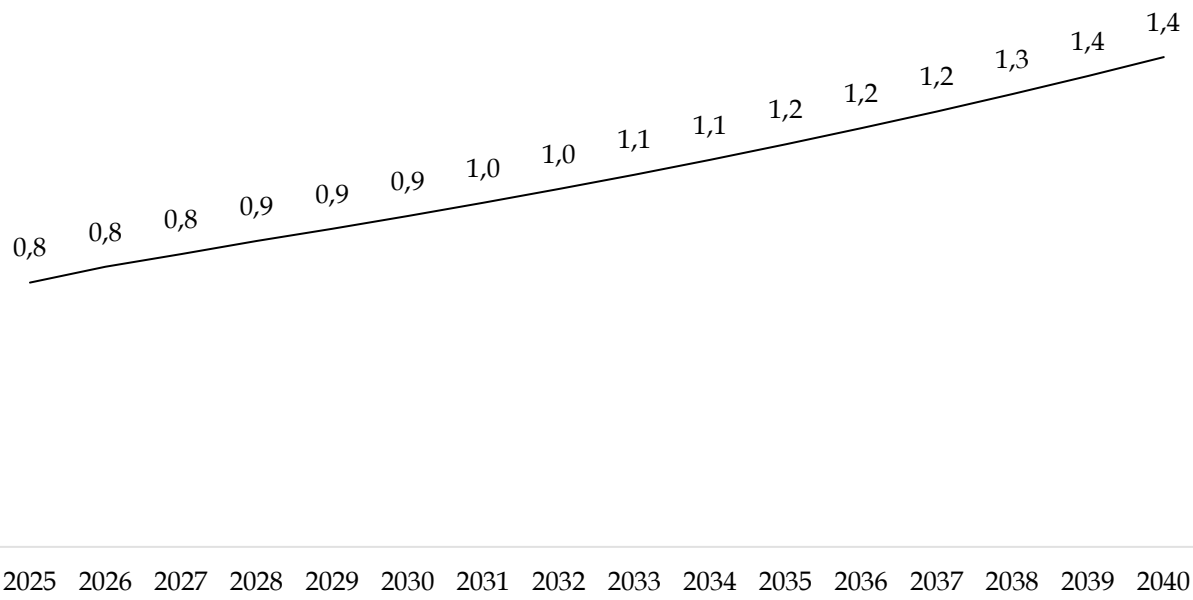

Рис. 1. Оценка стоимости внедрения КРК и постквантовых алгоритмов в систему информационной безопасности нефтепереработки ПАО «НК «Роснефть», млрд руб. Составлено автором.

Риски отказа от внедрения КРК и постквантовых алгоритмов оцениваются в соответствии с (3).

$$QR = QC * RL\,, \quad (3)$$

где QC – вероятность успешного создания и применения квантового компьютера, RL – ожидаемые потери выручки от простоя оборудования в результате успешной квантовой кибер-атаки.

Вероятность успешного создания квантового компьютера основана на опросе экспертов квантовой индустрии [23], учитывает корректирующий показатель автора и увеличивается с 5% в 2025 г. до 69% в 2040 г. с неравномерными темпами роста в периодах 2025-2030 гг., 2031-2040 гг.

Ожидаемые потери выручки от простоя оборудования в результате успешной квантовой кибер-атаки основаны на данных Рязанской нефтеперерабатывающей компании и учитывают индексацию [1], а также бенчмарк по временным показателям простоя оборудования промышленных компаний в результате реализации ransomware атак – 22 дня простоя [25].

3 Прогноз спроса на примере ПАО «НК «Роснефть»

Полученные результаты, по мнению автора, могут свидетельствовать о том, что услуги квантовых коммуникаций и квантовой трансформации информационной безопасности промышленных организаций начнут представлять интерес для конечных клиентов в 2030 г. с акселерацией силы рыночного притяжения в 2038 г. (рисунок 2).

Эксперты довольно высоко оценивают возможность создания квантового компьютера, способного взломать RSA к 2030 г. Риски экономических потерь превышают стоимость квантовой трансформации систем ИБ, в связи с чем возможен рост интереса покупателей. Но соотношение risk-profit 1:2, приемлемое для инвесторов, достигается в 2039 г., в связи с чем в данном периоде наиболее вероятна акселерация спроса.

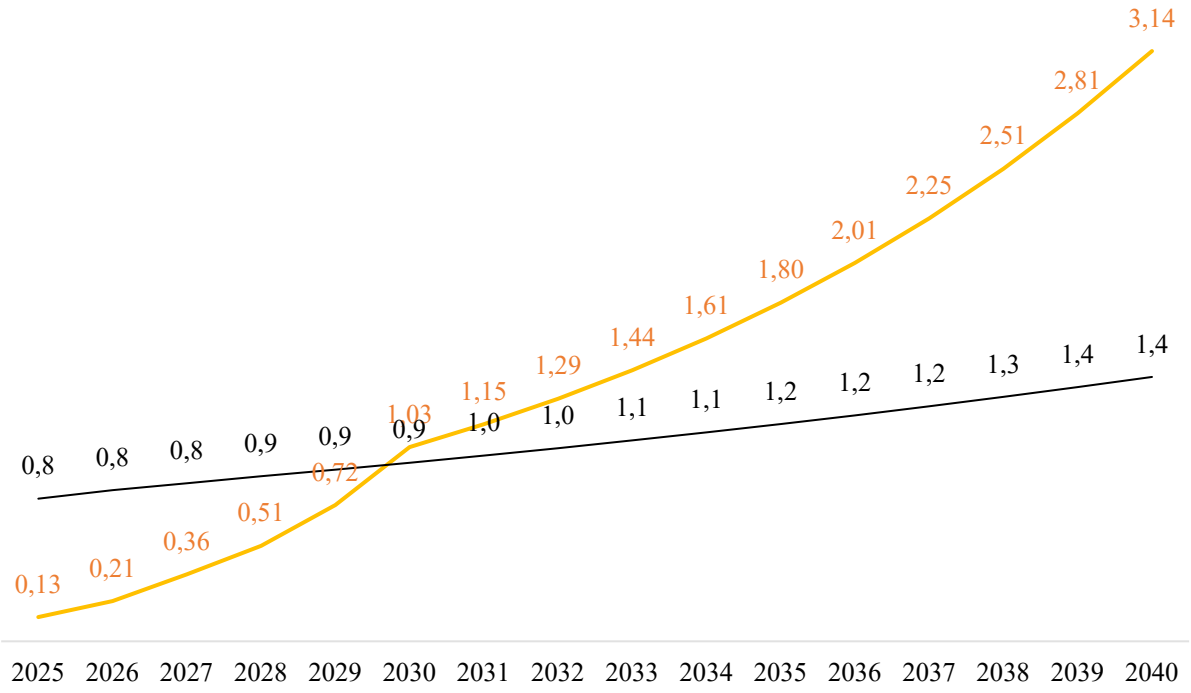

Рис. 2. Сравнение стоимости рисков экономических потерь от простоя оборудования и внедрения КРК и постквантовых алгоритмов в систему информационной безопасности нефтепереработки ПАО «НК «Роснефть», млрд руб. Составлено автором.

Автор считает, что данная оценка соответствует ожиданиям NIST и Белого дома, касающихся рисков применения квантового компьютера и нарушения работы критической информационной инфраструктуры, ставших основой решения о переходе на постквантовые алгоритмы в период до 2035 г. [33].

4 Прогноз спроса на примере ПАО «НК «Роснефть»

Прогноз проникновения услуг квантовых коммуникаций в энергетическую отрасль осуществлен с применением следующих данных:

1. Уровень «восприятия цифровых инноваций» компаниями энергетической отрасли, основывающийся на данных о выручке, уровне рыночной готовности (MRL) стартапов-участников Инновационного центра Сколково, разрабатывающих ИТ-решения в сферах добычи нефти и природного газа, проведения геологоразведочных работ, производства нефтепродуктов (таблица 1).

2. Данные ФСТЭК о количестве объектов критической информационной инфраструктуры.

Таблица 3. Ключевые кибер-атаки на критическую информационную инфраструктуру в области энергетики

Отрасль применения	Компания	MRL	Выручка
Добыча нефти и природного газа	КиберПротект	9	2999
Добыча нефти и природного газа	Геолаб	7	453,7
Добыча нефти и природного газа	СтратаСолюшнс	8	418
Геологоразведочные работы	Сибгеотех	9	199,4
Добыча нефти и природного газа	ТетраСофт	9	157,4
Добыча нефти и природного газа	Юником	9	151,6
Производство кокса и нефтепродуктов	Ртсим	9	80,2
Добыча нефти и природного газа	Симмейкерс	8	77,8
Производство кокса и нефтепродуктов	Датафабрик	8	77,7
Добыча нефти и природного газа	ЭйпТекнолоджи	7	24,9
Геологоразведочные работы	ДГР	7	11,1
Добыча нефти и природного газа	Ласмера	7	8,5
Добыча нефти и природного газа	НЦВ	7	6,5
Добыча нефти и природного газа	Праймгео	7	3,4
Производство кокса и нефтепродуктов	РА	3	0
Добыча нефти и природного газа	МИКРОМОДЕЛ	4	0

Источник: составлено автором на основе данных https://sk.ru/

Проведена корректировка перечня компаний, представленных в таблице 3, с учетом статистических выбросов. Выручка переведена в проценты пропорционально наибольшему объему выручки по компании из скорректированного перечня. Проведен регрессионный анализ (Y – потенциальный рынок, X – MRL) для выявления зависимости между объемом продаж и уровнем рыночной готовности технологии.

Полученная индикативная формула регрессии:

$$Y = 0.3416 * X - 2.3375, \quad (3)$$

при которой R^2 равен 0.84.

Таблица 4. Обработанные данные по стартапам-участникам Инновационного центра Сколково

Отрасль применения	Компания	MRL	Потенциальный рынок
Геологоразведочные работы	Сибгеотех	9	100%
Добыча нефти и природного газа	ТетраСофт	9	79%
Добыча нефти и природного газа	Юником	9	76%
Производство кокса и нефтепродуктов	Ртсим	9	40%
Добыча нефти и природного газа	Симмейкерс	8	39%
Производство кокса и нефтепродуктов	Датафабрик	8	39%
Добыча нефти и природного газа	ЭйпТекнолоджи	7	12%
Геологоразведочные работы	ДГР	7	6%
Добыча нефти и природного газа	Ласмера	7	4%
Добыча нефти и природного газа	НЦВ	7	3%
Добыча нефти и природного газа	Праймгео	7	2%

Уровни рыночной готовности технологий (MRL):

1. Определен целевой рынок, выявлены области применения продукта/технологии.
2. Определены потенциальные потребители и сформулированы проблемы клиентов, сделан базовый конкурентный анализ, сформулирована базовая бизнес-модель.
3. Определены ключевые клиентские сегменты, определены базовые каналы продаж.
4. Получена обратная связь от потенциальных потребителей.
5. Подтверждены параметры спроса, достигнуто первое взаимодействие с потребителями/клиентами.
6. Достигнуты предварительные договоренности с контрагентами, проведены предварительные переговоры с потенциальными потребителями.
7. Достигнуты первые продажи/пилотные внедрения.
8. Достигнуты продажи рыночным потребителям, безубыточность.
9. Масштабирование продаж.

Сегодня уровень рыночной готовности квантовых коммуникаций равен 7: осуществлено пилотное подключение к квантовым сетям компании ПАО «Газпром». Однако в течение нескольких лет аналогичные пилотные проекты единичны, рост рынка обеспечивается преимущественно за счет средств государственной поддержки.

В соответствии с рисунком 2 можно предположить, что стабильное развитие рынка квантовых коммуникаций будет достигнуто в 2030 году, когда экономические риски снижения устойчивости шифрования будут преобладать над стоимостью внедрения продуктов квантового распределения ключей. Соответственно в 2030 году будет достигнут 8 уровень MRL. Основываясь на той же логике можно предположить, что масштабирование продаж и агрессивное проникновение на рынок начнутся в 2038 году с достижением уровня MRL 9.

В соответствии с формулой 4 и прогнозом уровня MRL можно сделать выводы о коэффициенте проникновения квантовых технологий в нефтегазовую отрасль:

- до 2030 г. уровень проникновения может вырасти с 0 до 5%;
- с 2030 г. по 2038 г. уровень проникновения может вырасти с 5% до 40%;
- с 2038 г. уровень проникновения может превысить 40%.

В соответствии с отчетностью ФСТЭК, доля энергетических объектов составляет около 46% от всех объектов критической информационной инфраструктуры [8]. Так как в России общее число объектов КИИ составляет не менее 500 тыс. [5] (включая незарегистрированные), при 100% проникновении услуг квантовых коммуникаций в энергетическую отрасль количество подключений может составить до 230 тыс. В соответствии с прогнозными значениями проникновения, в 2030 г. максимальное количество подключений энергетических объектов к квантовой сети может составить до 12 тыс., в 2038 году – 92 тыс. Отставания от данных показателей могут свидетельствовать о реализации консервативного сценария проникновения квантовых коммуникаций на перспективные рынки.

Заключение

Полученные в ходе исследования результаты позволили дать количественную оценку экономическому аспекту ценностного предложения квантовых коммуникаций для конечных пользователей на примере нефтегазовой компании ПАО «НК «Роснефть», а также определить временные горизонты роста спроса на решения квантовой криптографии.

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.

Литература

1. Аудит-ИТ. Бухгалтерская отчетность и финансовый анализ, 2020. URL: https://www.audit-it.ru/
2. Банк России. Основные направления единой государственной денежно-кредитной политики на 2025 год и период 2026 и 2027 годов, 2024. URL: https://cbr.ru/about_br/publ/ondkp/on_2025_2027
3. Ермакова Е. О., Ерохина А. А. Применение квантовых коммуникаций в ОАО «РЖД»: логистические аспекты //Потенциал логистики XXI века: молодежное измерение. – 2022. – С. 86-93.
4. Лобов Д. С. Финансирование НИОКР, патентная активность и развитие рынка квантовых коммуникаций в России и за рубежом //Информационное общество. – 2023. – №. 5. – С. 123-133.
5. Музалевский Ф. Категорирование: что дальше? О перспективах регулирования КИИ // BIS Journal. М., 2024. URL: https://ib-bank.ru/bisjournal/post/2185
6. 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.
7. 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.
8. Торенко Е.Б. Вопросы реализации ФЗ «О безопасности КИИ РФ», 2019. URL: https://xn--90acqjv.xn--p1ai/wp-content/uploads/2019/03/Torbenko.pdf?ysclid=m2qeci07b2883432236
9. 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. – С. 26-36.
10. Bonnetain X., Naya-Plasencia M., Schrottenloher A. Quantum Security Analysis of AES // IACR Transactions on Symmetric Cryptology. – 2019. 10.46586/tosc.v2019.i2.55-93.
11. Cavaliere F. et al. Secure quantum communication technologies and systems: From labs to markets //Quantum Reports. – 2020. – Т. 2. – №. 1. – С. 80-106.
12. Dervisevic E. et al. Quantum Key Distribution Networks--Key Management: A Survey //arXiv preprint arXiv:2408.04580. – 2024.
13. Freebody M. Quantum Communications Finds Many Paths to Commercialization // Photonics spectra. - 2014. – 48. – С. 42-45.
14. Gartner. IT Key Metrics Data 2022: Industry Measures — Energy Analysis, 2022. URL: https://www.gartner.com/en/documents/4008861
15. Ghosh S. et al. A Survey of Security in SCADA Networks: Current Issues and Future Challenges // IEEE Access. – 2019. 1-1. 10.1109/ACCESS.2019.2926441.
16. Ghosh S. et al. An intrusion resistant scada framework based on quantum and post-quantum scheme //Applied Sciences. – 2021. – Т. 11. – №. 5. – С. 2082.
17. Hötte K. Demand-pull, technology-push, and the direction of technological change //Research Policy. – 2023. – Т. 52. – №. 5. – С. 104740.
18. Ismail S. et al. SCADA systems cyber security for critical infrastructures: Case Studies in the transport sector // In International Conference on Cyber Warfare and Security. – 2015. – С. 446-464. https://doi.org/10.4018/978-1-7998-2466-4.ch028
19. 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. – Т. 31. – №. 1. – С. 205-211.
20. Kaspersky ICS. Первое полугодие 2023 года — краткий обзор основных инцидентов промышленной кибербезопасности, 2023. URL: https://ics-cert.kaspersky.ru/publications/reports/2023/10/05/h1-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity/?ysclid=m26afwdxeq592712534
21. L'Heureux A. V. Prevention effectiveness of Critical Infrastructure Networks: the analysis of California's Oil Spill Prevention and Response Network //International Oil Spill Conference Proceedings. – Allen Press, 2024. – Т. 2024. – №. 1.

22. Malina L. et al. Post-quantum era privacy protection for intelligent infrastructures //IEEE Access. – 2021. – Т. 9. – С. 36038-36077.
23. McKinsey. Enabling the next frontier of quantum computing, 2024. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/enabling-the-next-frontier-of-quantum-computing
24. 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. – Т. 28. – С. 101381.
25. Pentest People. Lost Downtime, 2022. URL: https://www.pentestpeople.com/blog-posts/ransomware-2022-facts-and-statistics#:~:text=Lost%20Downtime,ransomware%20attack%20is%2022%20days
26. Popa A. B., Popescu P. G. The Future of QKD Networks //arXiv preprint arXiv:2407.00877. – 2024.
27. Quantum Insider. White House Report: U.S. Federal Agencies Brace for $7.1 Billion Post-Quantum Cryptography Migration, 2024. URL: https://thequantuminsider.com/2024/08/12/white-house-report-u-s-federal-agencies-brace-for-7-1-billion-post-quantum-cryptography-migration/
28. 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. – Т. 12. – №. 18. – С. 3824.
29. Security Intelligence. 2022 industry threat recap: Energy, 2022. URL: https://securityintelligence.com/articles/2022-industry-threat-recap-energy/
30. Sharma M. et al. Leveraging the power of quantum computing for breaking RSA encryption //Cyber-Physical Systems. – 2021. – Т. 7. – №. 2. – С. 73-92.
31. 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. – Т. 8. – С. 128440-128475.
32. Teigeler H. et al. 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. – 2019.
33. The White House. Budget of the U.S. Government FISCAL YEAR 2024. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/budget_fy2024.pdf

FORECASTING DEMAND FOR QUANTUM COMMUNICATIONS SERVICES IN THE OIL AND GAS INDUSTRY TAKING INTO ACCOUNT THE VALUE PROPOSITION

Lobov Daniil Sergeevich

PhD in economics
MGIMO
Kept, Associate Manager
Moscow, Russian Federation
d.lobov@odin.mgimo.ru

Abstract

The research is dedicated to the study of economic aspects of the implementation of quantum communications technologies. The purpose of the study is to predict the conditions under which the implementation of this innovation will be of economic interest to end users using the example of the oil and gas industry. The hypothesis was that the implementation of quantum communications as an information security tool is of interest to oil and gas companies that own critical information infrastructure in order to reduce the risks of economic losses from the consequences of cybercrimes. To prove this hypothesis, the author conducted a study of the place and role of quantum communications in the information security system of an energy enterprise, estimated the amount of costs for transforming the infrastructure using a quantum component, and gave an economic assessment of the risks associated with the lack of a quantum level of network security. As a result of a comparative analysis of potential costs and risks, the author comes to the conclusion that the lack of mass demand for quantum communications piloting services may be due to insufficient economic effects at the current stage of technological progress, but the success of a potential adversary in the development of quantum computers will increase the demand for quantum communications in the long-term horizon of 2030-2038. The findings may be of interest to specialists working in the field of development and commercialization of the new branch of quantum communications in the Russian Federation.

Keywords

quantum communications, quantum key distribution, post-quantum cryptography, critical information infrastructure, innovation economics

References

1. Audit-IT. Buhgalterskaya otchetnost' i finansovyj analiz, 2020. URL: https://www.audit-it.ru/
2. Bank Rossii. Osnovnye napravleniya edinoj gosudarstvennoj denezhno-kreditnoj politiki na 2025 god i period 2026 i 2027 godov, 2024. URL: https://cbr.ru/about_br/publ/ondkp/on_2025_2027
3. Ermakova E. O., Erohina A. A. Primenenie kvantovyh kommunikacij v OAO «RZhD»: logisticheskie aspekty //Potencial logistiki XXI veka: molodezhnoe izmerenie. – 2022. – S. 86-93.
4. Lobov D. S. Finansirovanie NIOKR, patentnaya aktivnost' i razvitie rynka kvantovyh kommunikacij v Rossii i za rubezhom //Informacionnoe obshchestvo. – 2023. – №. 5. – S. 123-133.
5. Muzalevskij F. Kategorirovanie: chto dal'she? O perspektivah regulirovaniya KII // BIS Journal. M., 2024. URL: https://ib-bank.ru/bisjournal/post/2185
6. Ratkin L. S. Kvantovo-kommunikacionnye sistemy raspredelennyh reestrov dlya hraneniya i obrabotki dannyh o tehnicheskih harakteristikah i finansovo-ekonomicheskih parametrah investicionnyh proektov po razrabotke perspektivnyh modelej avtotransporta //Transport: nauka, tekhnika, upravlenie. Nauchnyj informacionnyj sbornik. – 2021. – №. 5. – S. 61-64.
7. Salygin, V. I., Lobov, D. S. Perspektivy primeneniya tekhnologij kvantovogo raspredeleniya klyuchej na primere ob"ektov neftegazovoj otrasli // Drukerovskij vestnik. – 2023. – № 1(51). – S. 246-253.
8. Torenko E.B. Voprosy realizacii FZ «O bezopasnosti KII RF», 2019. URL: https://xn--90acqjv.xn--p1ai/wp-content/uploads/2019/03/Torbenko.pdf?ysclid=m2qeci07b2883432236 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. – C. 26-36.

9. 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. – С. 26-36.
10. Bonnetain X., Naya-Plasencia M., Schrottenloher A. Quantum Security Analysis of AES // IACR Transactions on Symmetric Cryptology. – 2019. 10.46586/tosc.v2019.i2.55-93.
11. Cavaliere F. et al. Secure quantum communication technologies and systems: From labs to markets //Quantum Reports. – 2020. – Т. 2. – №. 1. – С. 80-106.
12. Dervisevic E. et al. Quantum Key Distribution Networks--Key Management: A Survey //arXiv preprint arXiv:2408.04580. – 2024.
13. Freebody M. Quantum Communications Finds Many Paths to Commercialization // Photonics spectra. - 2014. – 48. – С. 42-45.
14. Gartner. IT Key Metrics Data 2022: Industry Measures — Energy Analysis, 2022. URL: https://www.gartner.com/en/documents/4008861
15. Ghosh S. et al. A Survey of Security in SCADA Networks: Current Issues and Future Challenges // IEEE Access. – 2019. 1-1. 10.1109/ACCESS.2019.2926441.
16. Ghosh S. et al. An intrusion resistant scada framework based on quantum and post-quantum scheme //Applied Sciences. – 2021. – Т. 11. – №. 5. – С. 2082.
17. Hötte K. Demand-pull, technology-push, and the direction of technological change //Research Policy. – 2023. – Т. 52. – №. 5. – С. 104740.
18. Ismail S. et al. SCADA systems cyber security for critical infrastructures: Case Studies in the transport sector // In International Conference on Cyber Warfare and Security. – 2015. – С. 446-464. https://doi.org/10.4018/978-1-7998-2466-4.ch028
19. 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. – Т. 31. – №. 1. – С. 205-211.
20. Kaspersky ICS. Первое полугодие 2023 года — краткий обзор основных инцидентов промышленной кибербезопасности, 2023. URL: https://ics-cert.kaspersky.ru/publications/reports/2023/10/05/h1-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity/?ysclid=m26afwdxeq592712534
21. L'Heureux A. V. Prevention effectiveness of Critical Infrastructure Networks: the analysis of California's Oil Spill Prevention and Response Network //International Oil Spill Conference Proceedings. – Allen Press, 2024. – Т. 2024. – №. 1.
22. Malina L. et al. Post-quantum era privacy protection for intelligent infrastructures //IEEE Access. – 2021. – Т. 9. – С. 36038-36077.
23. McKinsey. Enabling the next frontier of quantum computing, 2024. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/enabling-the-next-frontier-of-quantum-computing
24. 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. – Т. 28. – С. 101381.
25. Pentest People. Lost Downtime, 2022. URL: https://www.pentestpeople.com/blog-posts/ransomware-2022-facts-and-statistics#:~:text=Lost%20Downtime,ransomware%20attack%20is%2022%20days
26. Popa A. B., Popescu P. G. The Future of QKD Networks //arXiv preprint arXiv:2407.00877. – 2024.
27. Quantum Insider. White House Report: U.S. Federal Agencies Brace for $7.1 Billion Post-Quantum Cryptography Migration, 2024. URL: https://thequantuminsider.com/2024/08/12/white-house-report-u-s-federal-agencies-brace-for-7-1-billion-post-quantum-cryptography-migration/
28. 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. – Т. 12. – №. 18. – С. 3824.
29. Security Intelligence. 2022 industry threat recap: Energy, 2022. URL: https://securityintelligence.com/articles/2022-industry-threat-recap-energy/
30. Sharma M. et al. Leveraging the power of quantum computing for breaking RSA encryption //Cyber-Physical Systems. – 2021. – Т. 7. – №. 2. – С. 73-92.

31. 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. – Т. 8. – С. 128440-128475.
32. Teigeler H. et al. 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. – 2019.
33. The White House. Budget of the U.S. Government FISCAL YEAR 2024. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/budget_fy2024.pdf