Кирилл Сергеевич ЕВСИКОВ,
доцент кафедры государственного и административного права Тульского государственного университета, доцент кафедры информационного права и цифровых технологий Университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук, доцент
aid-ltd@yandex.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Информационная безопасность цифрового государства в квантовую эпоху[1]

Аннотация. *В статье проведен обзор цифровой технологии «квантовая коммуникация» и ее места среди «сквозных» цифровых технологий, рассмотрена проблема квантовой угрозы для информационной безопасности Российской Федерации. Используемая сегодня криптография основана на дискретных логарифмах или факторизации, которые утратят свою криптографическую стойкость после появления квантового компьютера. Все страны начали развивать новые технологии защиты информации, способные обеспечить ее конфиденциальность в квантовую эпоху.*

Проанализирован опыт построения новой системы информационной безопасности в Великобритании, Евросоюзе, США, Китае. Проведенный анализ позволил выявить недостатки в нормативной базе, регулирующей квантовую криптографию, к которой относятся квантовое распределение ключей, квантовый генератор случайных чисел, постквантовая криптография.

Автором обосновывается необходимость введения экспериментального правового режима и создания института криптографической гибкости. Реализация этих предложений позволит подготовить нормативную базу для миграции данных в среду, защищенную шифрами, криптоустойчивыми для квантового вычислителя. Изложенное позволяет говорить, что квантовая коммуникация является новым способом защиты информации в цифровом государстве, где данные играют ключевую роль, а их конфиденциальность и целостность становятся залогом национальной безопасности.

Ключевые слова: *квантовый вычислитель, квантовая безопасность, квантовый компьютер, квантовая угроза, квантовая уязвимость, квантовая коммуникация, квантовая криптография, квантовое распределение ключей, квантово-безопасная криптография, постквантовая криптография, квантовый генератор случайных чисел, информационная безопасность, криптографическая гибкость.*

DOI: 10.17803/2311-5998.2022.92.4.046-058

[1] Исследование выполнено в рамках программы стратегического академического лидерства «Приоритет-2030».

KIRILL S. EVSIKOV,
Associate Professor of the Department of state and administrative law of Tula State University,
Associate Professor of the Department of information law and digital technologies of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law), Associate Professor
aid-ltd@yandex.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Information Security of the Digital State in the Quantum Era

Abstract. *The article provides an overview of the digital technology quantum communication and its place among end-to-end digital technologies. Also the problem of quantum threat to the information security of the Russian Federation is considered. The cryptography used today is based on discrete logarithms or factorization, which will lose their cryptographic strength after the implementation of a quantum computer. All countries have started to analyze and develop new information security technologies which are capable to ensure its confidentiality in the quantum era.*

The article analyzes the experience of building a new information security system in several countries (Great Britain, the European Union, the USA, China). The analysis made it possible to evaluate Russian actions in this area, as well as to identify shortcomings in the regulatory framework governing quantum cryptography, which include quantum key distribution, quantum random number generator, post-quantum cryptography.

The author substantiates the need for the introduction of an experimental legal regime and the creation of the «cryptographic agility». The implementation of these proposals will help to prepare a regulatory framework for data migration to an environment protected by cryptographic ciphers resistant to quantum computing. The quantum communication is a new way to protect information in a digital state, where data plays a key role, and their confidentiality and integrity become the key to national security.

Keywords: *quantum computer, quantum security, quantum computer, quantum threat, quantum vulnerability, quantum communication, quantum cryptography, quantum key distribution, quantum secure cryptography, post-quantum cryptography, quantum random number generator, information security, cryptographic flexibility,cryptographic agility.*

Введение

Информация — это ценнейший ресурс, который позволяет менять общество и государство, обеспечивая развитие стран в условиях глобальной конкуренции. Усиление данного фактора сегодня обусловлено появлением новых технологий обработки данных, которые требуют новых правовых регуляторов[2].

Российская Федерация в 2019 г. утвердила Национальную программу развития цифровой экономики[3]. Одной из целей программы является создание «сквозных» цифровых технологий преимущественно на основе отечественных разработок[4]. К ним органы публичной власти отнесли: технологии распределенных реестров, искусственный интеллект, квантовые вычисления, квантовые коммуникации и т.д.[5]

Указанные технологии требуют правовой регламентации, что отмечено специалистами[6]. Следуя общественному запросу, представители всех отраслей права стали активно прорабатывать вопросы регулирования «сквозных» цифровых технологий. Сегодня уже опубликовано значительное количество научных работ с моделями правовой регламентации искусственного интеллекта, смарт-контрактов[7]. Однако до сих пор terra incognita для отечественной юриспруденции остаются квантовые технологии. Хотя риски внедрения квантовых технологий для общества и государства не меньше, чем риски внедрения технологий искусственного интеллекта[8].

Европейский институт телекоммуникационных стандартов (ETSI) в 2016 г. опубликовал отчет о возникновении при создании квантового вычислителя угрозы безопасности информации, защищаемой современными криптографическими

---

2 *Минбалеев А. В.* Система информации: теоретико-правовой анализ : автореф. дис. ... канд. юрид. наук. Челябинск, 2006. 33 с.

3 Паспорт национального проекта «Национальная программа “Цифровая экономика Российской Федерации”», утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7 // СПС «КонсультантПлюс».

4 Паспорт федерального проекта «Цифровые технологии», утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 № 9 // СПС «КонсультантПлюс».

5 Постановление Правительства РФ от 29.03.2019 № 377 (ред. от 22.10.2021) «Об утверждении государственной программы Российской Федерации “Научно-технологическое развитие Российской Федерации”» // СЗ РФ. 2019. № 15 (ч. III). Ст. 1750.

6 *Полякова Т. А., Минбалеев А. В.*, *Кроткова Н. В.* Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права (прошлое и будущее) // Государство и право. 2021. № 12. С. 97—108.

7 Цифровое право : учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. М. : Проспект, 2020. 640 с.

8 *Минбалеев А. В.* Регулирование использования искусственного интеллекта в России // Информационное право. 2020. № 1. С. 36—39.

методами[9]. Криптография — методы обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации[10]. К аналогичным выводам пришли эксперты США[11], Японии[12] и других стран.

В настоящей статье рассмотрены способы защиты информации в условиях квантовой угрозы.

Вторая квантовая революция

В Дорожной карте развития «квантовых технологий» указано, что «первая квантовая революция» привела к появлению лазеров, транзисторов, ядерного оружия, а ее достижения применяются в компьютерах, мобильных телефонах, МРТ-сканерах и т.д.[13] Сегодня мир находится на пороге «второй квантовой революции», позволяющей создавать новые технологические продукты («квантовые технологии»), перечень которых достаточно широк. Важность развития данных технологий отмечена РАН[14].

Российская Федерация определила три квантовые технологии, которым будет оказана государственная поддержка:

1) квантовые вычисления — новый класс вычислительных устройств, использующий для решения задач принципы квантовой механики;
2) квантовые коммуникации — технология криптографической защиты информации;
3) квантовые сенсоры и метрология — совокупность высокоточных измерительных приборов, основанных на квантовых эффектах.

Все эти технологии имеют важное значение для обеспечения позиций России в мировой экономике, а также для построения цифрового государства. Для

[9] ETSI — EG 203 310 Quantum Computing Impact on security of ICT Systems ; Recommendations on Business Continuity and Algorithm Selection // URL: https://standards.globalspec.com/std/10026941/eg%20203%20310 (дата обращения: 04.03.2021).

[10] Национальный стандарт Российской Федерации ГОСТ Р 56875-2016 «Информационные технологии системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий» (утв. приказом Росстандарта от 26.02.2016 № 81-ст.). М. : Стандартинформ, 2016.

[11] Information Security and Privacy Advisoryboard. Meeting Minutes. March 29, 30 and 31, 2017 // URL: https://csrc.nist.gov/csrc/media/events/ispab-march-2017-meeting/documents/ispab-meeting-minutes-march-2017.pdf.

[12] SQAT(r) セキュリティレポート /2019年9月号 // URL: https://www.bbsec.co.jp/report/security_report.html (дата обращения: 04.03.2021).

[13] Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии» // СПС «КонсультантПлюс».

[14] Постановление Президиума РАН от 18.05.2021 № 79 «О состоянии и перспективах развития квантовых технологий в Российской Федерации» // СПС «КонсультантПлюс».

координации процесса их создания и внедрения сегодня используются следующие способы:

— децентрализованный — определены ведущие публичные компании, которые осуществляют развитие конкретной субтехнологии, например вопросами квантовой коммуникации занимается ОАО РЖД[15];
— централизованный — создаются специализированные научные центры, например «Квантовая долина»[16].

Квантовый вычислитель и квантовая угроза

В октябре 2021 г. Министерство внутренней безопасности США опубликовало Меморандум о подготовке к постквантовой криптографии, в котором отметило, что столкнулось с проблемами в области национальной безопасности, включая защиту данных критически важной инфраструктуры[17]. Причиной этого объявлена недостаточная подготовка к переходу на постквантовую криптографию.

Постквантовая криптография — это новый институт в области защиты информации, развивающийся в связи с успехами в создании квантового компьютера.

Квантовые компьютеры и симуляторы — это вычислительные системы, использующие для решения задач квантовые явления[18]. Кроме позитивных результатов от их создания, социум ждет появление устройств, способных расшифровать большинство современных шифров[19]. Эту ситуацию называют квантовой угрозой.

Сегодня продемонстрированы работающие квантовые вычислители. В 2019 г. компания Google опубликовала результаты эксперимента Quantum Supremacy, в ходе которого квантовый процессор Sycamore, который выполнял вычисления за 200 секунд, что эквивалентно 10 000 годам работы обычного компьютера[20].

---

[15] Паспорт «дорожной карты» развития высокотехнологичной области «квантовые коммуникации» на период до 2024 года, утв. Минцифры России 27.08.2020 № 17 // СПС «КонсультантПлюс».

[16] Постановление Правительства РФ от 30.11.2021 № 2133 «О создании инновационного научно-технологического центра “Квантовая” долина» (вместе с Правилами проекта по созданию и обеспечению функционирования инновационного научно-технологического центра «Квантовая» долина) // СЗ РФ. 2021. № 49 (ч. II). Ст. 8318.

[17] Memorandum on Preparing for Post-Quantum Cryptography // URL: https://www.dhs.gov/publication/memorandum-preparing-post-quantum-cryptography (дата обращения: 04.03.2021).

[18] Дорожная карта развития «сквозной» цифровой технологии «квантовые технологии» // СПС «КонсультантПлюс».

[19] *Корольков А. В.* О некоторых прикладных аспектах квантовой криптографии в контексте развития квантовых вычислений и появления квантовых компьютеров // Вопросы кибербезопасности. 2015. № 1 (9). С. 6—13.

[20] Quantum supremacy using a programmable superconducting processor / F. Arute, K Arya., R. Babbush [et al.] // Nature. 2019. 574. 505—510. URL: https://doi.org/10.1038/s41586-019-1666-5 (дата обращения: 04.03.2021).

В 2021 г. китайская группа ученых описала процессор Zuchongzhi, мощность которого в 2—3 раза выше, чем у Google[21].

Кроме этих компаний, в мире существуют десятки организаций, привлекающих значительные инвестиции для создания квантовых вычислителей[22]. Эти результаты позволили специалистам прогнозировать, что технология, способная взломать шифр биткоина, может быть создана в 2027 г., а шифр RSA — в 2031 г.[23] Регулятор Великобритании (The National Cyber Security Centre — NCSC) в рекомендациях 2020 г. прогнозирует появление криптографически значимого квантового компьютерав 2030 г.[24]

Следует учитывать, что большинство прогнозов ориентируются на открытые данные, а в условиях геополитического противостояния существует вероятность, что реальные успехи в построении работоспособного квантового вычислителя будут являться конфиденциальной информацией, и выявить этот момент возможно только после компрометации значительного массива данных.

Таким образом, выдвигаются различные прогнозы создания квантового компьютера, но все они сходятся в двух факторах:

— действующие шифры с открытым ключом будут взломаны, а вероятность взлома других видов шифров высока;
— быстрый переход на новые средства криптографии невозможен.

Важно отметить, что уже сегодня создается программное обеспечение под квантовый компьютер. Квантовые симуляторы, имитирующие квантовый вычислитель на обычном компьютере, доступны для работы всем желающим, например приложение Microsoft[25] и приложение Quirk[26].

---

[21] Strong Quantum Computational Advantage Using a Superconducting Quantum Processor / Yulin Wu [et al.] // Physical Review Letters. American Physical Society. 2021. № 127. URL: https://physics.aps.org/featured-article-pdf/10.1103/PhysRevLett.127.180501 (дата обращения: 04.03.2021).

[22] *Barney Cotton.* Quantum computing start-up Multiverse Computing closes € 10m investment round // Business Leader. 2021. URL: https://www.businessleader.co.uk/quantum-computing-start-up-multiverse-computing-closes-e10m-investment-round/ (дата обращения: 04.03.2021) ; PsiQuantum Closes $ 450 Million Funding Round to Build the World's First Commercially Viable Quantum Computer // URL: https://psiquantum.com/news/psiquantum-closes-450-million-funding-round-to-build-the-worlds-first-commercially-viable-quantum-computer (дата обращения: 04.03.2021) ; IonQ Becomes First Publicly Traded, Pure-Play Quantum Computing Company ; Closes Business Combination with dMY Technology Group III // URL: https://ionq.com/news/october-01-2021-ionq-listed-on-nyse ; (дата обращения: 04.03.2021).

[23] *Mosca M.* Cybersecurity in an Era with Quantum Computers: Will We Be Ready? // IEEE Security & Privacy. 2018. Vol. 16. № 5. P. 38—41. Doi: 10.1109/MSP.2018.3761723.

[24] Quantum-safe cryptography (white paper) // URL: https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography (дата обращения: 04.03.2021).

[25] Квантовые симуляторы // URL: https://docs.microsoft.com/ru-ru/azure/quantum/user-guide/machines/ (дата обращения: 04.03.2021).

[26] URL: https://algassert.com/quirk (дата обращения: 04.03.2021).

Зарубежный опыт по защите информации в условиях квантовой угрозы

Информационная безопасность — важнейший элемент при формировании информационного общества и построении электронного государства[27]. Большинство стран мира признали наличие квантовой угрозы и начали разработку новых методов защиты информации — постквантовой криптографии (Quantum-Safe Cryptography). Анализ зарубежного права позволяет выделить два способа обеспечения информационной безопасности в эпоху квантового компьютера:

1) квантово-устойчивый алгоритм шифрования (Post-Quantum Cryptographic Algorithms);
2) квантовое распределение ключей (Quantum Key Distribution).

Важно отметить, что в отечественных нормативных актах используется иная терминология. Квантовую криптографию приравнивают к квантовому распределению ключей[28], а квантово-устойчивый алгоритм шифрования называется постквантовым алгоритмом.

Приведенный перечень методов защиты информации не является исчерпывающим. NCSC указывает на возможность применения шифров на основе квантового генератора случайных чисел (Quantum Random Number Generation)[29]. Одновременно регулятор отмечает, что хотя существует много научных исследований безопасности и эффективности различных постквантовых криптографических схем, но в настоящее время дать точные рекомендации он затрудняется. Вероятно, это обусловлено тем, что NCSC планирует использовать постквантовый алгоритм, который будет стандартизирован регулятором США (National Institute of Standardsand Technology — NIST).

NIST сегодня является мировым центром по анализу алгоритмов постквантовой криптографии, чему способствовало проведение открытого конкурса, объявленного в 2018 г. В ходе него группы исследователей предложили шифры, которые квантовый компьютер не способен взломать. На первом этапе представлено 50 шифров различными научными организациями (в их числе Корейский университет, Китайская академия наук, Университет Сорбонны, Университет Ватерлоо и др.) и технологическими компаниями (IBM Research, Microsoft, Philips Research, Intel и др.)[30].

---

[27] *Полякова Т. А.* О современных тенденциях развития правового регулирования в области обеспечения информационной безопасности при построении информационного общества в России // Вестник Российского университета дружбы народов. Серия : Информатизация образования. 2008. № 1. С. 12—19.

[28] Указ Президента РФ от 17.12.2011 № 1661 (ред. от 19.02.2021) «Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль» // СЗ РФ. 2011. № 52. Ст. 7563.

[29] Quantum security technologies (white paper) // URL: https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies (дата обращения: 04.03.2021).

[30] First PQC Standardization Conference // URL: https://csrc.nist.gov/events/2018/first-pqc-standardization-conference.

После публичного обсуждения отобраны алгоритмы, которые перешли во второй этап, а далее — в финальный третий раунд конкурса, после которого американский регулятор планирует сертифицировать квантово-устойчивый алгоритм шифрования[31]. Новые стандарты криптографии планируется опубликовать до 2024 г.[32], но уже сегодня регулятор рекомендует учитывать «криптографическую гибкость», которая гарантирует, что шифрование будет легко обновлено или заменено.

Пока органы власти анализируют алгоритмы защиты информации, компании начали внедрять их в свою деятельность. Так, IBM в 2022 г. предоставляет пользователям облачных сервисов гибридный алгоритм защиты информации, который использует комбинацию квантового безопасного алгоритма и классических алгоритмов обмена ключами[33]. Данный пример касается отдельного сервиса, тогда как массовое внедрение постквантовых алгоритмов шифрования требует значительного времени и ресурсов для обновления криптографической инфраструктуры.

К миграции данных под квантово-безопасную криптографию готовится и Европа. Европейский регулятор (ETSI) подготовил Стратегию миграции и рекомендации по схемам квантовой безопасности[34]. Документ способствует переходу на полностью квантово-безопасное криптографическое состояние (Fully Quantum Safe Cryptographic State — FQSCS). По стандарту ETSI, это состояние системы, в котором все криптографические активы используют квантово-безопасную криптографию, основы которой определены регулятором[35].

Пока одни страны осуществляют анализ и стандартизацию алгоритмов криптографии, устойчивых к квантовым вычислителям, другие развивают технологию квантового распределения ключей. Эта технология защиты информации основана не на математических задачах, а на законах квантовой физики, нарушить которые злоумышленник не может.

Лидером в данной сфере является Китай, который создал линию связи, защищенной протоколами квантового шифрования протяженностью 4 600 километров[36]. Функционирование китайской линии квантовой связи обеспечивается двумя спутниками. Для развития квантового распределения ключей КНР

---

[31] Post-Quantum Cryptography. Round 3 Submissions // URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions (дата обращения: 04.03.2021).

[32] Post-Quantum Cryptography Frequently Asked Questions / U. S. Department of Homeland Security. October 2021 // URL: https://www.dhs.gov/sites/default/files/publications/post_quantum_cryptography_faq_3_seals_october_2021_508.pdf (дата обращения: 04.03.2021).

[33] Introduction to Quantum-safe Cryptography in TLS // URL: https://cloud.ibm.com/docs/key-protect?topic=key-protect-quantum-safe-cryptography-tls-introduction (дата обращения: 04.03.2021).

[34] Migration strategies and recommendations to Quantum Safe schemes // Technical Report. ETSITR 103 619 V 1.1.1 (2020-07). URL: https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf (дата обращения: 04.03.2021).

[35] Quantum-Safe Cryptography. Quantum-Safe threat assessment // ETSI GR QSC 004 V1.1.1 (2017-03). URL: https://www.etsi.org/deliver/etsi_gr/qsc/001_099/004/01.01.01_60/gr_qsc004v010101p.pdf (дата обращения: 04.03.2021).

[36] An integrated space-to-ground quantum communication network over 4,600 kilometres / Y. A. Chen, Q. Zhang, T. Y. Chen [et al.] // Nature. 2021. № 589. P. 214—219. URL: https://doi.org/10.1038/s41586-020-03093-8.

реформировал нормативную базу. В 2020 г. принят Закон о шифровании, задачами которого являются:
— развитие криптографии;
— стандартизация и управление криптографией;
— развитие криптографической индустрии;
— стимулирование создания качественных рыночных продуктов.

В соответствии с данным нормативным правовым актом Китай продолжает жесткую регламентацию средств криптографии, используемых для защиты данных органов публичной власти, но допускает формирование «коммерческой криптографии». В 2021 г. КНР утвердил три стандарта для оборудования, используемого в процессе квантового распределения ключей. Кроме стандартов для оборудования, китайский регулятор в 2021 г. утвердил 16 новых стандартов криптографии, два из которых полностью посвящены квантовому распределению ключей.

Важность технологий квантового распределения ключей для национальной безопасности признано не только Китаем. Евросоюз отнес оборудование для квантовой криптографии к товарам двойного назначения[37]. Квантовую криптографию сегодня начали использовать и представители цифрового рынка. Например, в 2021 г. Samsung представил смартфон Galaxy Quantum2 со встроенным квантовым генератором случайных чисел.

Российская Федерация в условиях квантовой угрозы

В пункте «м» ст. 71 Конституции РФ закреплено, что в ве́дении Российской Федерации находится обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных[38]. Это означает, что обязанностью федеральных органов публичной власти является обеспечение информационной безопасности граждан и организаций. Данная норма приобретает новое значение в условиях развития квантовых технологий.

Сегодня в России существуют нормативная база, подробно регламентирующая создание и эксплуатацию средств защиты информации[39], а также несколько государственных стандартов, описывавших алгоритмы шифрования, например блочные шифры «Магма» и «Кузнечик»[40]. Эти шифры некриптоустойчивы к квантовому компьютеру, а значит, требуют усиления в ближайшей перспективе.

---

[37] Council Regulation (EC) № 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items // OJ L 134. 29.05.2009. P. 1—269.

[38] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изм., одобренными в ходе общероссийского голосования 01.07.2020) // URL: http://www.pravo.gov.ru (дата обращения: 04.03.2021).

[39] Приказ ФСБ России от 09.02.2005 № 66 (ред. от 12.04.2010) «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (зарегистр. в Минюсте РФ 03.03.2005 № 6382) // Российская газета. 19.03.2005. № 55.

[40] Национальный стандарт РФ ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» // СПС «Кодекс».

В Дорожной карте развития «квантовых технологий» закреплено, что защита распределенных реестров, блокчейнов и критически важных производственных сегментов должна осуществляться при помощи квантовой криптографии и постквантовых алгоритмов. Это значит, что Российская Федерация рассматривает оба способа защиты информации в постквантовую эпоху.

При этом в России нет рекомендаций о шифровании данных коммерческими компаниями квантовой или постквантовой криптографией. Отсутствуют данные о рисках информационной безопасности, необходимые для планирования криптоустойчивости создаваемых информационных систем к квантовым атакам. Оценка подобных рисков основана на трех параметрах: сроке хранения данных, времени миграции на системы, предназначенные для защиты от квантовых атак, и времени, оставшемся до того, как квантовые компьютеры взломают систему безопасности.

Неопределенность усугубляет и тот факт, что массовое использование любого из существующих сегодня способов постквантового шифрования требует нескольких лет для безопасной миграции данных. Запаздывание существует и в сфере разработки и принятия нормативных правовых актов. Например, в Великобритании в 2020 г. вышла обновленная официальная версия рекомендаций (white paper) о квантово-безопасной криптографии (Quantum-safe cryptography),[41] а в России не опубликовано ни официальных рекомендаций, ни стандартов.

Сегодня есть несколько отечественных центров, проводящих исследования в области квантовых технологий, создающих технологические решения в области защиты информации. Ряд разработок уже нашли свое реальное воплощение. В 2016 г. запущена в эксплуатацию линия квантовой связи, соединившая два здания «Газпромбанка» в Москве, а в 2017 г. проведена первая в мире экспериментальная демонстрация технологии квантового блокчейна[42]. В 2021 г. ОАО «РЖД» запущена первая линия квантовой связи между Москвой и Санкт-Петербургом[43]. Однако исследования показывают, что проекты находятся в правовом вакууме. Важно отметить, что деятельность по распространению криптографических систем является лицензируемым видом деятельности[44], что накладывает ограничения на исследователей в данной сфере.

Также в России не урегулирован вопрос о линиях передачи квантовых состояний, и пока для квантовой коммуникации не создан специальный правовой режим, она регулируется законодательством о связи. Представляется, что указанные правовые барьеры могут быть устранены в рамках «регуляторных песочниц».

---

[41] Preparing for Quantum-Safe Cryptography // URL: https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography (дата обращения: 04.03.2021).

[42] Информационная безопасность в эпоху квантовых технологий // URL: https://www.pwc.ru/ru/assets/pdf/quantim-cybersecurity-publication-rus.pdf (дата обращения: 04.03.2021).

[43] Дмитрий Чернышенко запустил первую линию квантовой связи между Москвой и Санкт-Петербургом // URL: http://government.ru/news/42449/ (дата обращения: 04.03.2021).

[44] Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» (с изм. и доп., вступ. в силу с 01.01.2022). П. 1 ч. 1 ст. 12 // Российская газета. 06.05.2011. № 97.

Квантовая коммуникация включена в перечень технологий, для которых может быть установлен экспериментальный правовой режим в сфере цифровых инноваций[45].

Таким образом, ОАО «РЖД» может инициировать его создание для линии квантовой коммуникации. Важно отметить, что специальный правовой режим не заменит полноценного правового регулирования, так как он ограничивается периодом времени и служит для разработки, апробации и внедрения цифровой инновации[46]. Однако он станет связующим элементом для гармонизации многочисленных требований нормативных правовых актов в области связи и информационно-телекоммуникационных технологий.

Заключение

Появление новых информационных технологий открыло для общества и государства новые возможности по сбору и обработки информации. Новые массивы данных, растущие в геометрической прогрессии, стали ресурсом, привлекающим внимание злоумышленников, желающих получить или повредить их содержимое. С этого момента государства всего мира начинают активно развивать институты защиты информации.

Однако, как справедливо отмечают специалисты, большинство шагов по регулированию защиты информации на национальном уровне терпят неудачу[47]. Это заставляет общество и государства искать принципиально новые способы защиты данных. Отдельные способы становятся самостоятельной цифровой технологией, формирующей целый сектор коммерческой деятельности. К подобным технологиям можно отнести новый метод шифрования, получивший наименование «блокчей»н»[48]. Его востребованность подтверждает, что запрос на новые и эффективные способы защиты данных в мире есть. Ожидается, что этот запрос увеличится в ближайшее время, что вызвано наличием квантовой угрозы.

Сегодня страны, занимающие лидерские позиции в развитии цифровых технологий, формируют новые методы защиты данных: квантовую и постквантовую криптографию. Их развитие относят к вопросам национальной безопасности, что подтверждает анализ нормативных актов иностранных государств. Важность технологий для Российской Федерации отмечается в федеральном проекте

---

[45] Постановление Правительства РФ от 28.10.2020 № 1750 «Об утверждении перечня технологий, применяемых в рамках экспериментальных правовых режимов в сфере цифровых инноваций» // СЗ РФ. 2020. № 44. Ст. 7003.

[46] Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (ред. от 02.07.2021) // СЗ РФ. 2020. № 31 (ч. I). Ст. 5017.

[47] *Полякова Т. А., Минбалеев А. В.*, *Бойченко И. С.* Проблемы правового обеспечения информационной безопасности в процессе использования цифровых технологий в глобальной цифровой среде // Вестник Академии права и управления. 2018. № 3 (52). С. 32—36.

[48] *Минбалеев А. В., Сафронов Е. Г.* Правовая природа блокчейн // Вестник Южно-Уральского государственного университета. Серия : Право. 2018. Т. 18. № 2. С. 94—97.

«Информационная безопасность»[49]. Все это говорит, что страны признают наличие квантовой угрозы, и пытаются избежать рисков разрушения систем защиты данных, вызванных появлением квантового компьютера.

Ряд стран придерживаются мнения, что постквантовая криптография позволит освободиться от угрозы информационной безопасности в квантовую эпоху. Однако криптоустойчивость новых алгоритмов оценивается экспертами, которые могут ошибаться. Например, в США использовались алгоритмы MD5 и SHA-1, которые, по оценке специалистов, обеспечивали достаточный уровень информационной безопасности. Однако китаянка Ван Сяоюнь в 2004 г. взломала MD5, а в 2005 г. — SHA-1 шифры[50]. Важно отметить, что Китай имеет высокий уровень развития криптографии, позволяющий не только создавать шифры, но и находить в них уязвимости. Не вызывает сомнений, что создание квантового компьютера сможет поднять данную сферу деятельности на новый уровень.

Важно отметить, что отсутствие квантового компьютера сегодня не делает коммуникацию, основанную на действующих ГОСТах, криптоустойчивой. Передаваемые данные могут быть сохранены злоумышленником и взломаны в момент появления квантового компьютера. Исходя из этого, в России необходимо принимать неотложные меры по развитию квантовой и постквантовой криптографии, особенно там, где участие человека для смены ключа затруднительно (беспилотный транспорт, интернет вещей). Чтобы смягчить затраты на миграцию данных, уже сегодня целесообразно ввести институт криптографической гибкости.

БИБЛИОГРАФИЯ

1. *Корольков А. В.* О некоторых прикладных аспектах квантовой криптографии в контексте развития квантовых вычислений и появления квантовых компьютеров // Вопросы кибербезопасности. — 2015. — № 1 (9). — С. 6—13.
2. *Минбалеев А. В.* Регулирование использования искусственного интеллекта в России // Информационное право. — 2020. — № 1. — С. 36—39.
3. *Минбалеев А. В.* Система информации: теоретико-правовой анализ : автореф. дис. ... канд. юрид. наук. — Челябинск, 2006. — 33 с.
4. *Минбалеев А. В., Сафронов Е. Г.* Правовая природа блокчейн // Вестник Южно-Уральского государственного университета. — Серия : Право. — 2018. — Т. 18. — № 2. — С. 94—97.
5. *Полякова Т. А.* О современных тенденциях развития правового регулирования в области обеспечения информационной безопасности при построении информационного общества в России // Вестник Российского университе-

[49] План мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации», утв. Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 18.12.2017 № 2) // СПС «КонсультантПлюс».

[50] 王小云：连破两套美国顶级密码，获711万国家奖金，美国不淡定了 // URL: https://www.163.com/dy/article/go4uua6a0543idaw.html (дата обращения: 04.03.2021).

та дружбы народов. — Серия : Информатизация образования. — 2008. — № 1. — С. 12—19.
6. *Полякова Т. А., Минбалеев А. В.*, *Бойченко И. С.* Проблемы правового обеспечения информационной безопасности в процессе использования цифровых технологий в глобальной цифровой среде // Вестник Академии права и управления. — 2018. — № 3 (52). — С. 32—36.
7. *Полякова Т. А., Минбалеев А. В.*, *Кроткова Н. В.* Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права (прошлое и будущее) // Государство и право. — 2021. — № 12. — С. 97—108.
8. Цифровое право : учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. — М. : Проспект, 2020. — 640 с.
9. An integrated space-to-ground quantum communication network over 4,600 kilometres / Y. A. Chen, Q. Zhang, T. Y. Chen [et al.] // Nature. — 2021. — № 589. — P. 214—219.
10. *Mosca M.* Cybersecurity in an Era with Quantum Computers: Will We Be Ready? // IEEE Security & Privacy. — 2018. — Vol. 16. — № 5. — P. 38—41. — Doi: 10.1109/MSP.2018.3761723.
11. Strong Quantum Computational Advantage Using a Superconducting Quantum Processor / Yulin Wu [et al.] // Physical Review Letters / American Physical Society. — 2021. — № 127. — https://physics.aps.org/featured-article-pdf/10.1103/physrevlett.127.180501 (дата обращения: 04.03.2021).
12. Quantum supremacy using a programmable superconducting processor. F. Arute, K. Arya, R. Babbush [et al.] // Nature. — 2019. — 574. — 505—510. — URL: https://doi.org/10.1038/s41586-019-1666-5 (дата обращения: 04.03.2021).