Информационное общество и право

ОБЗОР НОРМАТИВНЫХ ТРЕБОВАНИЙ, ОБЕСПЕЧИВАЮЩИХ НАЦИОНАЛЬНУЮ БЕЗОПАСНОСТЬ США В СФЕРЕ КВАНТОВЫХ ТЕХНОЛОГИЙ

Статья рекомендована к публикации членом редакционного совета М.В. Якушевым 20.10.2022.

Жарова Анна Константиновна

Доктор юридических наук, доцент
Институт государства и права РАН, старший научный сотрудник
Москва, Российская Федерация
Anna_jarova@mail.ru

Аннотация

Ощущается нехватка российских правовых исследований в области применения квантовых технологий. С одной стороны, это объяснимо, поскольку реализация квантовых технологий в обществе еще не начата. С другой стороны, за рубежом уже обсуждаются вопросы о рисках и угрозах, которые может принести применение квантовых технологий. В статье сделан обзор нормативных правовых документов США, принятых за период с 2019 по 2022 год, направленных на регулирование использования квантовых технологий в гражданском и военном секторе, возможных социальных рисков и угроз, а также основных направлений развития и формирования системы обеспечения национальной безопасности США.

Ключевые слова

квантовые технологии; риски; угрозы; стандартизация; США; национальная безопасность

Понятие квантовых технологий

Первая теоретическая модель квантовых вычислений, и в дальнейшем, разработка на ее основе квантовой технологии, была создана в СССР в 1980 –х годах основателем квантовой информатики Ю.И. Маниным [1]. Хотя авторы из США считают, что основателем квантовых вычислений является Д. Дойч, который в 1990-х годах предположил возможность разработки квантового компьютера[2]. Квантовый компьютер работает с кубитами, в отличие от привычного компьютера, производящего вычисления в битах. У квантового компьютера три состояния 0, 1 или сразу 0 и 1. Свойство кванта – одновременно являться частицей и волной, т.е. находиться в состоянии суперпозиции позволяет ему одновременно занимать состояние 0 и 1.

Несмотря на то, что на теоретическом уровне возможность разработки квантовой технологии и квантовых вычислительных устройств была доказана еще в 1980-х годах, проблемы, связанные с интеграцией этой технологии в общество и обеспечением национальной безопасности при использовании квантовых технологий стали обсуждаться в научных статьях только в последнее время. Связано это с тем, что к настоящему времени ученые приблизились к решению проблемы реализации процессов квантовой физики.

Для описания этапов развития теоретической и экспериментальной квантовой физики и квантовых технологий используются термины «первая и вторая квантовая революция» [5]. С конца XX века мир находится на пороге «второй квантовой революции»[3],[4] происходит переход развития общества от цифровых отношений к квантовым отношениям. «Вторая квантовая революция» отражает появление у ученых возможностей и инструментов манипуляции «не только атомами, группами частиц и их наблюдаемыми свойствами, но и индивидуальными квантовыми объектами в состоянии суперпозиции, а также сложными системами в запутанном состоянии» [6].

© Жарова А.К., 2023.
Производство и хостинг журнала «Информационное общество» осуществляется Институтом развития информационного общества.
Данная статья распространяется на условиях международной лицензии Creative Commons «Атрибуция — Некоммерческое использование — На тех же условиях» Всемирная 4.0 (Creative Commons Attribution – NonCommercial - ShareAlike 4.0 International; CC BY-NC-SA 4.0). См. https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.ru
https://doi.org/10.52605/16059921_2023_03_69

В соответствии с Дорожной картой развития «сквозной» цифровой технологии «Квантовые технологии» (далее Дорожная карта развития квантовых технологий) [5] квантовые технологии «основаны на высоком уровне управления сложными квантовыми системами на уровне отдельных частиц, например, атомов и фотонов» и делятся на три субтехнологии: квантовые вычисления, квантовые коммуникации и квантовые сенсоры и метрология [5].

1.Мировые центры развития квантовых технологий

Основным пользователем данных технологий является государство и это объясняется стратегической важностью квантовых технологий для обеспечения национальной безопасности.

В мире стали создаваться несколько основных центров развития квантовых технологий – Китай и США[5]. К сожалению, Российская научная школа «значительно пострадала из-за массового отъезда ученых за границу в 90-х и 2000-х годах»[5], но в настоящее время перед учеными Российской Федерации поставлена задача прорыва и захвата лидирующих позиций в отдельных направлениях квантовых технологий.[5]

Клон К. сравнивая состояние исследований в Российской Федерации и США, пишет, что объем российских исследований незначителен по сравнению с зарубежным. «Один только Стэнфордский университет имеет более 6200 исследовательских проектов, финансируемых извне, с общим бюджетом в 1,64 миллиарда долларов в 2017-2018 годах, в результате чего ежегодно публикуется более 700 научных работ». [7]. Зарубежные исследователи связывают рост государственно-частного партнерства в США в области создания квантовых технологий с тесным взаимодействием государства с военным и разведывательным сообществом и их финансированием [8]. Рост китайской научной школы связывается сугубо с местными инновациями [8].

Хотелось бы подчеркнуть, что, несмотря на большие финансовые вливания и государственную поддержку, все мировые центры работают на перспективу, поскольку до настоящего времени в области квантовой инженерии не решены многие технологические проблемы, например, проблемы передачи кванта на расстояние, минимизации шума. Хотя математические методы устранения названных проблем уже предлагаются. По оценкам некоторых экспертов, большие квантовые компьютеры могут появиться не раньше, чем через десять лет[9],[13]., другие считают, что через двадцать лет[10],[11],[12].

2. Правовое предотвращение рисков и угроз национальной безопасности

Несмотря на то, что речь о правом регулировании отношений можно вести только тогда, когда они возникли, ученые в области права уже сейчас задумались о вероятных рисках и угрозах национальной безопасности, которые может принести использование квантовых технологий. В Дорожной карте развития квантовых технологий угроза информационной безопасности связывается с «использование свойств квантовых систем для передачи ключей» [5]. Эту же угрозу отмечают ученые [14] и Агентство национальной безопасности США (АНБ) [15].

Дорожной картой развития квантовых технологий к рискам информационной безопасности отнесены «наличие закладок в оборудовании», «ограничение доступа к продуктам зарубежных производителей», несанкционированный «доступ к защищаемой информации». В данном документе определено, что для обеспечения безопасности Российской Федерации необходимо установить риски и возможные ограничения развития квантовых технологий, а также создать перспективные российские решения на их базе к 2024 г. Важность разработки норм, методов и средств оценки безопасности систем квантовой криптографии, работающих по открытому пространству, а также технологий квантового интернета, подтверждается Минцифры России [16].

К сожалению, на данный момент в открытом доступе не размещен официальный документ, содержащий комплексный анализ и оценку потенциальных уязвимостей, угроз и рисков информационной безопасности, характерных для систем, реализованных на квантовых технологиях.

Наиболее полно в научной литературе представлена информация о возможных квантовых угрозах безопасности компании, которые могут возникнуть в связи с возможностью расшифровки информации с помощью квантовых компьютеров [17], системной незащищенностью данных, невыполнением положений стандартов, [21], [10], отсутствием рекомендаций государственных

органов, определяющих план перехода на квантово-устойчивое шифрование[18]. В США в целях исправления обозначенной проблемы обнародован в 2021 г. многолетний план перехода государственных организаций США на квантово-устойчивую криптографию [29], [30].

Большая часть правовых исследований в области квантовых технологий посвящены проблемам безопасности обрабатываемой информации в связи с увеличивающейся вероятностью раскрытия информации ограниченного доступа. Это объясняется необходимостью предотвращения рисков нарушения конфиденциальности информации [32], раскрытия различных тайн[33], в том числе тайны частной жизни лица[14]. Развитие квантовой криптографии позволит минимизировать данные риски. Квантовая криптография отнесена к наиболее перспективной области развития российской науки и технологий на период до 2030 г., обеспечивающей реализацию конкурентных преимуществ страны[19] и принципиально новым парадигмам, благодаря которой планируется обеспечение информационной безопасности Российской Федерации и разработка средств защиты компьютерных инфраструктур (п.6).[19] Обеспечение информационной безопасности национальных сетей связи также связывается с использованием квантовых криптографических технологий [20].

3.Обзор правовых средств США в области квантовых технологий

Формирование законодательной системы США в области квантовых технологий условно можно обозначить 2019 г., когда был принят Закон о Национальной квантовой инициативе США (National Quantum Initiative Act - (NQIA)) [22].

Целью NQIA является обеспечение постоянного лидерства США в области квантовой информатики и ее технологических приложений путем поддержки исследований, разработок, демонстрации и применения квантовой информатики и технологий, расширение числа исследователей, преподавателей и студентов, обучающихся квантовой информатике в целях формирования кадрового резерва, содействия разработке и включению междисциплинарных учебных программ в образовательный процесс.

Большое внимание в NQIA уделяется вопросам стандартизации квантовых технологий, а также их безопасности и коммерциализации. В NQIA сделана ставка на государственно-частное партнерство в целях доведения квантовых исследований до конкурентных разработок.

В целях развития положений NDAA направленных на модернизацию системы национальной безопасности США и правительственных КИИ, используемых в военной и разведывательной деятельности, а также для хранения или передачи секретной информации в январе 2022 г. президентом США был подписан меморандум о повышении обороноспособности систем национальной безопасности США[27]. В соответствии с данным меморандумом АНБ будет издавать обязательные оперативные директивы необходимые департаментам и агентствам для обеспечения их кибербезопасности, а также разъяснения о применении методов устранения уязвимостей в квантовых технологиях.

Обязательность проверки программных продуктов (ПО) на наличие уязвимостей и их соответствия стандартам, разработанным для госучреждений и госзакупок, была утверждена в 2021 г. исполнительным указом об улучшении национальной кибербезопасности [28]. Данный указ явился реакцией на произошедший инцидент, связанный с взломом инфраструктуры американской ИТ компании «SolarWinds». В соответствии с исполнительным указом закупленное государством коммерческое ПО должно проходить проверку на соответствие стандартам кибербезопасности, а поставщики ПО обязаны сообщать обо всех кибервзломах, произошедших при использовании разработанных ими технологий.

В 2022 г. Меморандум о национальной безопасности и продвижении лидерства США в области квантовых вычислений при одновременном снижении рисков для уязвимых криптографических систем (NSM)[9] обозначил начало поэтапного многолетнего процесса перевода уязвимых компьютерных систем на квантово-устойчивую криптографию. В NSM определены следующие риски национальной безопасности США: квантовая криптография, взлом систем контроля и управления КИИ, а также протоколов безопасности большинства интернет-транзакций.

В приложении к NSM сформулированы требования к агентствам, которые финансируют исследования, разрабатывают или приобретают квантовые компьютеры. Агентства в соответствии

с разделом 102 (b) (3) NQIA и разделом 6606 NDAA обязаны согласовывать свои действия с Национальным бюро по квантовой координации.

Вопрос стандартизации поднимается во всех правовых документах США. Так, в соответствии с NSM правительство США обеспечивает кибербезопасность посредством стандартизации закупаемых технологий. Правительственные учреждения США обязаны определить приоритеты перехода на квантово-устойчивую криптографию и разработать методики, позволяющие максимально снизить квантовый риск к 2035 г. Руководители агентств федеральных учреждений гражданской исполнительной власти, до выпуска NIST первого набора стандартов квантово-устойчивой криптографии, запланированного к 2024 г., используя существующие криптографические решения, обязаны проводить тестирование на их устойчивость, совместимость и безопасность. NSM также обязывает агентства перейти на использование средств защиты с симметричным ключом до 31 декабря 2023 г. Выбор системы симметричного шифрования, по мнению исследователей, связан с его устойчивостью квантовому взлому [31].

Кроме того, США предусматривают постоянное взаимодействие с другими странами, которые инвестируют в квантовые технологии. Национальный стратегический обзор науки квантовой информатики (National Strategic Overview for Quantum Information Science) подчеркивает важность двусторонних соглашений для поддержки совместных проектов. Так, в рамках двухстороннего сотрудничества США и Япония подписали Токийское заявление о квантовом сотрудничестве в 2019 году. Это было первым двусторонним дипломатическим соглашением в сфере сотрудничества США в области развития квантовой информатики [23].

Анализ нормативных инструментов обеспечения квантовой безопасности США позволяет заключить, что сделана ставка на комплексное применение следующих правовых, организационных и технических инструментов: стандартизации, внедрения квантово-устойчивой криптографии, государственно-частное партнерство, включая жесткое государственное планирование перехода на использование квантово-устойчивой криптографии, коммерциализация получаемых разработок, а также их диверсификация.

Заключение

Несмотря на то, что риски, связанные с нарушением квантового шифрования могут наступить как минимум только через десять лет, речь о решении социальных проблем ведется уже сейчас.

Сравнивая нормативные документы Российской Федерации и США можно отметить, что в России также ведется государственное планирование в области квантовых технологий. Однако в отечественных документах основной акцент сделан на научной, исследовательской и образовательной траектории. Вопросам обязательной стандартизации и разработки методологии перехода на квантово-устойчивое шифрование внимания почти не уделяется.

Отставание при переходе на кантовые технологии создаст серьезные риски нарушения информационной безопасности как для государственного сектора, так и для частного сектора. Возможным направлением развития государственно-частного партнерства является создание экосистемы квантовых технологий. Государство в таком партнерстве может получить контроль над разрабатываемыми технологиями, оказывать поддержку разработчикам, обеспечивать внедрение технологий в свою инфраструктуру и защиту этих технологий, тем самым обеспечивая собственную национальную безопасность.

Литература

1. Манин Ю.И. Вычислимое и невычислимое. - М. : Сов. радио. 1980. - 128 с., ил., (Кибернетика). с. 13—15.
2. The Father of Quantum Computing // https://www.wired.com/2007/02/the-father-of-quantum-computing/
3. Dowling J. and Milburn G., “Quantum Technology, the Second Quantum Revolution,” Phil. Trans. R. Soc. Lond. A (2003).
4. Jaeger L. The Second Quantum Revolution in book Entanglement to Quantum Computing and Other Super-Technologies, 2018 //

https://www.researchgate.net/publication/330196239_The_Second_Quantum_Revolution_From_Entanglement_to_Quantum_Computing_and_Other_Super-Technologies
5. Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии» (документ опубликован не был) // СПС «КонсультантПлюс».
6. Терехович В.Э. Революционные трансформации в квантовой физике и инновации в квантовых технологиях // https://cyberleninka.ru/article/n/revolyutsionnye-transformatsii-v-kvantovoy-fizike-i-innovatsii-v-kvantovyh-tehnologiyah DOI: 10.13140/RG.2.2.22297.88161
7. Klon K. Quantum Science and National Security: A Primer for Policymakers // https://www.heritage.org/technology/report/quantum-science-and-national-security-primer-policymakers
8. Elsa B. Kania & John K. Costello QUANTUM HEGEMONY? China's Ambitions and the Challenge to U.S. Innovation Leadership https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf?mtime=20180912133406%20(дата%20обращения:%2025%20января%202019%20года
9. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems // https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
10. Lee M. Quantum Computing and Cybersecurity // https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity#footnote-039
11. University of Science and Technology of China, "The World's First Integrated Quantum Communication Network," January 6, 2021, https://phys.org/news/2021-01-world-quantum-network.html.
12. Pires F. U.S. National Security Agency Issues Update on Quantum-Resistant Encryption. September 02, 2021 // https://www.tomshardware.com/news/us-national-security-agency-issues-update-on-crypto-resistant-encryption
13. Future Series: Cybersecurity, emerging technology and systemic risk// https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk/
14. Li-Zhen Gao, Xin Zhang, Song Lin, Ning Wang, Gong-De Guo Authenticated Multiparty Quantum Key Agreement for Optical-Ring Quantum Communication Networks // https://www.frontiersin.org/articles/10.3389/fphy.2022.962781/full
15. Ryan N. US Gov Issues Security Memo on Quantum Computing Risks // https://www.securityweek.com/us-gov-issues-security-memo-quantum-computing-risks
16. Письмо Минцифры России от 13.10.2021 № П25-18390-ОГ «О рассмотрении обращения» (вместе с "Паспортом федерального проекта "Информационная безопасность") (документ опубликован не был) // СПС «КонсультантПлюс».
17. Surapol R., Wanchai P. Analysis of Security of Quantum Key Distribution Based on Entangled Photon Pairs by Model Checking // Journal of Quantum Information Science. Vol.5 No.3, September 2015. DOI: 10.4236/jqis.2015.53012
18. Buchholz S., Mariani J, Routh A. The realist's guide to quantum technology and national security What nontechnical government leaders can do today to be ready for tomorrow's quantum world // https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html
19. Прогноз научно-технологического развития Российской Федерации на период до 2030 года (утв. Правительством РФ) (документ опубликован не был)// СПС «КонсультантПлюс».
20. Паспорт национального проекта «Национальная программа „Цифровая экономика Российской Федерации"» (документ опубликован не был)// СПС «КонсультантПлюс».
21. Kop M. Establishing a Legal-Ethical Framework for Quantum Technology Yale Law School. Yale Journal of Law & Technology (YJoLT), The Record, March 30 2021 Available from: https://www.researchgate.net/publication/350524217_Establishing_a_Legal-Ethical_Framework_for_Quantum_Technology [дата обращения: 30.09.2022].

22. H.R.6227 – National Quantum Initiative Act https://www.congress.gov/bill/115th-congress/house-bill/6227/text#HDEB502BED9CC4603A0E5F21C179960E7
23. Tokyo Statement on Quantum Cooperation (U.S. Department of State, December 19, 2019), https://www.state.gov/tokyo-statement-on-quantum-cooperation/
24. H.R.4350 - National Defense Authorization Act for Fiscal Year 2022 // https://www.congress.gov/bill/117th-congress/house-bill/4350
25. U. S. Government Accountability Office, "High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges," March 2021, https://www.gao.gov/products/ gao-21-288
26. NSA Issues FAQs on Quantum Computing and Post-Quantum Cryptography 2021-09-03 07:09 //https://www.itsecuritynews.info/nsa-issues-faqs-on-quantum-computing-and-post-quantum-cryptography/
27. Biden signs memo to boost US national security systems' defenses https://www.bleepingcomputer.com/news/security/biden-signs-memo-to-boost-us-national-security-systems-defenses/
28. Executive Order on Improving the Nation's Cybersecurity MAY 12, 2021 // https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
29. Preparing for post-quantum cryptography // https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf
30. Duncan Riley White House memo aimed at maintaining quantum computing leadership, mitigating risks // https://siliconangle.com/2022/05/05/white-house-memo-aimed-maintaining-quantum-computing-leadership-mitigating-risks/
31. Alagic G. Russell A. Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts, 2016, // https://www.researchgate.net/publication/315861652_Quantum-Secure_Symmetric-Key_Cryptography_Based_on_Hidden_Shifts
32. Zharova, A. K. Technical and Legal Principles of Information Security on the Example of Russia / A. K. Zharova, V. M. Elin // Proceedings of the 2021 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", T and QM and IS 2021, Yaroslavl, 06–10 сентября 2021 года. Yaroslavl, 2021. P. 131-135. DOI 10.1109/ITQMIS53292.2021.9642899. EDN SUSMYS.
33. Anna, Z. State regulation of the IoT in the Russian Federation: Fundamentals and challenges / Z. Anna, E. Vladimir // International Journal of Electrical and Computer Engineering. – 2021. – Vol. 11. – No 5. – P. 4542-4549. – DOI 10.11591/ijece.v11i5.pp4542-4549. EDN TLEEFT.

REVIEW OF REGULATORY REQUIREMENTS THAT ENSURE US NATIONAL SECURITY IN THE FIELD OF QUANTUM TECHNOLOGIES

Zharova, Anna Konstantinovna

Doctor of law, associate professor
Institute of State and Law of the Russian Academy of Sciences, senior researcher
Moscow, Russian Federation
Anna_jarova@mail.ru

Abstract

There is a shortage of Russian legal research in the application of quantum technologies. On the one hand, this is understandable, since the implementation of quantum technologies in society has not yet begun. On the other hand, questions about the risks and threats that the use of quantum technologies can bring are already being discussed abroad.

Keywords

quantum technologies; risks; threats; standardization; USA; national security

References

1. Manin Yu.I. Vychislimoe i nevychislimoe. - M. : Sov. radio. 1980. 128 s., il., (Kibernetika). C. 13-15.
2. The Father of Quantum Computing // https://www.wired.com/2007/02/the-father-of-quantum-computing/
3. Dowling J. and Milburn G., "Quantum Technology, the Second Quantum Revolution," Phil. Trans. R. Soc. Lond. A (2003).
4. Jaeger L. The Second Quantum Revolution in book Entanglement to Quantum Computing and Other Super-Technologies, 2018 // Terekhovich V.E. Revolyucionnye transformacii v kvantovoj fizike i innovacii v kvantovyh tekhnologiyah // https://cyberleninka.ru/article/n/revolyutsionnye-transformatsii-v-kvantovoy-fizike-i-innovatsii-v-kvantovyh-tehnologiyah DOI: 10.13140/RG.2.2.22297.88161
5. Dorozhnaya karta razvitiya «skvoznoj» cifrovoj tekhnologii «Kvantovye tekhnologii» (dokument opublikovan ne byl) // SPS "Konsul'tantPlyus"
6. Terekhovich V.E. Revolyutsionnyye transformatsii v kvantovoy fizike i innovatsii v kvantovykh tekhnologiyakh // https://cyberleninka.ru/article/n/revolyutsionnye-transformatsii-v-kvantovoy-fizike-i-innovatsii-v-kvantovyh-tehnologiyah DOI: 10.13140/RG.2.2.22297.88161
7. Klon K. Quantum Science and National Security: A Primer for Policymakers // https://www.heritage.org/technology/report/quantum-science-and-national-security-primer-policymakers
8. Elsa B. Kania & John K. Costello QUANTUM HEGEMONY? China's Ambitions and the Challenge to U.S. Innovation Leadership https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf?mtime=20180912133406%20(дата%20обращения:%2025%20января%202019%20года
9. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems // https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
10. Lee M. Quantum Computing and Cybersecurity // https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity#footnote-039
11. University of Science and Technology of China, "The World's First Integrated Quantum Communication Network," January 6, 2021, https://phys.org/news/2021-01-world-quantum-network.html.

12. Pires F. U.S. National Security Agency Issues Update on Quantum-Resistant Encryption. September 02, 2021 // https://www.tomshardware.com/news/us-national-security-agency-issues-update-on-crypto-resistant-encryption
13. Future Series: Cybersecurity, emerging technology and systemic risk// https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk/
14. Li-Zhen Gao, Xin Zhang, Song Lin, Ning Wang, Gong-De Guo Authenticated Multiparty Quantum Key Agreement for Optical-Ring Quantum Communication Networks // https://www.frontiersin.org/articles/10.3389/fphy.2022.962781/full
15. Ryan N. US Gov Issues Security Memo on Quantum Computing Risks // https://www.securityweek.com/us-gov-issues-security-memo-quantum-computing-risks
16. Pis'mo Mincifry Rossii ot 13.10.2021 № P25-18390-OG "O rassmotrenii obrashcheniya" (vmeste s "Pasportom federal'nogo proekta "Informacionnaya bezopasnost'") (dokument opublikovan ne byl) // SPS "Konsul'tantPlyus".
17. Surapol R., Wanchai P. Analysis of Security of Quantum Key Distribution Based on Entangled Photon Pairs by Model Checking // Journal of Quantum Information Science. Vol.5 No.3, September 2015. DOI: 10.4236/jqis.2015.53012
18. Buchholz S., Mariani J, Routh A. The realist's guide to quantum technology and national security What nontechnical government leaders can do today to be ready for tomorrow's quantum world // https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html
19. Prognoz nauchno-tekhnologicheskogo razvitiya Rossijskoj Federacii na period do 2030 goda (utv. Pravitel'stvom RF) (dokument opublikovan ne byl)// SPS "Konsul'tantPlyus"/
20. Pasport nacional'nogo proekta "Nacional'naya programma "Cifrovaya ekonomika Rossijskoj Federacii"" (dokument opublikovan ne byl)// SPS "Konsul'tantPlyus".
21. Kop M. Establishing a Legal-Ethical Framework for Quantum Technology Yale Law School. Yale Journal of Law & Technology (YJoLT), The Record, March 30 2021 Available from: https://www.researchgate.net/publication/350524217_Establishing_a_Legal-Ethical_Framework_for_Quantum_Technology [дата обращения: 30.09.2022].
22. H.R.6227 – National Quantum Initiative Act https://www.congress.gov/bill/115th-congress/house-bill/6227/text#HDEB502BED9CC4603A0E5F21C179960E7
23. Tokyo Statement on Quantum Cooperation (U.S. Department of State, December 19, 2019), https://www.state.gov/tokyo-statement-on-quantum-cooperation/
24. H.R.4350 - National Defense Authorization Act for Fiscal Year 2022 // https://www.congress.gov/bill/117th-congress/house-bill/4350
25. U. S. Government Accountability Office, "High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges," March 2021, https://www.gao.gov/products/ gao-21-288
26. NSA Issues FAQs on Quantum Computing and Post-Quantum Cryptography 2021-09-03 07:09 //https://www.itsecuritynews.info/nsa-issues-faqs-on-quantum-computing-and-post-quantum-cryptography/
27. Biden signs memo to boost US national security systems' defenses https://www.bleepingcomputer.com/news/security/biden-signs-memo-to-boost-us-national-security-systems-defenses/
28. Executive Order on Improving the Nation's Cybersecurity MAY 12, 2021 // https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
29. Preparing for post-quantum cryptography // https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf
30. Duncan Riley White House memo aimed at maintaining quantum computing leadership, mitigating risks // https://siliconangle.com/2022/05/05/white-house-memo-aimed-maintaining-quantum-computing-leadership-mitigating-risks/
31. Alagic G. Russell A. Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts, 2016, // https://www.researchgate.net/publication/315861652_Quantum-Secure_Symmetric-Key_Cryptography_Based_on_Hidden_Shifts

32. Zharova, A. K. Technical and Legal Principles of Information Security on the Example of Russia / A. K. Zharova, V. M. Elin // Proceedings of the 2021 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", T and QM and IS 2021, Yaroslavl, 06–10 сентября 2021 года. Yaroslavl, 2021. P. 131-135. DOI 10.1109/ITQMIS53292.2021.9642899. EDN SUSMYS.
33. Anna, Z. State regulation of the IoT in the Russian Federation: Fundamentals and challenges / Z. Anna, E. Vladimir // International Journal of Electrical and Computer Engineering. 2021. Vol. 11. No 5. P. 4542-4549. DOI 10.11591/ijece.v11i5.pp4542-4549. EDN TLEEFT.