DOI 10.37882/2223–2966.2023.01–2.03

СОВРЕМЕННЫЕ КВАНТОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

MODERN QUANTUM INFORMATION SECURITY TECHNOLOGIES

Wang Yi

Summary. Innovative projects that are being developed today, which are based on quantum technologies, open up new opportunities to make communication impossible to intercept and hack. In view of the above, this article considers modern quantum technologies for information protection. Special attention is paid to quantum key distribution, quantum direct secure network and quantum secret partitioning.

Keywords: protection, leakage, data quantum technology, network.

Ван И
Российский университет дружбы народов
lionpuls@outlook.com

Аннотация. Разрабатываемые на сегодняшний день инновационные проекты, которые основаны на квантовых технологиях, открывают новые возможности для того, чтобы сделать информационные сети невозможным для перехвата и взлома. С учетом вышеизложенного в статье рассмотрены современные квантовые технологии защиты информации. Отдельное внимание уделено квантовому распределению ключей, квантовой прямой безопасной сети и квантовому разделению секрета.

Ключевые слова: защита, утечка, данные, квантовые технологии, сеть.

На сегодняшний день первоочередным фактором, влияющим на составляющие национальной безопасности, является степень защищенности информационной среды. Вопросы информационной безопасности приобретают актуальность как в процессе стремительного развития компьютерных технологий, так и в контексте резкого увеличения преступлений и других противоправных действий, направленных на нарушение конфиденциальности, целостности и достоверности информации.

Кибератаки заняли пятое место в рейтинге рисков 2021 года и стали новой нормой в государственном и частном секторах. Прогнозируется, что в ближайшие годы эта рискованная отрасль продолжит расти, поскольку ожидается, что к 2025 году число кибератак только в сфере IoT удвоится. Кроме того, в отчете Всемирного экономического форума о глобальных рисках за 2021 год говорится, что процент обнаружения (или судебного преследования) несанкционированных атак на информационные ресурсы составляет всего 0,05%. В результате пандемии COVID-19 киберпреступность, которая включает в себя все — от кражи или растраты до взлома и уничтожения данных, выросла на 600% [1]. Общее количество заражений вредоносными программами за последние десять лет увеличилось в 70 раз (см. рис. 1).

Растущая зависимость от технологий для основных бизнес-процессов делает конфиденциальность, целостность и доступность информации критически важными условиями бесперебойной работы и требует эффективного планирования информационной безопасности с учетом рисков. Практически каждая отрасль в таких условиях вынуждена принять новые решения относительно использования более прогрессивных средств защиты данных. Информационная безопасность охватывает широкий спектр инструментов и процессов, которые организации используют для защиты информации. Сюда входят параметры политики, нацеленные на предотвращение доступа неавторизованных лиц к деловой или личной информации, средства обеспечения безопасности сети и инфраструктуры, методы тестирования и аудита.

В последние годы повышенный интерес вызывают квантовые технологии защиты информации, а именно квантовая криптография, значимое место в которой занимает квантовое распределение ключей. Подавляющее большинство теоретических и практических исследований в области квантовой криптографии посвящено разработке и совершенствованию квантовых протоколов распределения ключей.

Но в тоже время, ряд вопросов, связанных с перспективами и особенностями использования, например, квантовых алгоритмов, которые можно легко добавить к существующему оборудованию, и которые уже находятся на завершающей стадии стандартизации, остается открытым. Также особого внимания заслуживают квантовая стеганография, которая может использоваться для обнаружения перехватчиков. Недостаточно изученной остается природа квантовых состояний, имеющих значительный потенциал для предотвращения подделки данных.

С учетом вышеизложенного, актуальность и значимость исследования данной предметной области

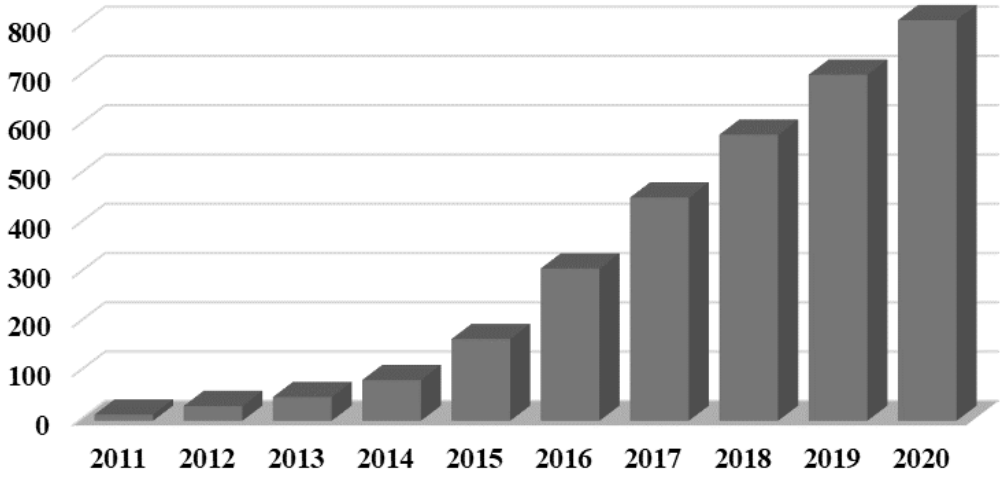

Рис. 1. Общее количество заражений вредоносными программами за последние десять лет, млн. [2]

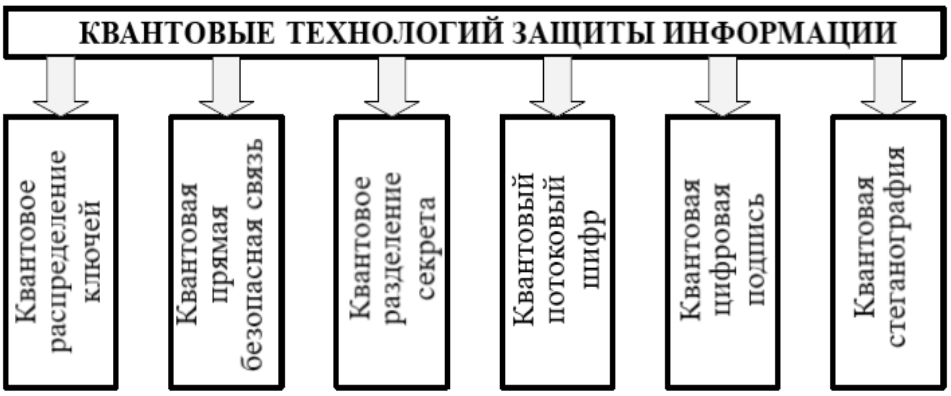

Рис. 2. Квантовые технологии защиты информации

не вызывает сомнений, что и обуславливает выбор темы данной статьи.

Вопросы, связанные с комплексными системами защиты информационных систем, которые включают в себя защиту объектов информационной системы, каналов связи, процессов, программ и процедур обработки информации, управление системой защиты прорабатываются такими авторами как: Жидко Е.А., Козлов В.А., Фефелов С.В., Popp, Robert; Poindexter, John; Oerke, E.-C.; Gerhards, R.

Над принципами информационной безопасности и методами защиты данных работают Касаткина Т.И., Россихина Л.В., Дубровин А.С., Кузьменко Р.В., Lioy, A.; Ramunno, G.; Vernizzi, D.; Corchado, E.

Систематизации и классификации современных квантовых технологий защиты информации посвящены труды Федосова Д.П., Дементьева Ю.Ю., Завтоновой А.В., Сибиряковой А.И., Longhi, Stefano; Giorgi, Luca; Z., Roberta.

Положительно оценивая имеющиеся на сегодняшний день достижения в области обеспечения безопасности данных, следует отметить, что квантовые технологии защиты информации находятся только на первоначальном этапе своего развития, поэтому еще много вопросов в данном направлении остается нераскрытых. Так, задачи расширении квантовых сетей и разработки квантовых повторителей требуют особого внимания. В более детальном исследовании нуждаются технологии квантовой коррекции ошибок и квантового смягчения ошибок, которые являются двумя важными методами защиты данных.

Таким образом, цель статьи заключается в изучении возможностей и перспектив современных квантовых технологии для защиты информации.

Рис. 3. Протоколы квантовой прямой безопасной связи

Квантовые информационные технологии, такие как квантовые компьютеры, криптография, радары, часы и другие системы, основываются на свойствах квантовой механики, описывающей поведение материи на субатомном уровне. Эта чрезвычайно сложная наука часто противоречит повседневным представлениям о том, как устроен мир, однако именно эти, противоречащие здравому смыслу особенности квантовой механики, позволяют различным технологиям получить их уникальные сильные и слабые стороны [3].

Опираясь на квантовую механику, в настоящее время разработаны различные квантовые технологии защиты информации, состав которых представлен на рис. 2.

Рассмотрим некоторые из представленных на рис. 2 технологий более подробно.

Квантовое распределение ключей

Квантовое распределение ключей (QKD) — это механизм согласования ключей шифрования между удаленными сторонами, основанный на свойствах квантовой механики, чтобы гарантировать, что ключ не был замечен или изменен при передаче. Поскольку традиционные алгоритмы криптографии с открытым ключом могут быть уязвимы для будущего крупномасштабного квантового компьютера, требуются новые подходы, которые не разделяют эту уязвимость. QKD претендует на потенциальное смягчение последствий, поскольку его свойства безопасности основаны на законах физики, а не на сложности некоторых математических задач.

Благодаря квантовому распределению ключей зашифрованное сообщение отправляется по традиционным сетям, а ключи для расшифровки информации передаются с помощью квантовых средств. Таким образом, только предполагаемый получатель может расшифровать сообщение, что делает невозможным любое подслушивание. Благодаря применению этого метода в рамках проекта Программы НАТО «Наука ради мира и безопасности» (SPS) впервые удалось соединить Италию и Мальту прототипом QKD-канала с помощью подводных оптоволоконных кабелей [4].

Протоколы QKD обеспечивают механизм шифрования для двух удаленных сторон. Благодаря ему можно согласовать общий секретный ключ, который не может быть замечен или подделан противником без предупреждения исходных сторон. Однако, поскольку протоколы QKD не обеспечивают аутентификацию, они уязвимы для физических атак типа «человек посередине», при которых противник может согласовать индивидуальные общие секретные ключи с двумя сторонами, считающими, что они общаются друг с другом.

По этой причине протоколы QKD должны быть развернуты вместе с криптографическими механизмами, обеспечивающими аутентификацию. Эти криптографические механизмы также должны быть защищены от квантовой угрозы.

Квантовая прямая безопасная сеть

Квантовая безопасная прямая связь (QSDC) привлекает большое внимание, поскольку она может передавать секретные сообщения напрямую, без совместного использования ключа.

QSDC отправляет секретную информацию непосредственно по защищенному квантовому каналу. Она не требует распределения и хранения ключей. В результате любой атаки на QSDC получается только случайное число, и из него нельзя извлечь никакой полезной информации. Протоколы QSDC могут быть разделены на четыре типа (рис. 3).

С точки зрения пользователя, конфиденциальное сообщение просто входит в защищенный QSDC частный канал и конфиденциально передается получателю. Весь процесс защиты информации выполняется протоколом. Более того, обеспечиваемая безопасность не зависит от ресурсов подслушивающего устройства,

поскольку основана на законах физики [5]. Безусловно безопасный QSDC является более сильным криптографическим примитивом, чем все формы QKD, поскольку он может быть использован для безопасной доставки как случайных ключей, так и чувствительных детерминированных сообщений.

В последнее время экспериментальные QSDC получили значительное развитие. Протоколы QSDC, основанные на запутанности, были реализованы в волоконно-оптической системе передачи данных длиной 0,5 км., также QSDC были протестированы в практическом эксперименте с использованием квантовой памяти. QSDC на основе одиночных фотонов были прошли испытания и в результате удалось получить их практический рабочий прототип. Также в 2022 году была продемонстрирована осуществимость QSDC с геосинхронного спутника на земной орбите на землю. Однако невозможность одновременно различать четыре набора закодированных ортогональных запутанных состояний в протоколах QSDC ограничивает их практическое применение.

Квантовое разделение секрета

Квантовое разделение секрета (QSS) — это процедура разделения сообщения на несколько частей таким образом, что ни одно из подмножеств частей не является достаточным для прочтения сообщения, но все множество является достаточным.

Подавляющая часть квантовых протоколов разделения секрета использует свойства перепутанных квантовых состояний [6]. Первый QSS был предложен Hillery, Buzek и Berthiaume в 1998 году, который аналогично некоторым протоколам квантовой безопасной связи использует ГХЦ-триплеты (четверки) кубитов. Этот протокол позволяет отправителю разделить свое сообщение между двумя (тремя) абонентами таким образом, что они смогут прочитать его, только действуя совместно.

В 2020 году исследователи из Южной Африки разработали и продемонстрировали схему QSS, которая позволяет 10 сторонам безопасно обмениваться информацией — самое большое число на сегодняшний день. Протокол предполагает, что каждая сторона выполняет квантовые операции с фотоном без измерения его состояния, ученые утверждают, что это может помочь увеличить как скорость обмена данными в безопасных квантовых сетях, так и количество сторон, которые могут участвовать в обмене.

Несмотря на наличие коммерческих систем QKD, протокол имеет свои недостатки. Один из них заключается в том, что поляризация фотонов имеет только два ортогональных состояния. Они традиционно используются для обозначения 1 и 0, как в обычном битовом потоке. Поэтому в новом исследовании Эндрю Форбс и его коллеги из Университета Витватерсранда в Йоханнесбурге закодировали данные не в поляризации фотона, а в его орбитальном угловом моменте, который в принципе может быть бесконечно большим.

Квантовый потоковый шифр

Этот тип шифра предусматривает шифрование данных подобно классическим потоковым шифрам, но с применением квантового шумового эффекта и может использоваться в оптических коммуникационных сетях [7]. Ожидается, что квантовый поточный шифр ускорит передовые приложения в будущих системах связи. Причина этого в том, что эта схема может использовать обычные устройства оптической связи и совместима с существующими системами связи. В его конструкции эффективно интегрированы оптическая связь, квантовая теория и криптография. Поэтому в исследованиях реализации квантовый поточный шифр также называют «квантовой криптографией оптической связи Y-00».

Таким образом, возможность новых высокоскоростных вычислений с использованием квантовой обработки информации для оптимизации и повышения эффективности систем защиты данных привлекает значительное внимание ученых и экспертов. В статье рассмотрены существующие на сегодняшний день современные квантовые технологии защиты информации. Детальное внимание уделено квантовому распределению ключей, квантовой прямой безопасной сети и квантовому разделению секрета.

ЛИТЕРАТУРА

1. Information security, cybersecurity and privacy protection. Biometric information protection. London: British Standards Institution, 2022, 74 p.
2. Data protection, migration and border control: the GDPR, the Law Enforcement Directive and beyond / Teresa Quintel. Oxford: Hart Publishing, 2022. 165 p.
3. Xue, Yun-Jia; Wang, Hao-Wen Quantum Information Protection Scheme Based on Reinforcement Learning for Periodic Surface Codes // Quantum engineering. 2022. Volume 20; pp 78–84.
4. Федоров А.К. Квантовые технологии: от научных открытий к новым приложениям, дополнение // Фотоника. 2019. Т. 13. № 8. С. 760–763.
5. Щербаков А.Ю. Перспективы современной криптографии // Проектирование будущего. Проблемы цифровой реальности. 2020. № 1 (3). С. 227–233.

6. Qu, Zhiguo Quantum identity authentication protocol based on three-photon quantum error avoidance code in edge computing // Transactions on emerging telecommunications technologies. 2022. Volume 33: Number 6; pp 56–63.
7. EL–Latif, Ahmed A. Abd Efficient quantum-based security protocols for information sharing and data protection in 5G networks // Future generation computer systems. 2019. Volume 100; pp 893–906.

Журнал «Современная наука: актуальные проблемы теории и практики»

Российский Университет Дружбы Народов