О ПЕРВИЧНЫХ ТЕХНИЧЕСКИХ УСТРОЙСТВАХ И ТРЕБОВАНИЯХ К КЛЮЧАМ БЕЗОПАСНОСТИ КВАНТОВЫХ СИСТЕМ

Аверьянов В.С.[1], Карцан И.Н.[2]

Цель исследования: *разработка новых методов, алгоритмов и моделей для выявления несанкционированных действий злоумышленника/ов в отношении к транслируемым данным, представленным в виде однофотонных чистых состояний световых частиц, что позволит усилить секретность основных ключей безопасности, усовершенствовать процедуры обмена и обработки данных легитимными пользователями телекоммуникационной системы, расширить функциональные возможности существующих технологических решений в их классическом представлении.*

Метод исследования: *системный анализ, метод оценки информационной защищённости*

Результат исследования: *представлены риски возникновения критичных системных ошибок для процедур согласования результатов измерений базисных состояний и предполагаемые потенциальные возможности злоумышленника по реализации уязвимостей через активную фазу атак с явным критическим исходом. Установлено, что трансляция смешанных однофотонных состояний и навязывание приемной аппаратуре явно бесконтрольно, безотчётно и не содержится ни в одном алгоритме квантовых протоколов, что по мнению авторов является наиболее критичной уязвимостью современных криптографических систем, построенных на базе квантовой механики. Предложен способ решения проблем «бесшумного» сканирования и противодействия скрытым активным атакам на квантовый канал и состояния частиц. Суть решения заключается в неортогональности состояний случайного базисного вектора и дублировании основного канала связи, содержащего информационный тракт по транслированию импульсных сигналов, где известное число синхропосылок в резервной линии позволяет отследить атакующего субъекта. Основополагающим является знание о первичных-естественных ошибках, возникающих на каждом из этапов формирования основного ключа безопасности.*

Научная новизна *заключается в новых методах выработки общего ключа безопасности, предназначенного для конфиденциального обмена данными между легитимными пользователями системы по протоколу BB84 (4+2). Разработанный метод содержит основные параметры и требования, предъявляемые к обеспечению информационной безопасности квантовых телекоммуникационных систем, в частности, к секретности транслируемой ключевой последовательности.*

Ключевые слова: *системные ошибки, протокол BB84 (4+2), однофотонные системы, оптические устройства, телекоммуникационные системы, злоумышленник, протокол передачи данных.*

DOI:10.21681/2311-3456-2023-2-65-72

Введение

Квантовые коммуникации – новая высокотехнологичная отрасль, формирующаяся на стыке нескольких технологий: фотоники и квантовых технологий. По данным Cybersecurity and Infrastructure Security Agency (CISA) [1], вторая квантовая революция, появление квантовых компьютеров способны нанести непоправимый ущерб любым криптографическим системам с открытым ключом шифрования, алгоритмы которых

1 Аверьянов Виталий Сергеевич, младший научный сотрудник кафедры «Безопасность информационных технологий» ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», Красноярск, Россия. E-mail: averyanov124@mail.ru, ORCID 0000-0001-6069-2537

2 Карцан Игорь Николаевич, доктор технических наук, доцент, профессор кафедры «Информационной безопасности» ФГБОУ ВО Севастопольского государственного университета, Севастополь, профессор кафедры «Безопасность информационных технологий» ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», Красноярск, Россия. E-mail: kartsan2003@mail.ru, ORCID 0000-0003-1833-4036

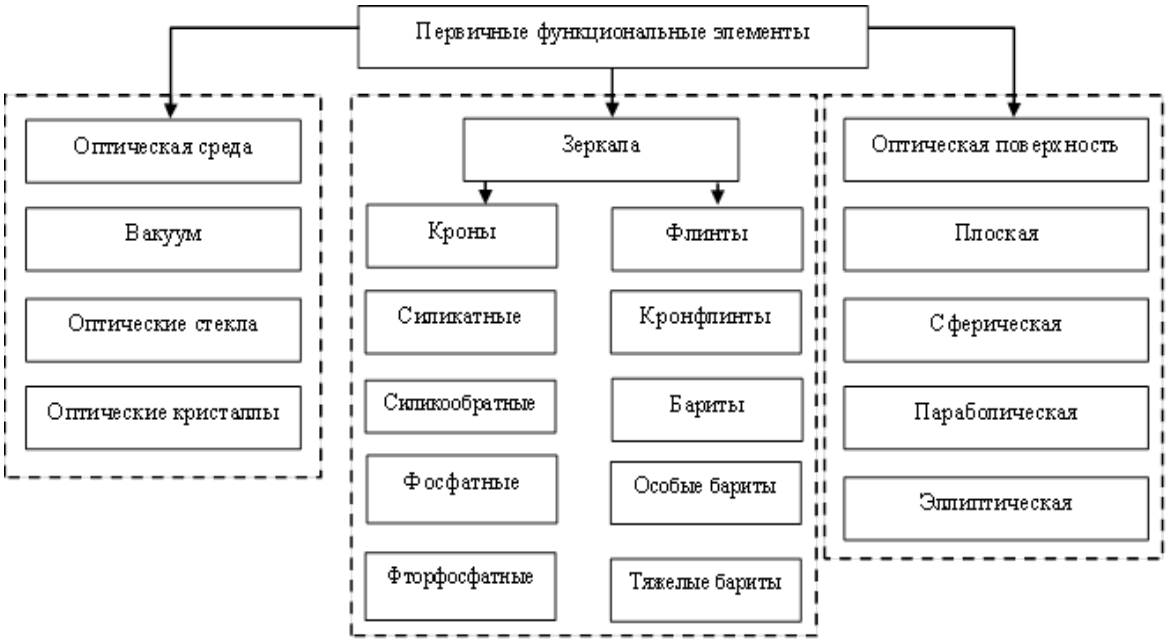


Рис. 1. Первичные элементы квантово-оптических систем

предусматривают процедуры передачи данных по незащищённому, доступному для стороннего наблюдателя каналу связи. Системы с открытым ключом шифрования сегодня распространены в различных сетевых протоколах, например: Transport Layer Security (TLS), предшественник Secure Sockets Layer (SSL), Hypertext Transfer Protocol Secure (HTTPS), Secure Shell Protocol (SSH), программное обеспечение (ПО) Pretty Good Privacy (PGP), стандарт Secure / Multipurpose Internet Mail Extensions (S/MIME) [2] обеспечивающий криптографическую безопасность электронной почты. Данные обстоятельства являются серьезной угрозой для государственных и частных организаций, которые уже в ближайшее время должны подготовиться к предстоящим вызовам в области квантовой криптографии и вычислений. Стоит отметить, что большинство современных цифровых телекоммуникаций, включая новый вид финансового инструмента в виде криптовалюты, используют тот же вид криптозащиты в виде открытой передачи ключа безопасности.

Высокоскоростное оборудование квантового распределения ключей безопасности (КРК) использует метод передачи зашифрованной последовательности [3] в виде световых частиц - фотонов, основанный на принципах квантовой физики, оптики и механики и позволяет транслировать секретный ключ на расстояние до 120 км без повторителей сигнала в заданный период времени. Оборудование КРК может устанавливаться как отдельной системой, так и поверх существующей классической инфраструктуры и, что немало важно, совместимо с предустановленными средствами криптографической защиты информации на открытых ключах [4]. Далее будут рассмотрены основные компоненты в составе таких систем.

1. Первичные квантово-оптические устройства

Квантово-оптическая система представляет собой совокупность оптических однородных сред, разделенных между собой лучепреломляющими поверхностями с преградами для поперечного сечения световых пучков в виде диафрагм. Комплекс первичных оптических элементов позволяет перераспределять в гильбертово-проективном пространстве электромагнитное поле, за счет трансформации реликтовых частиц. Состав элементов квантово-оптических систем представлен на (рис. 1).

Квантово-оптические устройства способны работать в видимом излучении при длине волны от 380-900 нм, в оптических волокнах при длине волны от 900-1700 нм, а также высокоэффективных, широкополосных, пикосекундных сверхпроводящих лазерах при длине волны от 780-1625 нм. Стоит отметить, что на работу устройств существенное влияние оказывают дисперсионные показатели оптической среды [5]:

$$n^2 = 1 + \sum_i^{\infty} \frac{e_i^2 / m}{\omega_a^2 - \omega^2} \qquad (1)$$

Выражение (1) представляет собой формулу Зельмейера [54], где n – показатель преломления, а ω_a – резонансная частота. В системах с квантовым распределением ключей безопасности (КРК) [6] в качестве первичных оптических элементов применяют плоские и сферические поверхности, с допустимыми отклонениями длины волны в пределах $0{,}12 \le \lambda \le 0{,}025$ нм.

2. Оптический светоделитель

Светоделитель представляет собой базовую модель технического устройства [7] квантовых телекоммуникационных систем связи по технологии КРК. Пассивный оптический элемент может быть представлен в двух физических исполнениях: произвольно изолированном кубе или плоскости с диэлектриком внутри. В квантовых экспериментах, требующих высокой точности настройки интерес представляет светоделитель кубической формы. К его отличительным особенностям относится: максимальная эффективность для любого типа поляризации и угла падения луча, техническая конвергенция под любой комплекс оптического оборудования, простота установки и оптической настройки. К недостаткам: высокая стоимость, большой вес, оптические потери порядка 10%, увеличенное время отклика, в отличии от плоского типа, высокий уровень хроматической дисперсии. Принцип работы кубического светоделителя изображен на (рис. 2). Механизм его работы прост и надежен: падающий на стекло или пластинку луч делится надвое, образовавшиеся лучи интерферируют между собой, позволяя фотодетектору на стороне измерений фиксировать данные [8].

В представлении об идеальных системах, существующих вне времени и пространства светоделитель обратим [9], условие позволяет воссоздать исходный луч через усиление электромагнитного поля волнового пакета, до полного совпадения фаз интерферирующих между собой волн.

При деструктивной интерференции, фазы двух падающих лучей не совпадают, волны ослабляют друг друга, а их взаимная интерференция позволяет рассматривать систему как четырехполюсник с парами входных и выходных мод. В классическом представлении деструктивная интерференция двух когерентных лучей обеспечивает наложение амплитуд волн $X1$ и $X2$, а их линейное преобразование выглядит как:

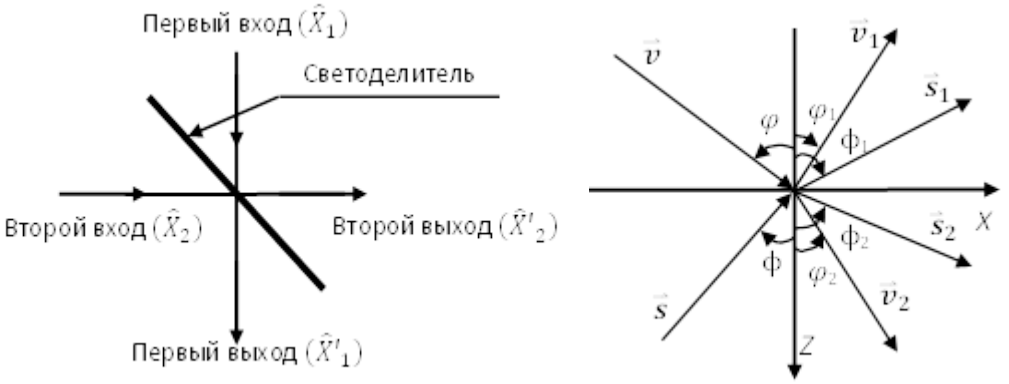
$$\begin{pmatrix} X'_1 \\ X'_2 \end{pmatrix} = S \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} \quad (2)$$

Для квантовых систем помимо собственных амплитуд волн необходимо рассматривать и световые поля. Для выражения (2) линейные состояния в квантовой оптике согласно классическому представлению светового поля, в котором волновой пакет нулевого состояния системы смещен от широкополосного лазерного источника, а излученные волны не расплываются в процессе трансформации [10] системы может быть выражен через статистический параметр Манделя $\xi \ge 0$ [11]. При этом когерентные состояния рассматриваются как собственные состояния оператора уничтожения n:

$$\hat{n}|n\rangle = n|n\rangle \quad (3)$$

В таком случае деструктивная интерференция для квантовых состояний в световом поле соответствует операторам $\hat{X}_1$ и $\hat{X}_2$ и может быть представлена как:

$$\begin{pmatrix} \hat{X}'_1 \\ \hat{X}'_2 \end{pmatrix} = S \begin{pmatrix} \hat{X}_1 \\ \hat{X}_2 \end{pmatrix} \quad (4)$$



(а) (б)

Рис. 2. Схема пассивного кубического светоделителя (а), расщепление светового потока падающих лучей, угол 450 (б)

Выражение (4) указывает на схожесть классических и квантовых представлений интерференции, а её оптические эффекты задействованы в большинстве пассивных оптических устройств без потерь для систем связи с КРК. К ним относятся: интерферометры, полупрозрачные зеркала, волноводы, поляризаторы и другие устройства фотоники [12].

3. Фотоприемное устройство для регистрации одиночных фотонов

Современные методы фиксации фотонов являются одним из важных моментов в процедурах оптических измерений квантовых состояний элементарных частиц. При этом число «щелчков» фотодетектора соответствует его оптической мощности и определено как:

$$N\left|\lambda = 5,03\times10^{15}\lambda P\right. \quad (5)$$

В выражении (5): P – оптическая мощность фотодетектора, λ – длина волны. Стоит отметить, что для конкретных условий (наземное или атмосферное размещение) требования к устройству различны, но обладают одной общей чертой – необходимостью высокоэффективного счета одиночных фотонов с низким уровнем фиксации темновых шумов приемо-передающей аппаратуры и возникающих флуктуаций в канале связи. Далее рассмотрим несколько технологических решений, выполненных на основе фотодиодов с различными характеристиками, пригодных для счета фотонов в системах с КРК.

1. *На основе лавинных фотодиодов (SPAD-диоды).* Лавинные фотодиоды (APD) представляют собой фотодиоды с высокой чувствительностью и минимальным временем отклика порядка *50* нс. В отличие от обычных диодов с p-i-n структурой, лавинные фотодиоды используют внутреннее усиление для создания лавины электронно-дырочных пар под действием ударной ионизации. Высокое напряжение смещения расширяет область поглощения лавинного фотодиода, что обеспечивает появление достаточного количества электронов/дырок при ионизации и позволяет достигать скорости фиксации одиночных фотонов ≥ 10 МГц. Сам процесс регистрации подразумевает переход излученных микрочастиц из зоны валентности в зону проводимости, т.е. до момента поглощения чистого состояния фотона. К преимуществам устройств можно отнести минимальное количество ложных срабатываний при детектировании однофотонных импульсных информационных посылок, высокую квантовую эффективность, которая в свою очередь связана с чувствительностью фотоприёмного устройства следующим выражением:

$$QE = \left(R_0 \times 1240\right) \Big/ \lambda \times 100\% \quad (6)$$

В выражении (6) R_0 – чувствительность фотодетектора, λ – длина волны. К недостаткам устройства относится невозможность регистрации частиц в системах из двух попарно некоррелированных во времени импульсных сигналов, когда вероятность обнаружения каждого стремится к нулю.

2. *На основе фотодиодов с линейными характеристиками*. Фоточувствительный элемент детектора выполнен в виде p-i-n структуры, где p – область с положительным дотированием, n – отрицательна, i – внутренняя имеет удельное сопротивление в 106-107 раз больше, чем сопротивление легированных областей n - и p - типов. К переходу можно прикладывать большие обратные напряжения, и однородное электрическое поле устанавливается по всей i - области. Падающее световое излучение поглощается i - областью, имеющей сильное электрическое поле, что позволяет детектировать волновые пакеты от 1 до 1,1 мкм. Класс устройств идеален для работы в интенсивных комбинационных рассеяниях фотонных квазиимпульсов. Недостатки: низкая квантовая эффективность при детектировании частиц в тепловом состоянии ввиду собственных темновых шумов и внешних флуктуаций канала связи на длительных маршрутах.

Далее проанализированы основные протоколы передачи данных, на предмет их неустойчивости по отношению к классу активных атак с явно определенными состояниями, где динамические переменные представлены операторами гильбертово-проективного пространства и энергетическими полями релятивистских частиц.

4. Однофотонные системы, протокол BB84 (4+2)

Впервые, квантовый протокол BB84(4+2) детально представлен в работе “Quantum Cryptography with Coherent States” Б. Хаттнера, Н. Иммото, Н. Гисина и Т. Мора в 1995 году. По своему алгоритмическому типу кодирования основных ключей безопасности [13] он является неким средним представлением между B92 и классическим квантовым BB84 [14-17]. Аналогично предыдущим версиям защищенного обмена данными между легитимными пользователями «4+2» оперирует все теми же четырьмя состояниями в двух базисах [18], для логических «0» и «1». К существенному отличию относится факт неортогональности состояний случайного базисного вектора 0(+), 1(×),1(+), 0(×). Графическое представление изображено на (рис.3).

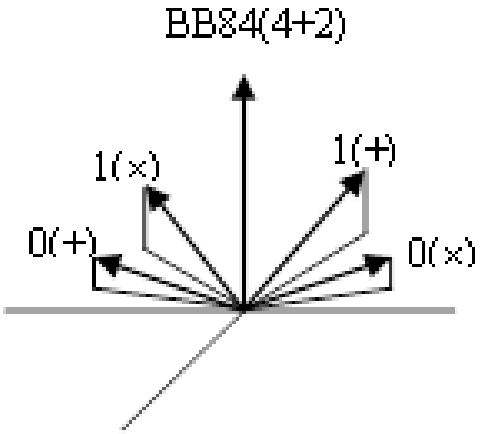


Рис. 3. Неортогональность базисных состояний по протоколу BB84(4+2)

Алгоритмическая часть. На стороне передающего устройства А в произвольной форме определяется один из двух доступных базисов. Формируются логические информационные состояния «0» или «1». По завершению этапа предварительного кодирования, пакет с информационными данными отправляется по открытому квантовому каналу связи устройству В. Инициируется процедура измерений по базисам (+) и (×). Аналогично алгоритму B92 разный тип измерений [19] представлен как произвольное разложение единичного базисного вектора состояний в гильбертово-проективном пространстве. В качестве примера рассмотрим измерения на приемной стороне в базисе (×):

$$\acute{S}_{0(\times)} + \acute{S}_{1(\times)} + \acute{S}_{n(\times)} = 1 \quad (7)$$

$$\acute{S}_{0(\times)} = \hat{H}(\times)\left(1 - 0_{(\times)}|0_{(\times)}\right) \quad (8)$$

$$\acute{S}_{1(\times)} = \hat{H}(\times)\left(1 - 1_{(\times)}|1_{(\times)}\right) \quad (9)$$

$$\acute{S}_{n(\times)} = 1 - \left(0_{(\times)}|0_{(\times)} - 1_{(\times)}|1_{(\times)}\right) \quad (10)$$

$$H(\times) = \frac{1}{1 + cos\xi(\times)} \quad (11)$$

$$cos\xi(\times) = 0_{(\times)}|1 - (0_{(\times)}|0_{(\times)} - 1_{(\times)}|1_{(\times)}|0_{(\times)} = \\ = 1_{(\times)}|1 - (0_{(\times)}|0_{(\times)} - 1_{(\times)}|1_{(\times)}|1_{(\times)} \quad (12)$$

Измерения по базису (+) аналогичны (×):

$$\acute{S}_{0(+)} + \acute{S}_{1(+)} + \acute{S}_{n(+)} = 1 \quad (13)$$

$$\acute{S}_{0(+)} = \hat{H}(+)\left(1 - 0_{(+)}|0_{(+)}\right) \quad (14)$$

$$\acute{S}_{1(+)} = \hat{H}(+)\left(1 - 1_{(+)}|1_{(+)}\right) \quad (15)$$

$$\acute{S}_{n(+)} = 1 - \left(0_{(+)}|0_{(+)} - 1_{(+)}|1_{(+)}\right) \quad (16)$$

$$\hat{H}(+) = \frac{1}{1 + cos\xi(+)} \quad (17)$$

$$cos\xi(+) = 0_{(+)}|1 - (0_{(+)}|0_{(+)} - 1_{(+)}|1_{(+)}|0_{(+)} = \\ = 1_{(+)}|1 - (0_{(+)}|0_{(+)} - 1_{(+)}|1_{(+)}|1_{(+)} \quad (18)$$

Работа алгоритма после измерений кодированных однофотонных состояний аналогична классическому протоколу BB84, исключение составляет этап согласования. Здесь номера не отбракованных измерений с неопределенными исходами [20] $\acute{S}_{n(\times)(+)}$ являются общедоступной информацией. В последующем неопределенность $\acute{S}_{n(\times)(+)}$ следует рассматривать как измерения с предельно допустимым уровнем ошибок M_c, т.е. превышающем пороговое значение в 11% при котором данные считаются скомпрометированными. По причине общедоступности и критерия ошибочности пакеты отбраковываются. Из оставшегося числа формируется основной ключ безопасности. Одним из преимуществ протокола BB84(4+2) является высокий уровень секретности и экспериментально доказанная дальность передачи данных, превышающая 150 км, данные показатели достижимы за счет неортогональности базисных состояний.

Выводы

Согласно (7-18) секретность основных ключей безопасности зависит от количества системных ошибок, процедур измерений базисных состояний и технических изъянов квантовой системы.

Определено, что к информационному направлению, оказывающему влияние на имитостойкость ключевой последовательности по отношению к внешним деструктивным воздействия относится:

1. Детектирование системных ошибок на стороне приемной аппаратуры, таких что: $2h(M_c) = 1$ при $M_c = 11\%$.

2. Формирование на стороне передающей аппаратуры конечной последовательности однофотонных импульсных посылок и соответствующего числа задетектированных состояний приемной стороны в сопряженных базисах «+» и «×».

3. Приготовление физического состояния частиц, транслируемых по волоконно-оптическим или пространственным линиям связи [21].

Недостатки технической реализации, способные привести к возникновению системных ошибок:

1. Квантовая эффективность фотодетекторов, от которой зависит число ложных срабатываний при регистрации однофотонных импульсных информационных посылок.

2. Высокий уровень темновых шумов приемо/передающей аппаратуры [22].

3. Внешние флуктуации в канале связи имеют прямую зависимость от хаотично взаимодействующих частиц с квантовомеханическими эффектами [23] в тепловом представлении состояния.

Литература

1. Krebs C. et al. Advisory memorandum on identification of essential critical infrastructure workers during Covid-19 response. – 2020.
2. Schaad J., Ramsdell B., Turner S. Secure/multipurpose internet mail extensions (S/MIME) version 4.0 message specification. – 2019. – №. rfc8551.
3. Жуков А.О., Карцан И.Н., Аверьянов В.С. Кибербезопасность Арктической зоны. Информационные и телекоммуникационные технологии. 2021. № 51. С. 9-13.
4. Аверьянов В.С., Карцан И.Н. Цифровые методы организации связи в Арктической зоне. В книге: Измерения, автоматизация и моделирование в промышленности и научных исследованиях (ИАМП-2020). Материалы XV Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых с международным участием. 2020. С. 60-61.
5. Пучков И. И. Дисперсия и затухание сигнала в оптических линиях связи //ПРОФЕССИОНАЛ ГОДА 2018. – 2018. – С. 23-26.
6. Аверьянов В.С., Карцан И.Н. Об атаке расщепления в распределении криптографических ключей безопасности. Защита информации. Инсайд. 2022. № 4 (106). С. 20-23.
7. Kolyako A.V., Pleshkov A.S., Tret'yakov D.B., Entin V.M., Ryabtsev I.I., Neizvestny I. Investigation of the long-term stability of single-photon quantum key generation in a polarization-coded circuit. Siberian Physical Journal. 2021. Vol. 16(2). pp. 81-93.
8. Левченко С.А., Роенков Д.Н. Квантово-криптографические методы защиты информации. СПбНТОРЭС: труды ежегодной НТК. 2019. № 1(74). С. 201-203.
9. Белинский А. В. О нарушении причинности в экспериментах с фотонами //Вестник Московского университета. Серия 3. Физика. Астрономия. – 2018. – №. 3. – С. 14-25.
10. Аверьянов В.С., Карцан И.Н. Безопасность ключевой последовательности по протоколу Чарльза Беннета. В сборнике: Российская наука, инновации, образование - РОСНИО-2022. сборник научных статей по материалам Всероссийской научной конференции. Красноярск, 2022. С. 72-75.
11. Ларионов Н. В. Q-распределение для одноатомного лазера, работающего в «классическом» режиме // Журнал экспериментальной и теоретической физики. – 2022. – Т. 161. – №. 2. – С. 166-176.
12. Сидоров А. И. Сенсорная фотоника //СПб.: Ун-т ИТМО. – 2019.
13. Беляев С. С. и др. Построение функции генерации криптографически стойких псевдослучайных последовательностей на базе алгоритма шифрования» Кузнечик» //Вопросы кибербезопасности. – 2021. – №. 4 (44). – С. 25-34.
14. Аксельрод В.А., Аверьянов В.С., Карцан И.Н. Протокол распределения квантовых ключей BB84. В сборнике: Российская наука, инновации, образование - РОСНИО-2022. сборник научных статей по материалам Всероссийской научной конференции. Красноярск, 2022. С. 142-147.
15. Вершинина К.В., Салтыков А.Р. Применение модифицированного протокола BB84-DS для квантового распределения ключей (QKD). В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей: в 4х томах. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021. С. 151-155.
16. Zavala M., Barán B. QKD BB84. A taxonomy. В сборнике: Proceedings - 2021 47th Latin American Computing Conference, CLEI 2021. 47. 2021. DOI: 10.1109/CLEI53233.2021.9639932.
17. Alshaer N., Nasr M.E., Ismail T. Hybrid MPPM-BB84 quantum key distribution over fso channel considering atmospheric turbulence and pointing errors. IEEE Photonics Journal. 2021. Т. 13. № 6. С. 7600109. DOI: 10.1109/JPHOT.2021.3119767.
18. Василиу Е. В. Стойкость пинг-понг протокола с триплетами Гринбергера–Хорна–Цайлингера к атаке с использованием вспомогательных квантовых систем //Информатика. – 2018. – №. 1 (21). – С. 117-128.
19. Tudorache A. G., Manta V., Caraiman S. Quantum steganography based on the B92 quantum protocol //Mathematics. – 2022. – Vol. 10. – №. 16. – С. 2870.
20. Комарова А. В., Коробейников А. Г. Анализ основных существующих пост-квантовых подходов и схем электронной подписи // Вопросы кибербезопасности. – 2019. – №. 2 (30). – С. 58-68.
21. Гулаков И. Р. и др. Обнаружение канала утечки информации из многомодового оптического волокна при помощи кремниевого фотоумножителя //Доклады БГУИР. – 2022. – Т. 20. – №. 6. – С. 37-44.
22. Коляко А. В. и др. Исследование долговременной стабильности генерации однофотонного квантового ключа в схеме с поляризационным кодированием //Сибирский физический журнал. – 2022. – Т. 16. – №. 2. – С. 81-93.
23. Торхов Н. А. Квантово-механическое состояние квантовой системы и эффект туннелирования (новый взгляд) //СВЧ-техника и телекоммуникационные технологии. – 2020. – №. 1-1. – С. 331-332.

ON PRIMARY TECHNICAL DEVICES AND REQUIREMENTS FOR QUANTUM SYSTEM SECURITY KEYS

Averyanov V.S.[3], Kartsan I.N.[4]

Purpose of the article: *development of new methods, algorithms and models to detect unauthorized actions of an intruder/s in relation to broadcast data represented in the form of one-photon pure states of light particles, which will allow: to strengthen the secrecy of basic security keys, improve procedures for data exchange and processing by legitimate users of the telecommunications system, expand the functionality of existing technological solutions in their classic representation.*

Research method: *system analysis, information security assessment method.*

The result: *risks of critical system errors for procedures of basic states measurement results matching and supposed potential possibilities of attacker to realize vulnerabilities through active phase of attacks with explicit critical outcome are presented. It is established that translation of mixed single-photon states and imposition on receiving hardware is explicitly uncontrolled, unaccountable and not contained in any algorithm of quantum protocols, which, according to the authors, is the most critical vulnerability of modern cryptographic systems based on quantum mechanics. A way to solve problems of "silent" scanning and to counteract hidden active attacks on quantum channel and particle states is proposed. The essence of the solution consists in non-orthogonality of states of a random basis vector and duplication of a main communication channel containing an information path on pulse signals broadcasting, where a known number of synchro-sentences in a backup line allows to trace an attacker. Fundamental is the knowledge of the primary-natural errors occurring at each of the stages of the formation of the main security key.*

Keywords: *system errors, BB84 protocol (4 + 2), single-photon systems, optical devices, telecommunication systems, attacker, data transfer protocol.*

References

1. Krebs C. et al. Advisory memorandum on identification of essential critical infrastructure workers during Covid-19 response. – 2020.
2. Schaad J., Ramsdell B., Turner S. Secure/multipurpose internet mail extensions (S/MIME) version 4.0 message specification. – 2019. – №. rfc8551.
3. Zhukov A.O., Kartsan I.N., Averyanov V.S. Cybersecurity of the Arctic Zone. Information and telecommunication technologies. 2021. № 51. pp. 9-13.
4. Averyanov V.S., Kartsan I.N. Digital methods of communication organization in the Arctic zone. In book: Measurement, Automation and Modelling in Industry and Scientific Research (IAMP-2020). Proceedings of the XV All-Russian scientific and technical conference of students, graduate students and young scientists with international participation. 2020. pp. 60-61.
5. Puchkov I.I. Dispersion and signal attenuation in optical communication lines//PROFESSIONAL OF THE YEAR 2018. – 2018. - S. 23-26.
6. Averyanov V.S., Kartsan I.N. On a splitting attack in distribution of cryptographic security keys. Information protection. Insider. 2022. № 4 (106). pp. 20-23.
7. Kolyako A.V., Pleshkov A.S., Tret'yakov D.B., Entin V.M., Ryabtsev I.I., Neizvestny I. Investigation of the long-term stability of single-photon quantum key generation in a polarization-coded circuit. Siberian Physical Journal. 2021. Vol. 16(2). pp. 81-93.
8. Levchenko S.A., Roenkov D.N. Quantum-cryptographic methods of information protection. SPbNTORES: Proceedings of the annual STC. 2019. № 1(74). pp. 201-203.
9. Belinsky A.V. On the violation of causality in experiments with photons // Vestnik of Moscow University. Series 3. Physics. Astronomy. - 2018. - №. 3. - pp. 14-25.
10. Averyanov V.S., Kartsan I.N. Key sequence safety by Charles Bennett protocol. In the collection: Russian science, innovations, education - ROSNIO-2022. collection of scientific articles on the materials of the All-Russian scientific conference. Krasnoyarsk, 2022. pp. 72-75.
11. Larionov N.V. Q-distribution for a single-atom laser operating in the "classical" mode // Journal of Experimental and Theoretical Physics. - 2022. - T. 161. - №. 2. - pp. 166-176.
12. Sidorov A.I. Sensor photonics // SPb: ITMO University. - 2019.

3 Vitaly S. Averyanov, postgraduate student of the "BIT" department, Siberian State University of Science and Technology named after Academician M.F. Reshetnev, Krasnoyarsk, Russia. E-mail: averyanov124@mail.ru, ORCID 0000-0001-6069-2537

4 Igor N. Kartsan, Dr.Sc., Associate Professor, Professor of the IS Department, Sevastopol State University, Sevastopol, Professor of the IS Department, Siberian State University of Science and Technology named after Academician M.F. Reshetnev, Krasnoyarsk, Russia. E-mail: kartsan2003@mail.ru, ORCID 0000-0003-1833-4036

13. Belyaev S.S. et al. Construction of cryptographically stable pseudorandom sequences generation function based on the “Grasshopper” encryption algorithm // Cyber Security Issues. - 2021. - №. 4 (44). - pp. 25-34.
14. Axelrod V.A., Averyanov V.S., Kartsan I.N. Quantum key distribution protocol BB84. In the collection: Russian science, innovations, education - RUSNIO-2022. collection of scientific articles on the materials of the All-Russian scientific conference. Krasnoyarsk, 2022. pp. 142-147.
15. Vershinina K.V., Saltykov A.R. Application of modified BB84-DS protocol for quantum key distribution (QKD). In the collection: Actual problems of infotelecommunications in science and education. collection of scientific works: in 4 volumes. Saint-Petersburg State University of Telecommunications by Prof. M.A.Bonch-Bruevich. Saint-Petersburg, 2021. pp. 151-155.
16. Zavala M., Barán B. QKD BB84. A taxonomy. В сборнике: Proceedings - 2021 47th Latin American Computing Conference, CLEI 2021. 47. 2021. DOI: 10.1109/CLEI53233.2021.9639932.
17. Alshaer N., Nasr M.E., Ismail T. Hybrid MPPM-BB84 quantum key distribution over fso channel considering atmospheric turbulence and pointing errors. IEEE Photonics Journal. 2021. Т. 13. № 6. С. 7600109. DOI: 10.1109/JPHOT.2021.3119767.
18. Vasiliu E. V. Resistance of ping-pong protocol with Greenberger-Horn-Zeilinger triplets to attack using auxiliary quantum systems // Informatics. - 2018. - №. 1 (21). - pp. 117-128.
19. Tudorache A.G., Manta V., Caraiman S. Quantum steganography based on the B92 quantum protocol //Mathematics. – 2022. – Vol. 10. – №. 16. – pp. 2870.
20. Komarova A. V., Korobeinikov A. G. Analysis of the main existing post-quantum approaches and electronic signature schemes // Cyber Security Issues. - 2019. - №. 2 (30). - pp. 58-68.
21. Gulakov I. R. et al. Detection of an information leakage channel from a multimode optical fiber by means of a silicon photomultiplier tube // Reports of the Belarusian State University of Informatics and Radioelectronics. - 2022. - Vol. 20. - №. 6. - pp. 37-44.
22. Kolyako A. V. et al. A study of the long-term stability of single-photon quantum key generation in a polarization-coded circuit // Siberian Physical Journal. - 2022. - Vol. 16. - №. 2. - pp. 81-93.
23. Torkhov N. A. Quantum-mechanical state of quantum system and tunneling effect (new view) // VHF Engineering and Telecommunication Technologies. - 2020. - №. 1-1. - pp. 331-332.