Цыганков Владимир Андреевич – Волгоградский государственный технический университет; e-mail: Vladimir.Tsygankov27@yandex.ru; г. Волгоград, Россия; тел.: 89176476959; магистр.

Шабалина Ольга Аркадьевна – e-mail: O.A.Shabalina@gmail.com; тел.: 89197958943; к.т.н.; доцент.

Катаев Александр Вадимович – e-mail: alexander.kataev@gmail.com; к.т.н.; доцент.

Tsygankov Vladimir Andreevich – Volgograd State technical University; e-mail: Vladimir.Tsygankov27@yandex.ru; Volgograd, Russia; phone: +79176476959; master.

Shabalina Olga Arkadevna – e-mail: O.A.Shabalina@gmail.com; phone: +79197958943; cand. of eng. sc.; associate professor.

Kataev Alexander Vadimovich – e-mail: alexander.kataev@gmail.com; cand. of eng. sc.; associate professor.

УДК 621.396.624 DOI 10.18522/2311-3103-2024-3-176-186

А.П. Плёнкин

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К СИСТЕМЕ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Рассматриваются вопросы современного состояния исследований и тенденции в области защиты передаваемых данных передовыми криптографическими методами. Приведено описание процесса шифрования и дешифрования информации при помощи абсолютно стойкого метода одноразового блокнота – шифра Вернама. В статье представлены типичные примеры задач, реализованные в области квантовой криптографии. Последнее включает в себя такие элементы, как неопределенность исходов, запутанность на квантовом уровне и принцип неопределенности Гейзенберга. Обсуждается подход к шифрованию данных с использованием симметричных алгоритмов и выдвигаются критерии для ключей шифрования, которые гарантируют полностью конфиденциальную передачу информации. Приводится краткий обзор истории развития квантовых коммуникационных систем и криптографии, подчеркивается важность дальнейших исследований в этой сфере. Отмечается, что в криптографии ключевым аспектом безопасности является распределение ключей шифрования среди авторизованных пользователей. Квантовая криптография предлагает решение для создания и распределения ключей с помощью методов, основанных на принципах квантовой механики, которые применяются в системах квантового распределения ключей. Современные реализации систем КРК всесторонне исследуются, в том числе на предмет различного рода атак, но подавляющее большинство исследований сосредоточено на поиске уязвимостей в работе квантовых протоколов, например, через техническое несовершенство компонентов систем КРК. В работе рассматривается способ осуществления несанкционированного доступа к системе КРК в процессе калибровки аппаратуры детектирования. Исследован способ получения несанкционированного доступа к работе системы квантового распределения ключей в режиме калибровки и предложен метод противодействия. Приведены результаты натурных исследований, которые показывают, что системы квантового распределения ключей имеют уязвимости не только при работе квантового протокола, но и в других жизненно важных стадиях функционирования системы. Описанный тип атаки позволяет несанкционированно получить данные о квантовом канале связи и осуществлять управляемую помеху процессу работы системы. Предложен способ построения автокомпенсационных систем оптической связи, обеспечивающий защищенность процесса калибровки от несанкционированного доступа. Показано влияние ослабленных до фотонного уровня синхроимпульсов на вероятность верного обнаружения отрезка времени с оптическим сигналом. В статье описаны результаты экспериментов, демонстрирующие различия между теоретическими данными и фактическими характеристиками отдельных элементов системы квантовой связи.

Синхроимпульс; распределение ключей; квантовые коммуникации; алгоритм поиска; контрмеры; атаки на квантовый канал.

A.P. Pljonkin

UNAUTHORIZED ACCESS TO QUANTUM KEY DISTRIBUTION SYSTEM

The paper examines the latest research and trends in safeguarding data transmission through state-of-the-art cryptographic techniques. It details the encryption and decryption process using the one-time pad method, also known as the Vernam cipher, renowned for its unparalleled security. The work showcases common challenges addressed by quantum cryptography, which encompasses concepts like outcome unpredictability, quantum entanglement, and the Heisenberg uncertainty principle. The paper discusses the use of symmetric algorithms for data encryption and sets forth standards for encryption keys that ensure the absolute confidentiality of data exchange. It provides a concise history of quantum communications and cryptography development, highlighting the critical need for ongoing research in this domain. A pivotal aspect of cryptographic security, the distribution of encryption keys to legitimate users, is underscored. Quantum cryptography presents a method for generating and sharing keys derived from quantum mechanical principles, integral to quantum key distribution (QKD) systems. Contemporary QKD systems undergo extensive scrutiny, including their susceptibility to various attack types, with most research aimed at identifying potential weaknesses in quantum protocols, often due to technical flaws in QKD system components. The study addresses a technique for unauthorized access to QKD systems during detector calibration. Furthermore, the paper explores a strategy for illicitly infiltrating the operations of a quantum key distribution system in calibration mode and suggests a defensive approach. Field research findings are presented, revealing that QKD systems are prone to vulnerabilities not only during quantum protocol execution but also throughout other crucial operational phases. The identified attack method enables the unauthorized acquisition of data from a quantum communication channel and the manipulation of system operations. A design for auto-compensating optical communication systems is proposed to protect the calibration process against unauthorized breaches. The impact of sync pulses, reduced to single-photon levels, on accurately detecting timing intervals with an optical signal is demonstrated. The article concludes with experimental results that exhibit variances between theoretical expectations and the actual performance of individual components within a quantum communication system.

Synchronization pulse; key distribution; quantum communications; search algorithm; countermeasures; attacks on the quantum channel.

Введение. Необходимость возникновения квантовой криптографии, как средства обеспечения защищенности передаваемых сообщений возникло в качестве логического продолжения гонки создания шифров и их взлома. Современная криптография основана на сложности математических вычислений (например, ассиметричное шифрование с открытым ключом) и уже известно, что теоретически такие методы будут взломаны в обозримом будущем. Таким образом, перед средствами обеспечения защищенности стоит задача использовать такой метод шифрования, который позволит сохранить конфиденциальность передаваемой информации необходимый (безопасный) период времени.

Идея квантовой криптографии заключается в том, чтобы создать вид шифрования, который невозможно взломать даже теоретически [1–3]. Существуют понятия абсолютно стойкого шифра и абсолютной секретности. Установлено, что для абсолютной секретности, ключ системы шифрования должен обладать следующими свойствами: быть абсолютно случайным; использоваться один раз; его длина должна быть не меньшей чем длина передаваемого сообщения [4].

Цель исследований состоит в том, чтобы продемонстрировать возможность несанкционированного вмешательства в работу системы квантового распределения ключей, оставаясь при этом незамеченным.

Требованиям абсолютной секретности удовлетворяют симметричные методы шифрования, такие как шифр Вернама, который также именуется одноразовым блокнотом [5, 6]. На рис. 1 представлена схема, поясняющая принцип шифрования методом одноразового блокнота.

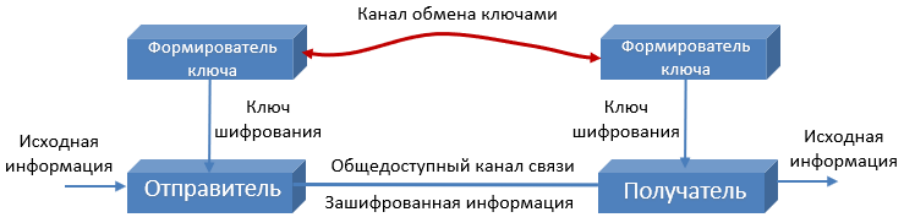


Рис. 1. Шифрование методом одноразового блокнота

Формирователь ключа приготавливает ключ (b), каждый бит которого абсолютно случаен. Далее каждый бит исходной информации (a) складывается по модулю с каждым битом ключа: $a = 0,1,0,1; b = 0,0,1,1; a \oplus b = 0,1,1,0$. После процедуры сложения информация становится настолько же защищенной, насколько защищен ключ. Другими словами, если к любому сообщению добавить случайное сообщение (последовательность), то итоговое сообщение становиться настолько же случайным. На приемной стороне Получатель производит обратную операцию с использованием ключа и получает исходную информацию. Уязвимым местом в приведенной схеме является способ передачи секретного ключа между пользователями. На практике это означает, что защищен должен быть не сам канал связи, а метод распределения ключа. Для реализации абсолютно секретной передачи должны быть соблюдены условия случайности ключа, его длины (относительно длины шифруемого сообщения) и его однократное использование. Однократное использование ключа необходимо в том числе для исключения атаки методом статистического анализа. Следовательно, в криптографических системах ключевым аспектом является гарантия безопасности, которая выражается в задаче распределения ключей шифрования между авторизованными пользователями. Методы квантовой криптографии предоставляют решение этой задачи, используя принципы квантовой физики, что находит применение в системах квантового распределения ключей (СКРК).

Современные реализации систем КРК всесторонне исследуются, в том числе на предмет различного рода атак. Подавляющее большинство исследований сосредоточено на поиске уязвимостей в работе квантовых протоколов, например, через техническое несовершенство компонентов систем КРК [7–10].

В нашей работе рассматривается способ осуществления несанкционированного доступа к системе КРК в процессе калибровки аппаратуры детектирования. Мы приводим результаты экспериментальных исследований автокомпенсационной системы КРК в различных режимах работы. В такой системе происходит компенсация фазовых изменений за счет оптического интерферометра и управляемых фазовых модуляторов [11, 12]. Работа систем КРК невозможна без процесса согласования станций, т.е. синхронизации разнесенных в пространстве передатчика и приёмника. В СКРК синхронизация заключается в высокоточном определении длины пути распространения оптического импульса и базируется на регистрации момента приёма синхроимпульса фотодетекторами. Под длиной пути будем понимать физическое расстояние, которое проходит оптический импульс от источника излучения до фотодетекторов. Отметим, что в различных реализациях систем КРК источник излучения и фотодетекторы могут располагаться в одном корпусе системы или по раздельности – источник излучения на передающей стороне, а фотодетекторы на приемной.

Известно, что наиболее эффективной формой сигнала в системах квантовой связи является периодическая последовательность оптических импульсов. Процесс синхронизации представляет собой последовательную отправку оптических импульсов с их последующим детектированием лавинными фотодетекторами. Так как процесс детектирования осуществляется пошагово, то такой тип синхронизации можно называть тактовым, т.е. передача и анализ осуществляется по тактам. В работе рассматривается волоконно-

оптическая реализация системы КРК, где источник излучения и фотодетекторы находятся в одном корпусе приемо-передающей станции. В кодирующей станции находится классический детектор синхронизации сигнала, фазовый модулятор для внесения изменений в сигнал.

Зная предельно допустимую длину квантового канала связи, скорость распространения оптических импульсов в волокне, можно вычислить максимальное время сигнала от источника излучения до кодирующей станции и обратно до фотодетекторов. Для функционирования системы КРК необходимо в определенный момент времени запускать лавинный фотодетектор. Этот момент времени измеряется в пикосекундах. Особенностью работы лавинных фотодетекторов является то, что они срабатывают при попадании первой частицы. При этом, последующие попадания не влияют на работу и не учитываются счетчиком. Временной интервал, в течение которого ОЛФД может регистрировать сигнал, назовем активным интервалом. После срабатывания, ОЛФД необходимо время для восстановления рабочего режима (мертвое время). Таким образом, для срабатывания детектора не имеет значения мощность импульса, или, в нашем случае количество фотонов в импульсе. Достаточно единичного фотона для запуска лавины. С другой стороны, если активный интервал будет открыт в течение 1 секунды, то мы не узнаем точное время попадания частицы в ОЛФД. Последнее означает, что на выходе из фотодетектора будет только сигнал о том, что за одну секунду было срабатывание. В работе [13] описана схема распространения оптического сигнала в автокомпенсационной системе КРК, а на рис. 2 показан процесс анализа временного интервала при обнаружении оптического синхросигнала.

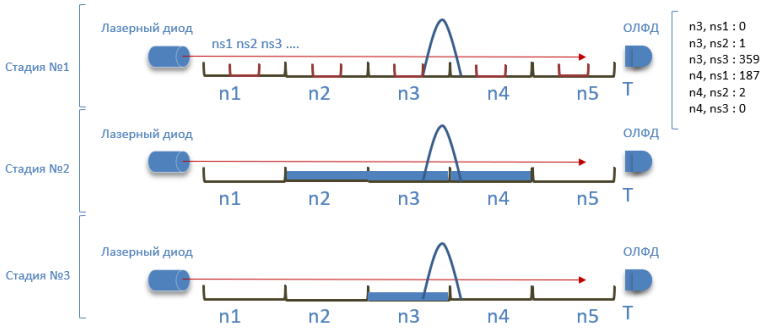


Рис. 2. Процесс обнаружения сигнала

Заключается в разбиении всего периода следования T на временные интервалы (временные окна) и подынтервалы. Период следования T – это время, выраженное через расстояние от источника излучения до кодирующей станции и обратно до фотодетекторов. Технически не имеет значения наличие кодирующей станции, так как ее функция на данном этапе заключается в отражении сигнала. Учитывая последнее, на рис. 2 источник излучения и фотодетекторы расположены на одной временной оси без отображения кодирующей станции. Разобьем весь период T на временные окна n. При этом n=1 нс. На всех трех этапах длительность временного окна одинаковая.

Стадия №1. Каждое временное окно разбивается на три равных по длительности подыинтервала (ns). Источник излучения осуществляет посылку оптического импульса с частотой 800Гц. Начальный момент посылки обозначим как момент 0 на оси времени. Фотодетекторы устанавливают активный интервал, равный ns и запускают его после каждой посылки импульса. Введем понятие временной задержки детектирования сигнала (d) – временной интервал, в течение которого лавинный фотодиод неактивен. При каждой посылке оптического импульса, параметр d=d+ns, т.е. временная задержка детектирования увеличивается на один подынтервал каждую итерацию. Активный интервал ОЛФД при этом не меняется. В каждом подынтервале регистрируется преобразование

фотона в первичный электрон. Для каждого ns осуществляется посылка порядка 800 импульсов. Последнее сделано для исключения ошибок при детектировании из-за темновых токов фотодетекторов. Таким образом, происходит последовательный анализ каждого временного подынтервала на всем периоде T. В каждом ns фиксируется количество срабатываний фотодетектора. На рис. 2 количество срабатываний на стадии №1 обозначено значениями 0,1,359,187,2,0. Видно, что разница между сигналом и ложными срабатываниями значительна. Система определяет временное окно nmax, к которому относится подынтервал ns с максимальным значением.

Стадия №2. Алгоритм калибровки аналогичен первой стадии, но теперь система анализирует не весь период T, а только временной отрезок длительностью 3 нс. Для этого берутся три временных окна: nmax-1; nmax; nmax+1, т.е. временное окно с максимальным числом срабатываний на первой стадии, предшествующее ему и следующее за ним по порядку. Каждое из n временных окон разбивается на подынтервалы таким образом, чтобы длительность каждого ns составляла 60 пс. Суммарное число подынтервалов на второй стадии равно 51 (по 17 ns в каждом n). Система определяет временное окно nmax, к которому относится подынтервал ns с максимальным значением.

Стадия №3. Алгоритм аналогичен предшествующим стадиям, но параметры и форма синхроимпульса отличаются. На этом этапе используется трейн мощных импульсов. Временной подынтервал ns с максимальным числом срабатываний, определенный на второй стадии, разбивается на подынтервалы с длительностью каждого 10 пс. Каждый из этих подынтервалов анализируется более 10000 раз.

Таким образом, итогом процесса синхронизации во временном выражении является интервал, равный 10 пс, а в выражении расстояния – измеренная длина квантового канала в метрах.

В [13, 14] описаны результаты натурных испытаний квантово-криптографической сети на базе системы КРК Clavis2 3110 фирмы IDQuantique и показано, что процесс синхронизации формирует многофотонные импульсы, а фотодетекторы работают в линейном режиме. Используя построенную энергетическую модель действующей системы КРК Clavis2 3110, покажем, что в режиме синхронизации не задействованы алгоритмы контроля мощности. Энергетическая модель системы КРК описывает характеристики аппаратуры детектирования. Для каждой стадии значение мощности (P) импульсов составляет: P1=-48,3 дБм, P2=-55,8 дБм, P3=-24,2 дБм (измерения проводились при помощи Yokogawa AQ2202). Суммарные потери в кодирующей станции (-47,7 дБм). Энергия фотона с учетом коэффициента преломления для волокна Corning®SMF-28e+ равна

$$E(p),\ [\text{Дж}] = \frac{h\frac{c}{n}}{\gamma} = \frac{6{,}62\cdot10^{-34}\cdot2{,}01\cdot10^{8}}{1550\cdot10^{-9}} = 0{,}0085\cdot10^{-17}.$$

Частота следования (f) для каждой стадии составляет: f1=800Гц, f2=800Гц, f3=5 МГц. Длительность синхроимпульса τ=1нс не изменяется. Моделирование показывает, что только при длине квантового канала в 50 км, среднее число фотонов в импульсе приближается к единице (усредненное значение трех этапов синхронизации). Стоит подчеркнуть, что начальный этап калибровки обладает самыми высокими энергетическими параметрами. Это критически важно для максимизации вероятности детектирования сигнала на этой стадии, поскольку любая ошибка в обнаружении или упущение сигнала на этапе начальной синхронизации может привести к серьезным ошибкам в детектировании на всех последующих этапах. Мощность лазера в системе не регулируется в соответствии с длиной квантового канала. Достижение однофотонного режима происходит за счет ослабления сигнала, что следует понимать не как разделение фотона, а как его присутствие в каждом отдельном i-ом импульсе. На практике это означает, что при однофотонной передаче, аттенюатор настраивается таким образом, чтобы энергия (мощность) детектировалось только в каждом десятом импульсе.

Покажем экспериментально, что калибровка в многофотонном режиме является уязвимостью для злоумышленника. Целью несанкционированного доступа к аппаратуре может быть не только перехват и расшифровка информации, но и создание помех в работе СКРК.

Схема экспериментального стенда показана на рис. 3. Станции системы КРК находятся в одном помещении и соединены квантовым каналом переменной длины (катушки оптического волокна Corning®SMF-28e+ длинами 1, 2, 4, 25 км).

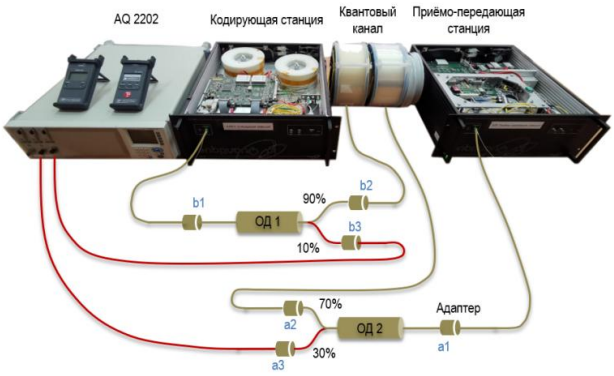


Рис. 3. Экспериментальный стенд

В точках соединения (адаптер) оптических катушек подключены последовательно два волоконно-оптических ответвителя (ОД) с коэффициентами деления 0,7x0,3 и 0,1x0,9. Выход приемо-передающей станции соединен с входом (a1) делителя, выход (a2) соединен с выходом (b2) через квантовый канал. Вход делителя (b1) соединен с выходом кодирующей станции получателя. Выходы (b3) (a2) подключены к измерителю оптической мощности и источнику излучения.

Технически внедрение ответвителей в волоконно-оптический канал связи не является сложной задачей и обеспечивается двумя точками подключения. Внедрение злоумышленника в квантовый канал позволяет получить технические данные о нем. Например, методами рефлектометрии можно определить расстояние до станций, а при помощи зондирующего импульса рассчитать время переотражения сигнала от кодирующей станции. Анализ зондирующего сигнала, идущего только в одну сторону, не предоставляет полной картины параметров квантового канала. Установка двух ответвителей дает возможность вычислить время, необходимое для возврата отраженного сигнала, что является ключевым для перехвата зондирующего сигнала при его обратном распространении. Зная время возврата сигнала, можно точно определить расстояние до кодирующего устройства и обратно, что может быть использовано для осуществления атаки типа "Троянский конь". В проведенном нами эксперименте была испытана другая техника атаки, позволяющая создавать помехи в системе, оставаясь незаметным.

Система КРК Clavis2 3110 введена в рабочий режим и синхронизирована. Работа квантового протокола BB84 осуществляется в штатном режиме, ключи циклично формируются, повторная синхронизация проходит успешно. Уровень ошибок QBER не превышает критический. Оптические ответвители были интегрированы в разрыв квантового канала на этапе калибровки (подсоединение осуществлялось при помощи переходных адаптеров). В таком режиме эксперимент длился 24 часа. Система КРК функционировала без сбоев, пополняя банк квантовых ключей и наличие в оптическом канале связи двух ответвителей мощности не было выявлено системой. Анализ сигналов на выходах (a3) и (b3) позволяет определить режим работы системы. Для осуществления помехи, к выходу (b3) подключается источник оптического излучения Yokogawa AQ2202 и в случайные моменты времени осуществляется подача сигнала-помехи. Помеха подавалась в течение нескольких временных интервалов с длительностью от 5 секунд до 5 минут. В режиме воздействия помехи запускался процесс повторной калибровки, при этом система не останавливала работу и не выдавала ошибок. После выключения помехи, возобновлялась работа квантового протокола. На рис. 4 показаны результаты компьютерного моделирования на основе полученных экспериментальных данных измеренной квантовой ошибки (QBER).

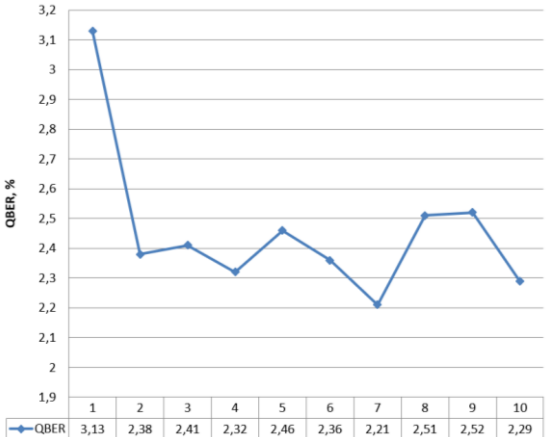


Рис. 4. Собранные данные о QBER

Зависимости на рисунке не показывают значительных отклонений. Анализ динамики квантовой битовой ошибки не обнаруживает индикаторов несанкционированного влияния на систему. Это также подтверждается информацией, представленной на рис. 5, демонстрирующем процесс генерации квантовых ключей во время эксперимента.

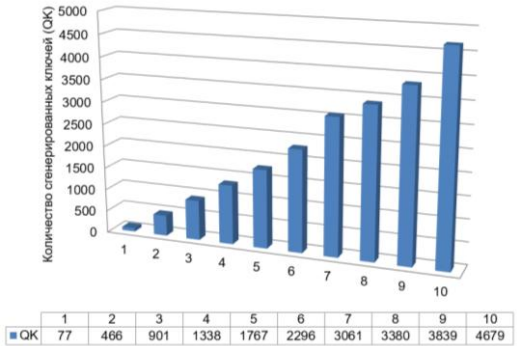
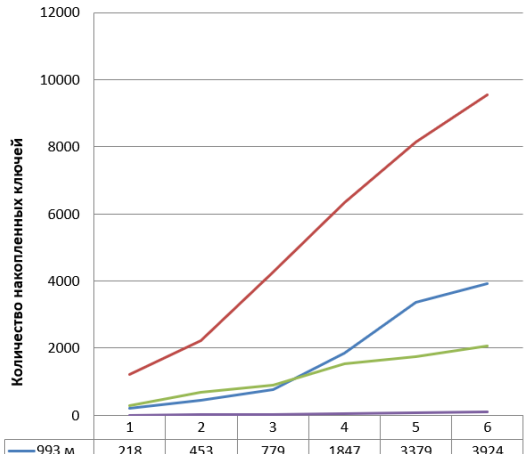


Рис. 5. Процесс аккумуляции квантовых ключей

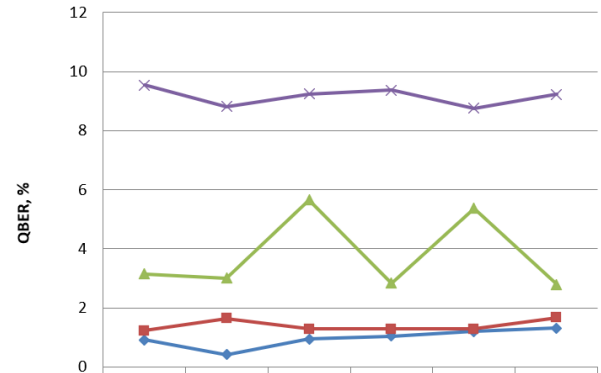
Итерации формирования ключей отражены на оси абсцисс. Ось ординат показывает количество накапливаемых 512-битных ключей в цикле.

Информация, представленная на рис. 4 и 5, была получена при использовании квантового канала длиной 25732 метра. Выявленные данные не дают возможности установить конкретные моменты времени, когда происходило воздействие помех на систему. При проецировании аппроксимированной зависимости (согласно рис. 5) на временную ось, можно заметить временные задержки в циклах с активированными помехами, отклонение которых не превышает 10% от среднего времени цикла формирования ключей. Такие задержки могут периодически возникать в процессе работы системы КРК и могут быть связаны с неоднородностями квантового канала или физическими изменениями в оптическом волокне, например, из-за влияния температур. Следовательно, анализ временных зависимостей в циклах накопления ключей также не указывает на наличие несанкционированных ответвлений в канале связи и не свидетельствует о неавторизированном вмешательстве. Обратимся к статистическим данным на рис. 6 и 7, где представлены зависимости накопленных ключей, QBER при различных длинах оптического канала связи. Экспериментальные результаты получены без использования ответвителей (т.е. без внесения помехи).



	1	2	3	4	5	6
993 м	218	453	779	1847	3379	3924
7880 м	1227	2215	4277	6342	8140	9546
25732 м	296	690	901	1547	1760	2073
50456 м	3	17	24	37	77	105

Рис. 6. Экспериментальные данные работы протокола



	1	2	3	4	5	6
993 м	0,91	0,42	0,94	1,04	1,19	1,31
7880 м	1,23	1,64	1,28	1,28	1,28	1,66
25732 м	3,15	3	5,65	2,83	5,37	2,79
50456 м	9,54	8,82	9,24	9,37	8,76	9,23

Рис. 7. Статистические данные работы квантового протокола BB84, QBER

Иллюстрация демонстрирует статистику работы квантового протокола BB84. На графике по оси абсцисс отложены итерации, а по оси ординат – число сгенерированных 512-битных ключей. Различные кривые соответствуют разным длинам квантового канала.

Анализ данных показывает, что за 6 итераций было собрано максимум 9546 ключей при длине квантового канала 7880 метров. Отчетливое различие наблюдается на графике для волоконно-оптической линии связи длиной 50456 метров, где количество ключей, сформированных за одну итерацию, заметно отличается от аналогичного показателя при меньшей длине ВОЛС, но тенденция роста остается неизменной. Это различие обусловлено значительным ослаблением сигнала из-за предельной длины квантового канала. Показатели QBER в диапазоне от 8,76 до 9,54 при длине квантового канала 50456 метров являются высокими, но не достигают критического уровня, так как не превышают расчетное значение QBER в 11%. Сравнивая изменения в количестве накопленных ключей и QBER с учетом наличия или отсутствия ответвителей, мы обращаем внимание на данные, представленные на рис. 5-8, сделанные для квантового канала длиной 25732 метра. При использовании ответвителей значение QBER находится в пределах от 2,3 до 3,1, в то

время как без ответвителей – от 2,8 до 5,7. Эти показатели находятся в приемлемых пределах и не свидетельствуют о присутствии злоумышленника в канале. Кроме того, экспериментальные данные показывают, что значения QBER без ответвителей превышают те, что были получены с их использованием.

Последнее указывает на то, что внешние дестабилизирующие факторы оказывают наиболее существенное влияние на QBER чем наличие дополнительных подготовленных соединений в канале связи.

Ось абсцисс – итерации, ординат – уровень квантовой ошибки. Разные зависимости – разные длины квантового канала.

Результаты эксперимента показывают возможность получения несанкционированного доступа к каналу связи и внесения помех в работу системы, оставаясь при этом незамеченным. В идеальных экспериментальных условиях, когда используется проверенное оптическое волокно (нормализующая катушка), рефлектометр позволяет обнаруживать ответвления (неоднородности). На разъемных соединениях можно заметить уменьшение сигнала на 0,2-0,4 дБ. Однако при использовании сварных соединений, выявление потерь сигнала становится крайне затруднительным. В условиях фактической эксплуатации, где строительная длина квантового канала редко превышает 800 метров, оптические муфты являются обычным элементом телекоммуникационной сети. Эти муфты и неоднородности волокна увеличивают затухание сигнала, что может маскировать неавторизированные подключения. Рефлектометрический метод в таких условиях не способен различать легитимные и нелегитимные неоднородности.

В качестве контрмер нами предложен метод калибровки станций, который обеспечивает повышенную защиту от несанкционированного доступа. В основе метода лежит использование ослабленных до однофотонного уровня синхроимпульсов. При этом ослабление оптического сигнала осуществляется на кодирующей станции управляемым аттенюатором, а значение затухания рассчитывается таким образом, чтобы на выходе из станции среднее число фотонов в синхроимпульсе составляло 0,1-0,5. В работе [15] приведено детальное описание метода, получены аналитические выражения вероятности обнаружения временного окна, погрешности обнаружения, проведено моделирование. В предлагаемом методе опрос временных интервалов осуществляется последовательно в каждом кадре, т.е. за период следования (T) анализируется один временной интервал. Такой подход позволяет не учитывать время восстановления рабочего режима фотодетектора при расчетах, а при заданных критических значениях среднего числа фотонов в импульсе, частоты появления импульсов темнового тока и квантовой эффективности фотокатода, переменным значением является только выборка в каждом временном окне. Импульсы темнового тока фотодетектора являются его дробовым шумом, которые могут вызвать лавинный эффект.

Выводы. В статье представлены результаты натурных испытаний действующей системы КРК, которые могут быть полезны другим коллективам для использования в исследованиях. Чем предложенный метод отличается от обрыва ВОЛС? Если злоумышленник повредит оптический кабель (перережет его), система легко это обнаружит. При использовании нашего метода, система не обнаружит нарушителя в квантовом канале, и он будет иметь возможность мешать работе системы в нужные ему моменты времени. Как дополнительная защита от неавторизированных вмешательств, применяется синхронизирующий импульс с изменяемой мощностью (для каждого этапа зондирования). Это, в сочетании с контролируемым уменьшением сигнала, усиливает защиту системы квантовой криптографии от НСД. Исследования показали, что система генерирует импульсы стабильной мощности, не зависящей от длины канала. Простые вычисления необходимой мощности синхронизирующего импульса могут помочь в регулировке мощности источника излучения и создании импульсов нужной мощности, соответствующих длине квантового канала.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Gisin N., Ribordy G., Tittel W., Zbinden H*. Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, No. 1. – P. 145-195.
2. *Bennett C.H., Brassard G., & Ekert A.K.* Quantum Cryptography // Scientific American. – 1992. – 267 (4). – P. 50-57. – http://www.jstor.org/stable/24939253.
3. *Кулик С.* Квантовая криптография // Фотоника. – 2010. – №. 2. – С. 36-41.
4. *Shannon C.E*. Communication theory of secrecy systems // in The Bell System Technical Journal. – Oct. 1949. – Vol. 28, No. 4. – P. 656-715. – DOI: 10.1002/j.1538-7305.1949.tb00928.x.
5. *Vernam G.S.* Cipher printing telegraph systems: For secret wire and radio telegraphic communications // Journal of the AIEE. – 1926. – 45 (2). – P. 109-115.
6. *Deng F.G., & Long G.L.* Secure direct communication with a quantum one-time pad // Physical Review A. – 2004. – 69 (5). – 052319.
7. *Heisenberg W.* The physical principles of the quantum theory. Courier Corporation. – 1949.
8. *Zhao Y., Fung C.H.F., Qi B., Chen C., & Lo H.K.* Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems // Physical Review A. – 2008. – 78 (4). – 042333.
9. *Makarov V., & Hjelme D.R.* Faked states attack on quantum cryptosystems // Journal of Modern Optics. – 2005. – 52 (5). – P. 691-705.
10. *Huang J.Z., Weedbrook C., Yin Z.Q., Wang S., Li H.W., Chen W., ... & Han Z.F.* Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack // Physical Review A. – 2013. – 87 (6). – 062329.
11. *Плёнкин А.П.* Безопасность предварительного этапа процесса синхронизации системы квантового распределения ключей. Информационные технологии // Радиоэлектроника. Телекоммуникации. – 2015. – №. 5-2. – С. 173-178.
12. *Кулик С.П., Молотков С.Н., Маккавеев А.П.* Комбинированный фазово-временной метод кодирования в квантовой криптографии // Письма в Журнал экспериментальной и теоретической физики. – 2007. – Т. 85, №. 5-6. – С. 354-359.
13. *Pljonkin A., Rumyantsev K., Singh P.K*. Synchronization in quantum key distribution systems // Cryptography. – 2017. – 1, 18. – DOI: 10.3390/cryptography1030018.
14. *Курочкин В.Л., Курочкин Ю.В., Зверев А.В., Рябцев И.И., Неизвестный И.Г.* Экспериментальные исследования в области квантовой криптографии // Фотоника. – 2012. – № 5. – С. 54-66.
15. *Румянцев К.Е., Плёнкин А.П.* Синхронизация системы квантового распределения ключа при использовании фотонных импульсов для повышения защищённости // Известия ЮФУ. Технические науки. – 2014. – № 8. – С. 81-96.
16. Futuristic Trends in Network and Communication Technologies Third International Conference, FTNCT 2020, Taganrog, 14–16 октября 2020 года. – Taganrog: Springer, 2021. – 533 p. – (Communications in Computer and Information Science; 2; Third International Conference, FTNCT 2020). – ISBN 978-981-16-1483-5.
17. *Pljonkin A., Petrov D., Sabantina L., Dakhkilgova K.* Nonclassical attack on a quantum keydistribution system // Entropy. – 2021. – Vol. 23, No. 5. – DOI: 10.3390/e23050509.
18. *Pljonkin A., Rumyantsev K.* Quantum-cryptographic network // Proceedings of 2016 IEEE East-West Design and Test Symposium, EWDTS 2016, Yerevan, 14–17 октября 2016 года. – Yerevan: Institute of Electrical and Electronics Engineers Inc., 2017. – P. 7807623. – DOI: 10.1109/EWDTS.2016.7807623.
19. *Шурупов А.П., Кулик С.П.* Квантовое распределение ключа на бифотонах-куквартах с проверочными состояниями // Письма в Журнал экспериментальной и теоретической физики. – 2008. – Т. 88, № 9-10. – С. 729-733.
20. *Финько В.Н., Киселев В.В., Джоган В.К. [и др.]*. Концептуальные понятия деятельности по защите информации // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2008. – № 2-1 (18). – С. 144-146.
21. *Alshaibi A., Al-Ani M., Al-Azzawi A. [et al.]*. The Comparison of Cybersecurity Datasets // Data. – 2022. – Vol. 7, No. 2. – DOI: 10.3390/data7020022.

REFERENCES

1. *Gisin N., Ribordy G., Tittel W., Zbinden H*. Quantum cryptography, *Reviews of Modern Physics,* 2002, Vol. 74, No. 1, pp. 145-195.
2. *Bennett C.H., Brassard G., & Ekert A.K.* Quantum Cryptography, *Scientific American,* 1992, 267 (4), pp. 50-57. Available at: http://www.jstor.org/stable/24939253.
3. *Kulik S.* Kvantovaya kriptografiya [Quantum cryptography], *Fotonika* [Photonics], 2010, No. 2, pp. 36-41.
4. *Shannon C.E*. Communication theory of secrecy systems, *in The Bell System Technical Journal,* Oct. 1949, Vol. 28, No. 4, pp. 656-715. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

5. *Vernam G.S.* Cipher printing telegraph systems: For secret wire and radio telegraphic communications, *Journal of the AIEE,* 1926, 45 (2), pp. 109-115.
6. *Deng F.G., & Long G.L.* Secure direct communication with a quantum one-time pad, *Physical Review A,* 2004, 69 (5), 052319.
7. *Heisenberg W.* The physical principles of the quantum theory. Courier Corporation, 1949.
8. *Zhao Y., Fung C.H.F., Qi B., Chen C., & Lo H.K.* Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, *Physical Review A,* 2008, 78 (4), 042333.
9. *Makarov V., & Hjelme D.R.* Faked states attack on quantum cryptosystems, *Journal of Modern Optics,* 2005, 52 (5), pp. 691-705.
10. *Huang J.Z., Weedbrook C., Yin Z.Q., Wang S., Li H.W., Chen W., ... & Han Z.F.* Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack, *Physical Review A,* 2013, 87 (6), 062329.
11. *Plenkin A.P.* Bezopasnost' predvaritel'nogo etapa protsessa sinkhronizatsii sistemy kvantovogo raspredeleniya klyuchey. Informatsionnye tekhnologii [Security of the preliminary stage of the synchronization process of a quantum key distribution system. Information technologies], *Radioelektronika. Telekommunikatsii* [Radioelectronics. Telecommunications], 2015, No. 5-2, pp. 173-178.
12. *Kulik S.P., Molotkov S.N., Makkaveev A.P.* Kombinirovannyy fazovo-vremennoy metod kodirovaniya v kvantovoy kriptografii [Combined phase-time coding method in quantum cryptography] *Pis'ma v Zhurnal eksperimental'noy i teoreticheskoy fiziki* [Letters to the Journal of Experimental and Theoretical Physics], 2007, Vol. 85, No. 5-6, pp. 354-359.
13. *Pljonkin A., Rumyantsev K., Singh P.K*. Synchronization in quantum key distribution systems, *Cryptography,* 2017, 1, 18. DOI: 10.3390/cryptography1030018.
14. *Kurochkin V.L., Kurochkin Yu.V., Zverev A.V., Ryabtsev I.I., Neizvestnyy I.G.* Eksperimental'nye issledovaniya v oblasti kvantovoy kriptografii [Experimental research in the field of quantum cryptography], *Fotonika* [Photonics], 2012, No. 5, pp. 54-66.
15. 15. Rumyantsev K.E., Plenkin A.P. Sinkhronizatsiya sistemy kvantovogo raspredeleniya klyucha pri ispol'zovanii fotonnykh impul'sov dlya povysheniya zashchishchennosti [Synchronization of a quantum key distribution system using photon pulses to increase security], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8, pp. 81-96.
16. Futuristic Trends in Network and Communication Technologies Third International Conference, FTNCT 2020, Taganrog, 14–16 октября 2020 года. Taganrog: Springer, 2021, 533 p. – (Communications in Computer and Information Science; 2; Third International Conference, FTNCT 2020). ISBN 978-981-16-1483-5.
17. *Pljonkin A., Petrov D., Sabantina L., Dakhkilgova K.* Nonclassical attack on a quantum keydistribution system, *Entropy,* 2021, Vol. 23, No. 5. DOI: 10.3390/e23050509.
18. *Pljonkin A., Rumyantsev K.* Quantum-cryptographic network, Proceedings of 2016 IEEE East-West Design and Test Symposium, EWDTS 2016, Yerevan, October 14–17, 2016. Yerevan: Institute of Electrical and Electronics Engineers Inc., 2017, pp. 7807623. DOI: 10.1109/EWDTS.2016.7807623.
19. *Shurupov A.P., Kulik S.P.* Kvantovoe raspredelenie klyucha na bifotonakh-kukvartakh s proverochnymi sostoyaniyami [Quantum key distribution on biphotons-cuquarts with test states], *Pis'ma v Zhurnal eksperimental'noy i teoreticheskoy fiziki* [Letters to the Journal of Experimental and Theoretical Physics], 2008, Vol. 88, No. 9-10, pp. 729-733.
20. *Fin'ko V.N., Kiselev V.V., Dzhogan V.K. [i dr.].* Kontseptual'nye ponyatiya deyatel'nosti po zashchite informatsii [Conceptual concepts of information security activities], *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [Reports of the Tomsk State University of Control Systems and Radioelectronics], 2008, No. 2-1 (18), pp. 144-146.
21. *Alshaibi A., Al-Ani M., Al-Azzawi A. [et al.].* The Comparison of Cybersecurity Datasets, *Data,* 2022, Vol. 7, No. 2. DOI: 10.3390/data7020022.

Статью рекомендовал к опубликованию д.т.н., профессор А.Н. Целых.

Плёнкин Антон Павлович – Южный федеральный университет; e-mail: pljonkin@sfedu.ru; г. Таганрог, Россия; тел.: 89054592158; кафедра ИБТКС; к.т.н.; доцент.

Pljonkin Anton Pavlovich – Southern Federal University; e-mail: pljonkin@sfedu.ru; Taganrog, Russia; phone: +79054592158; the department of information security of telecommunication systems; associate professor.