УДК 621.396.624

А.П. Плёнкин

Экспериментальная синхронизация системы квантовой связи

Рассматривается алгоритм обнаружения оптического сигнального импульса в процессе тактовой синхронизации системы квантового распределения ключей. Проведен обзор нескольких методов синхронизации аппаратуры квантовой связи и показано, что отличительные характеристики сводятся к значениям вероятности правильного обнаружения сигнального временного интервала, содержащего оптический импульс и среднему времени вхождения в синхронизм. Описана схема экспериментального стенда и приведены результаты натурных исследований автокомпенсационной системы квантового распределения ключей, которые показывают параметры энергетической модели процесса тактовой синхронизации при наличии дестабилизирующих факторов в квантовом канале. Поставлен эксперимент по внедрению в квантовый канал оптических ответвителей с атмосферным трактом. Продемонстрирована возможность отвода части оптического излучения из канала связи в процессе тактовой синхронизации, что может быть использовано злоумышленником для внесения помех в работу системы квантового распределения ключей. Описаны возможные каналы утечки данных в общей структуре квантово-криптографических сетей.

Ключевые слова: квантовые коммуникации, квантовый ключ, фотонный импульс, вероятность обнаружения, доверенные узлы.

DOI: 10.21293/1818-0442-2024-27-3-37-41

Обзор литературных и патентных источников показывает, что подавляющее большинство научных исследований сосредоточено на работе квантовых протоколов в системах квантового распределения ключей (КРК), их разработке, анализе, стойкости [1–9]. Для функционирования любой системы квантовой связи, в том числе при построении сетей квантовых коммуникаций необходимо синхронизировать аппаратуру и иметь аутентифицированные каналы [10–13]. Так, при работе большинства протоколов квантового распределения ключей необходимо, чтобы отправитель и получатель однозначно идентифицировали друг друга. Аутентификация и идентификация происходят по общедоступному каналу связи. Синхронизация оптической части систем КРК требуется, например, для того, чтобы аппаратура получателя определяла, в какой момент времени прикладывать напряжение к фазовому модулятору. Рассмотрим процесс тактовой синхронизации, реализованный в системах КРК с фазовым и поляризационным кодированием. Отметим, что какое-либо воздействие на процесс синхронизации не влияет на стойкость квантового протокола или полученных ключей, но может рассматриваться как уязвимость в работе системы квантовой связи в целом.

В процессе тактовой синхронизации происходит обнаружение сигнального оптического импульса в конкретный момент времени T_0. Например, для реализации протокола BB84 в системах КРК с фазовым кодированием длительность T_0 составляет 10 пс. Процесс поиска T_0 заключается в вычислении длины оптического пути – расстояние, которое проходит оптический импульс от отправителя к получателю, а точнее – от источника оптического излучения к фотоприемнику. Если рассматривать реализацию системы КРК с автоматической компенсацией фазы, то источник излучения и фотодетекторы конструктивно расположены в одном корпусе. Программное обеспечение системы КРК дробит период следования оптических импульсов на временные интервалы T_w таким образом, чтобы длительность T_w была не больше длительности зондирующего оптического импульса T_i. Далее происходит поэтапный анализ всех интервалов T_w. Технически это реализовано пошаговым переключением счетчика фотоэлектронов по временной оси. Описывая процесс тактовой синхронизации, можно выделить два этапа:

– с заданной частотой следования и длительностью T_i осуществляется посылка импульсов. Система пошагово анализирует временные интервалы $T_w/3$ и фиксирует количество срабатываний фотодетектора в каждом из них. В процессе синхронизации фотодетекторы функционируют в линейном режиме, что позволяет исключить задержку в детектировании из-за «мертвого времени» и фиксировать все зарегистрированные фотоны. По завершении сканирования система знает количество срабатываний фотодетектора в каждом интервале T_w. На практике это выражается в числовом значении, причем разница между сигнальным интервалом и шумовым однозначно интерпретируется;

– интервал T_w с максимальными значениями и два соседних T_w разбиваются на более короткие интервалы $T_w/17$. Алгоритм анализирует не весь период T, а только временной отрезок $3T_w$. В результате второго этапа определяется интервал $T_w/17$ с максимальным числом срабатываний фотодетектора. Далее осуществляется многократный анализ найденного $T_w/17$ и уточнение длительности до значения в 10 пс.

Таким образом, в процессе тактовой синхронизации осуществляется поиск интервала, равного 10 пс, что в выражении расстояния является длиной квантового канала в метрах.

В работах [14–18] исследуются схожие алгоритмы синхронизации, отличающиеся методикой дробления и анализа периода следования. Ориги-

нальный алгоритм тактовой синхронизации использует пошаговый анализ временных интервалов. Приведенные в исследованиях алгоритмы предлагают, например, на первом этапе разделить весь период следования на два интервала. После анализа каждого из этих интервалов и выделения сигнального, разделить его еще на два и т.д. до получения искомого интервала в 10 пс.

Известно, что особенность работы ОЛФД заключается в его срабатывании при попадании первого фотона. Последующие регистрации в течение определенного времени (мертвое время) не учитываются детектором. ОЛФД необходимо время для восстановления рабочего режима. Последнее говорит о том, что мощность импульса (или количество фотонов) не влияет на факт регистрации. Как это влияет на процесс обнаружения оптического импульса в процессе синхронизации? Если ОЛФД будет активен в течение 1 с, то мы не сможем уточнить время регистрации фотона, т.е. на выходе фотодетектора будет только электрический сигнал о том, что за одну секунду было срабатывание.

Анализ работ [14–17] показывает, что сравнение исследуемых алгоритмов можно провести по двум параметрам – вероятность правильного обнаружения сигнального временного интервала и суммарное время поиска. Отметим, что приведенные в статьях данные вероятности правильного обнаружения справедливы только при определенных заданных условиях (например, при частоте темнового тока фотодетектора не более 100 Гц, при строгом расположении оптического импульса в одном временном интервале и т.д.). Время вхождения в синхронизм также не может являться критерием эффективности или сравнения алгоритмов в данном случае, так как в работах приводятся весьма усредненные значения.

В исследованиях [18] рассматривается практическая система распределения квантовых ключей с непрерывной переменной (CVQKD) и процесс её синхронизации. Авторы предлагают высокопроизводительный метод синхронизации кадров для систем CVQKD, который способен работать при низких отношениях сигнал/шум (SNR) и совместим со случайным сдвигом фаз, вызванным квантовым каналом. В работе описана практическая реализация метода и проанализирована его эффективность. Суть метода заключается в регулировании длины кадра синхронизации, что позволяет работать с большим диапазоном значений SNR и увеличить рабочее расстояние квантового канала.

В наших исследованиях [19] приводится детальное описание процесса тактовой синхронизации для систем КРК с фазовым кодированием состояний фотонов и описывается эксперимент по осуществлению неклассической атаки на системы КРК. Результаты эксперимента показывают, что в процессе тактовой синхронизации возможно несанкционированное внедрение в квантовый канал с целью дальнейшего внесения помехи в работу системы на этапе формирования ключей.

Задачей исследования является демонстрация работы системы КРК при наличии несанкционированных устройств в квантовом канале.

На рис. 1 и 2 представлены экспериментальные стенды схем расширенного эксперимента, целью которого является демонстрация работы автокомпенсационной системы КРК с интегрированным атмосферным оптическим каналом связи (АОЛС). Суть эксперимента заключается в попытке отведения части оптической мощности из квантового канала в процессе синхронизации и распределения квантовых ключей. Особенностью натурных испытаний является то, что в качестве побочного канала используется атмосферный тракт (АОЛС, рис. 2).

Рис. 1. Схема 1: система квантового распределения ключей Clavis^2; осциллограф LeCroy 104Xs; модульная система Yokogawa AQ2202; коллиматоры с эффективным фокусным расстоянием 100 см, ВОЛС

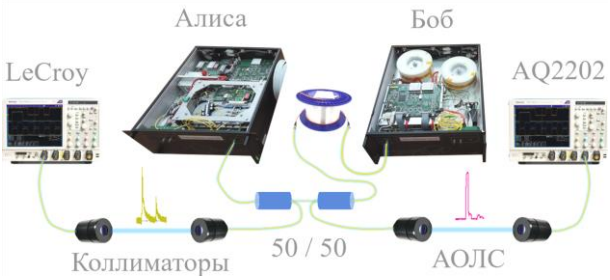

Рис. 2. Схема 2

Станции системы КРК соединены по топологии «точка-точка» и находятся на расстоянии друг от друга в 980 м. Квантовый канал выполнен из стандартного одномодового оптического волокна с типовым затуханием 0,2 дБ/км. Волоконно-оптические ответвители с коэффициентами деления 50/50 подключаются в разрыв ВОЛС так, чтобы на их входы подавались сигналы от отправителя и получателя. К выходам ответвителей подключены коллиматоры, которые установлены на расстоянии в 1 м.

В схеме 1 часть волоконно-оптического квантового канала заменяется на атмосферный. Наблюдения в течение 30 циклов работы (от задания параметров синхронизации до формирования квантового ключа) системы КРК показывают, что процесс тактовой синхронизации и работа квантового протокола протекают в стандартном режиме. Уровень квантовых ошибок не превышает критический. Другими словами, наличие ответвителей и атмосферного канала не влияют на нормальное функционирование систем КРК.

В схеме 2 коллиматоры подключены таким образом, чтобы отводить 50% оптической мощности на аппаратуру анализа. Отвод оптической мощности производится как при прямом прохождении сигнала, так и при обратном (отраженного от зеркала Фарадея). В такой схеме наблюдения также показывают стабильную работу системы КРК во всех режимах. Схема 2 дает возможность зафиксировать моменты регистрации оптических сигналов при прямом и обратном распространении, что может быть полезным злоумышленнику, например, для вычисления удаленности станции получателя. Использование рефлектометра (при подключении на входы ответвителей) позволит провести детальный энергетический анализ всего квантового канала.

Отметим, что калибровка коллиматоров производилась ручным способом без каких-либо специальных приспособлений, а сами коллиматоры доступны в открытой продаже и также не являются специализированным или дорогостоящим оборудованием.

Выводы и дискуссия

В данной статье мы рассмотрели алгоритм обнаружения оптического сигнального импульса в процессе тактовой синхронизации системы квантового распределения ключей. Провели обзор нескольких методов синхронизации аппаратуры квантовой связи и показали отличия. Проанализировали алгоритмы тактовой синхронизации, которые используются или предлагаются к использованию в системах квантовой связи. Известно, что эффективность алгоритмов синхронизации можно оценить по нескольким параметрам, таким как вероятность правильного обнаружения сигнального временного интервала и общее время вхождения в синхронизм. В статье мы не рассматриваем количественные значения данных параметров, но приводим ссылки на материалы, где они описаны.

Показали этапы работы алгоритма обнаружения оптического импульса на примере автокомпенсационной системы квантового распределения ключей. Описали эксперимент по внедрению в квантовый канал оптических ответвителей с атмосферным трактом. Продемонстрировали возможность отвода части оптического излучения из канала связи в процессе тактовой синхронизации. Внедрение в канал связи может быть использовано злоумышленником для внесения помех в работу системы квантового распределения ключей.

Поясним, что используемые в описываемых системах КРК ОЛФД функционируют как в линейном режиме, так и в режиме Гейгера. Так, в процессе синхронизации ОЛФД функционируют в линейном режиме, а в процессе работы квантового протокола они переводятся в режим Гейгера (одиночного счета фотонов).

Описывая возможные каналы утечки данных в общей структуре квантово-криптографических сетей, можно выделить несколько «слабых», на наш взгляд, мест:

– Каналы взаимодействия между станцией системы КРК и сервером, сервером и СКЗИ и т.д. Часто это патч-корды USB или RJ45. Эти отрезки кабеля не защищены от НСД, и если предположить, что к ним есть доступ, то возможен несанкционированный съем данных. Эти же каналы утечки можно рассмотреть в отношении сервера, обеспечивающего работу системы КРК. Если рассматривать надежность и защищенность вспомогательного оборудования, то необходимо предусмотреть периодический анализ помещения на предмет утечек по побочным каналам (в том числе ПЭМИН). В магистральных сетях с использованием ДПУ необходимо, в зависимости от метода распределения квантовых ключей и шифрования информации, разрабатывать специальные мероприятия по обнаружению возможных каналов утечки данных в помещениях ДПУ.

– ВОЛС или канал синхронизации. Когда мы говорим об уязвимостях в сетях КРК, то чаще всего подразумевается взлом квантовых ключей (квантовых протоколов). Исследования и практическое использование систем КРК показывают, что не менее важным является обеспечение защищенности каналов синхронизации и аутентификации. Такие каналы в зависимости от схемы КРК могут быть реализованы, например, в волокне, по которому происходит формирование квантовых ключей. Проведенный эксперимент показывает, что для внедрения в квантовый канал не требуется специальной дорогостоящей аппаратуры или специализированных знаний. Достаточно навыков сварки оптического волокна и умения обращаться с осциллографом. Модель злоумышленника в данном случае трансформируется из высококлассного специалиста в рядового исполнителя. Отметим, что целью атаки на систему или сеть КРК может являться контролируемая помеха, которую атакующий применяет в определенные моменты времени (например, при передаче секретной информации).

Для начала взаимодействия между отправителем и получателем должен быть реализован аутентифицированный канал связи. Это крайне важное условие, влияющее на защищенную реализацию сети в целом. В частности, актуальным вопросом является осуществление надежной и защищенной аутентификации в отсутствие квантовых ключей.

В книге [20] детально рассматриваются вопросы идентификации и аутентификации в цифровом пространстве. Интересными представляются работы [21–23], которые предлагают протокол квантового распределения ключей через открытое пространство. Протокол, кроме ограничений квантовой механики на различимость неортогональных квантовых состояний, использует дополнительные ограничения, диктуемые специальной теорией относительности. В отличие от всех существующих протоколов квантового распределения ключей, данный протокол обеспечивает секретность ключей при не строго однофотонном источнике квантовых состояний и произвольной длине квантового канала связи.

В заключение можно сделать акцент на том, что реализация квантово-криптографических сетей в идеальном варианте исполнения возможна, но требует тщательной подготовки и постоянного монито-

ринга всех компонентов сети. Системы квантового распределения ключей активно используются, но их техническая реализация ещё нуждается в совершенствовании. Квантовые сети большой длины и смешанной топологии уже эксплуатируются, но детальное описание алгоритмов, используемых узлов, методов и компонентов в литературе отсутствует. Вектор развития технологии КРК направлен на преодоление барьера ограниченной длины квантового канала, развитие интегральной фотоники, атмосферных (космических) и подводных систем квантовой связи.

Литература

1. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // Reviews of Modern Physics. – 2002. – Vol. 74, No. 1. – P. 145−195.

2. Bennett C.H. Quantum Cryptography / C.H. Bennett, G. Brassard, A.K. Ekert // Scientific American. – No. 267 (4). – P. 50–57.

3. Кулик С.П. Квантовая криптография // Фотоника. – 2010. – № 2. – С. 36–41.

4. Shannon C.E. Communication theory of secrecy systems // The Bell System Technical Journal. – 1949. – Vol. 28, No. 4. – P. 656–715.

5. Vernam G.S. Cipher printing telegraph systems: For secret wire and radio telegraphic communications // Journal of the AIEE. – 1926. – Vol. 45 (2). – P. 109–115.

6. Deng F.G. Secure direct communication with a quantum one-time pad / F.G. Deng, G.L. Long // Physical Review. – 2004. – Vol. A. 69 (5). – P. 052319.

7. Деев А.Д. Квантовые коммуникации через атмосферные (космические) каналы связи / А.Д. Деев, А.А. Калинкин, С.П. Кулик // Интернет изнутри. – 2024. – № 20. – С. 43–47.

8. Зякин Е.В. Перспективные протоколы КРК для оптической связи в свободном пространстве / Е.В. Зякин, А.В. Молоканов, К.М. Чуриков // Новые технологии. Наука, техника, педагогика. – 2024. – С. 141–148.

9. Zhao Y. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems / Y. Zhao, C.H.F. Fung, B. Qi, C. Chen, H.K. Lo // Phys. Rev. – 2008. – Vol. A 78 (4). – P. 042333.

10. Chen Y.A. An integrated space-to-ground quantum communication network over 4,600 kilometres // Nature. – 2021. – Vol. 589, No. 7841. – P. 214–219.

11. Beals T.R. Distributed relay protocol for probabilistic information-theoretic security in a randomly-compromised network / T.R. Beals, B.C. Sanders // Information Theoretic Security: Third International Conference ICITS 2008. – Canada, Calgary, 2008. – P. 29–39.

12. Dianati M. Architecture of the Secoqc quantum key distribution network / M. Dianati, R. Alleaume // First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07). – IEEE. – 2007. – P. 13.

13. Barnett S.M. Securing a quantum key distribution relay network using secret sharing / S.M. Barnett, S.J.D. Phoenix // Conference and Exhibition (GCC). – IEEE. – 2011. – P. 143–145.

14. Румянцев К.Е. Вероятностные характеристики алгоритма обнаружения синхросигналов на основе выбора смежной пары сегментов с максимальным суммарным отсчётом / К.Е. Румянцев, П.Д. Миронова // Известия ЮФУ. Технические науки. – 2023. – № 3 (233). – С. 96–107.

15. Миронова П.Д. Алгоритм обнаружения синхросигналов на основе выбора смежной пары сегментов с максимальным суммарным отсчётом // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: Сборник статей Всерос. науч.-техн. конф. – Таганрог: ЮФУ, 2023. – P. 52–53.

16. Pljonkin A. Synchronization in quantum key distribution systems / A. Pljonkin, K. Rumyantsev, P.K. Singh // Cryptography. – 2017. – No. 1. – P. 18.

17. Румянцев К.Е. Синхронизация системы квантового распределения ключа при использовании фотонных импульсов для повышения защищённости / К.Е. Румянцев, А.П. Плёнкин // Известия ЮФУ. Технические науки. – 2014. – № 8. – С. 81–96.

18. Lin D. High performance frame synchronization for continuous variable quantum key distribution systems // Optics Express. – 2015. – Vol. 23, No. 17. – P. 22190–22198.

19. Nonclassical attack on a quantum keydistribution system / A. Pljonkin, D. Petrov, L. Sabantina, K. Dakhkilgova // Entropy. – 2021. – Vol. 23, No. 5.

20. Сабанов А. Г. Идентификация и аутентификация в цифровом мире / А.Г. Сабанов, А.А. Шелупанов. – М.: Горячая Линия – Телеком. – 2022.

21. Пат. 2667755 РФ, МПК H04L9/08. Система релятивистской квантовой криптографии / Кравцов К.С. и др. (РФ). – № 2017117184; заявл. 05.17.2017; опубл. 24.09.2024.

22. Кулик С.П. Комбинированный фазово-временной метод кодирования в квантовой криптографии / С.П. Кулик, С.Н. Молотков, А.П. Маккавеев // Письма в журнал экспериментальной и теоретической физики. – 2007. – Т. 85, № 5-6. – С. 354–359.

23. Шурупов А.П. Квантовое распределение ключа на бифотонах-куквартах с проверочными состояниями / А.П. Шурупов, С.П. Кулик // Письма в журнал экспериментальной и теоретической физики. – 2008. – Т. 88, № 9-10. – С. 729–733.

Плёнкин Антон Павлович
Канд. техн. наук, доцент каф. информационной безопасности телекоммуникационных систем
Института компьютерных технологий и информационной безопасности Южного федерального университета
Чехова ул., 2, г. Таганрог, Россия, 347900
Scopus: 57190492977
ORCID: 0000-0001-6713-9347
Тел.: +7-905-459-21-58
Эл. почта: pljonkin@sfedu.ru

Pljonkin A.P.

Experimental Synchronization of a Quantum Communication System

The article considers an algorithm for detecting an optical signal pulse during the clock synchronization of a quantum key distribution system. Several methods for synchronizing quantum communication equipment are reviewed and it is shown that the distinctive characteristics are reduced to the values of the probability of correctly detecting a signal time interval containing an optical pulse and the average time of entering synchronization. The scheme of the experimental setup is described and the results of full-scale studies of the autocompensation quantum key distribution system are presented. The results show the parameters of the energy model of the clock synchronization process in the presence of destabilizing factors in the quantum channel. An experiment was conducted to introduce optical couplers with an atmospheric path into the quantum

channel. The possibility of diverting part of the optical radiation from the communication channel during clock synchronization is demonstrated, which can be used by an intruder to interfere with the operation of the quantum key distribution system. The possible data leakage channels in the general structure of quantum cryptographic networks are described.

Keywords: quantum communications, quantum key, photon pulse, detection probability, trusted nodes.
DOI: 10.21293/1818-0442-2024-27-3-37-41

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, no. 267 (4), pp. 50–57, http://www.jstor.org/stable/24939253

3. Kulik S. Quantum cryptography. Photonica. 2010, no. 2, pp. 36–41.

4. Shannon C.E. Communication theory of secrecy systems. *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 American Institute of Electrical Engineers*, 1926, vol. 45 (2), pp. 109–115.

6. Deng F.G., Long G.L. Secure direct communication with a quantum one-time pad. *Physical Review*, 2004, Vol. A 69 (5), p. 052319.

7. Quantum communications through atmospheric (space) communication channels / A.D. Deev, A.A. Kalinkin, S.P. Kulik // *Internet Inside*, 2024, pp. 20, pp. 43–47.

8. Zyakin E.V. Promising QKD protocols for optical communications in free space / E.V. Zyakin, A.V. Molokanov, K.M. Churikov // *New Technologies. Science, Engineering, Pedagogics: Proceedings of the All-Russian Scientific-Practical Conference*, Moscow, 2024, pp. 141–148.

9. 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,* 2008, vol. A 78 (4), p. 042333.

10. Chen Y.A. An integrated space-to-ground quantum communication network over 4,600 kilometres // *Nature*, 2021, no. 7841, pp. 214–219.

11. Beals T.R., Sanders B.C. Distributed relay protocol for probabilistic information-theoretic security in a randomly-compromised network //Information Theoretic Security: *Third International Conference, ICITS 2008, Calgary, Canada, August 10-13, 2008. Proceedings 3*. Berlin Heidelberg, Springer, 2008, pp. 29–39.

12. Dianati M., Alléaume R. Architecture of the Secoqc quantum key distribution network //2007 *First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*. *IEEE*, 2007, pp. 13.

13. Barnett S.M., Phoenix S.J.D. Securing a quantum key distribution relay network using secret sharing // 2011 *IEEE GCC Conference and Exhibition (GCC). IEEE*, 2011, pp. 143–145.

14. Rumyantsev K.E., Mironova P.D. Probabilistic characteristics of the algorithm for detecting synchronization signals based on the selection of an adjacent pair of segments with the maximum total count // *Izvestiya SFedU. Engineering Sciences*, 2023, no. 3 (233), pp. 96–107. doi: 10.18522/2311-3103-2023-3-96-107.

15. Mironova, P.D. Algorithm for detecting synchronization signals based on selecting an adjacent pair of segments with the maximum total count // *Fundamental and Applied Aspects of Computer Technology and Information Security: Collection of Articles of the All-Russian Scientific and Technical Conference, Taganrog, April 10–15*. 2023. Taganrog, Southern Federal University, 2023, pp. 52–53.

16. Pljonkin A., Rumyantsev K., Singh P.K. Synchronization in quantum key distribution systems. *Cryptography*. 2017, pp. 18. doi:10.3390/cryptography1030018.

17. Rumyantsev K.E., Plenkin A.P. Synchronization of the quantum key distribution system using photon pulses to increase security. *Izvestiya SFedU. Engineering Sciences*, 2014, No. 8, pp. 81–96.

18. Lin D. et al. High performance frame synchronization for continuous variable quantum key distribution systems // *Optics Express*, 2015, vol. 23, no.17, pp. 22190–22198.

19. Nonclassical attack on a quantum keydistribution system / A. Pljonkin D. Petrov L. Sabantina K. Dakhkilgova // *Entropy*, 2021, vol. 23, no. 5, doi: 10.3390/e23050509.

20. Sabanov A.G., Shelupanov A.A. *Identification and authentication in the digital world*. Moscow, Hot Line-Telecom, 2022.

21. Kravtsov K.S. et al. [Relativistic quantum cryptography system]. Patent RF, no. 2667755, 2024/

22. Kulik S.P., Molotkov S. N., Makkaveev A.P. Combined phase-time coding method in quantum cryptography. *Letters to the Journal of Experimental and Theoretical Physics*. 2007, vol. 85, pp. 354–-359.

23. Shurupov A.P., Kulik S.P. Quantum key distribution on biphotons-ququarts with test states. *Letters to the Journal of Experimental and Theoretical Physics*, 2008, vol. 88, no. 9-10, pp. 729–733.

Anton P. Pljonkin
Candidate of Sciences in Engineering, Associate Professor, Department of Information Security of Telecommunication Systems, Institute of Computer Technologies and Information Security, Southern Federal University
2, Chekhova st., Taganrog, Russia, 347900
Scopus: 57190492977
ORCID: 0000-0001-6713-9347
Phone: +7-905-459-21-58
Email: pljonkin@sfedu.ru