13. *Erdelj M., Natalizio E., Kaushik R.* Help from the Sky: Leveraging UAVs for Disaster Management // IEEE Pervasive Computing. 2017. Vol. 16, № 1. P. 24–32.
14. *Kersnovski T., Gonzalez F., Morton K.* A UAV System for Autonomous Target Detection and Gas Sensing // Materials of IEEE Aerospace Conference (Yellowstone Conference Center, Big Sky, Montana, 4–11 March 2017). Big Sky, 2017. P. 1–12.
15. *Motlagh N.H., Bagaa M., Taleb T.* UAV-Based IoT Platform: A Crowd Surveillance Use Case // IEEE Communications Magazine. 2017. February. P. 128–134.
16. *Sharma V., Srinivasan K., Chao H.-C.* Intelligent Deployment of UAVs in 5G Heterogeneous Communication Environment for Improved Coverage // Journal of Network and Computer Applications. 2017. Vol. 85, issue C. P. 94–105.
17. *Subramaniam S.K., Nilavalan R., Balachandran W.* Enhancing Pipeline Network Performance Using Dual Interleaving Cluster Head Routing Protocol // International Journal of Computer Science and Network Security. 2017. Vol. 17, № 4. P. 284–291.
18. *Tashakkori H., Rajabifard A., Kalantari M.* Facilitating the 3D Indoor Search and Rescue Problem: An Overview of the Problem and an Ant Colony Solution Approach // ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences: 11th 3D Geoinfo Conference (Athens, Greece, 20–21 October 2016). Vol. IV-2/W1. Athens, 2016. P. 333–240.
19. *Wang A., Ji X., Wu D.* GuideLoc: UAV-Assisted Multitarget Localization System for Disaster Rescue // Hindawi Mobile Information Systems. 2017. March. P. 1–13.

DOI: 10.25586/RNU.V9187.19.04.P.100 УДК 004.056.55:621.389:535.14

А.В. Борисова, А.Е. Жиляев, С.В. Алфёров, В.Л. Елисеев,
Ю.В. Кармазиков, А.Н. Климов, К.А. Балыгин

ИСПЫТАНИЕ КОМПЛЕКСА КВАНТОВОЙ КРИПТОГРАФИЧЕСКОЙ АППАРАТУРЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ГОРОДСКИХ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЯХ СВЯЗИ

Описываются особенности работы на реальных городских линиях комплекса квантовой криптографической аппаратуры защиты информации, разработанного компанией «ИнфоТеКС» совместно с Московским государственным университетом имени М.В. Ломоносова. Система тестировалась как в стабильных внешних условиях, так и при наличии температурного градиента. Отмечено, что изменение температуры с +25 до +18 °С вызвало возрастание квантовых ошибок в два раза и, следовательно, снижение скорости выработки секретных квантовых ключей, но не привело к полной остановке генерации ключей. По результатам испытаний выделены направления развития и способы повышения качества работы комплекса и выработки квантовых ключей.
Ключевые слова: квантовое распределение ключей, квантовая криптография, волоконно-оптические линии связи, защита информации, полевые испытания.

A.V. Borisova, A.E. Zhilyaev, S.V. Alferov, V.L. Eliseev,
Yu.V. Karmazikov, A.N. Klimov, K.A. Balygin

TESTING OF QUANTUM KEY DISTRIBUTION SYSTEM IN URBAN FIBER-OPTIC COMMUNICATION LINES

The features of working on real city lines of a complex of quantum cryptographic information protection equipment, developed by InfoTeCS in conjunction with Lomonosov Moscow State University. The system was tested both in stable external conditions and in the presence of a temperature gradient. It was noted that a temperature change from +25 to +18 °C caused a twofold increase in quantum errors and, consequently, a decrease in the secret key rate, but did not lead to a complete stop of secret key generation. According to test results direction of future work and ways to improve the quality of quantum key distribution system are developed.

Keywords: quantum key distribution, quantum cryptography, fiber-optic communication lines, information security, field test.

Введение

В последние годы технология квантового распределения ключей (КРК) постоянно совершенствуется не только в теории, но и на практике. Так как квантовая криптография позволяет обеспечить высокозащищенную связь между двумя легитимными пользователями [5] с опорой на ограничение возможностей злоумышленника фундаментальными законами физики, особое внимание уделяется физическим реализациям систем, использующих КРК. Устройства КРК уже давно представлены не только в виде лабораторных установок, но и в виде коммерческих моделей, поэтому особенно актуальной задачей является тестирование устойчивости их работы на реальных линиях оптической связи [6; 7; 8; 9; 10; 11; 12]. В настоящей статье демонстрируется работа комплекса квантовой криптографической аппаратуры защиты информации на городских линиях связи в Москве, приводится длина секретного ключа и скорость его выработки при разных условиях эксплуатации.

Состав тестируемого комплекса

В рамках проекта ОАО «ИнфоТеКС» и Московского государственного университета (МГУ) имени М.В. Ломоносова, поддержанного Минобрнауки России (Соглашение от 28 апреля 2017 г. № 075-11-2018-074, внутренний номер договора – № 03.G25.31.0254), был разработан комплекс квантовой криптографической аппаратуры защиты информации. Комплекс обеспечивает передачу защищенной информации по сетям связи общего пользования и включает автоматическую аппаратуру КРК и два идентичных квантово-криптографических шифратора (ККШ). Последние обеспечивают защиту данных пользователей на канальном уровне (L2) на скорости 10 Гбит/с с использованием отечественного криптоалгоритма ГОСТ Р 34.12-2015 «Кузнечик», работающего в совмещенном режиме шифрования и имитозащиты.

Работа комплекса осуществляется по следующему алгоритму:

1. Физический датчик случайных чисел (ФДСЧ) генерирует случайную последовательность, которая используется для кодирования состояний в соответствии с квантовым протоколом.

2. Квазиоднофотонные состояния передаются по квантовому каналу и регистрируются на приемной стороне детектором одиночных фотонов.

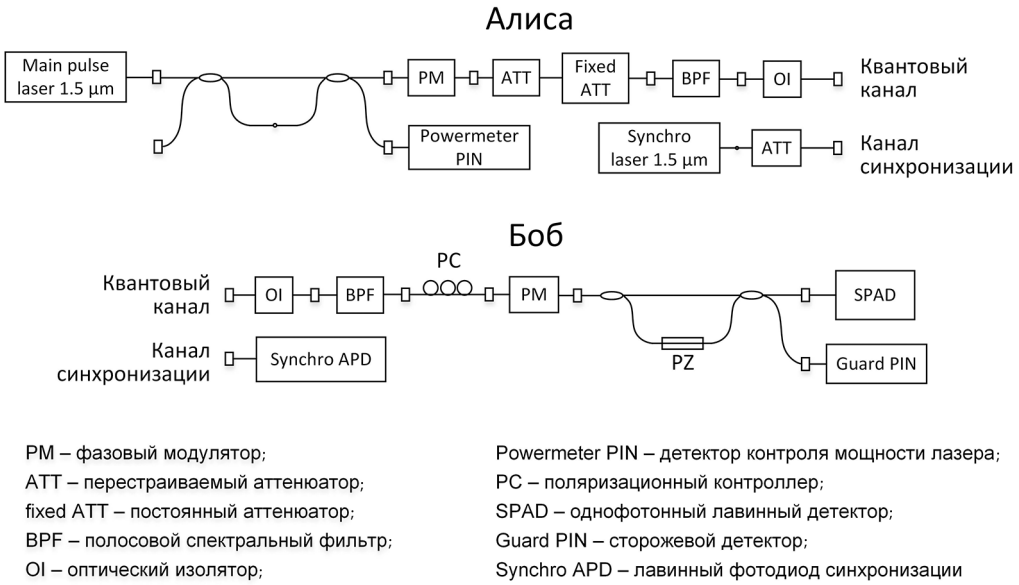
3. Последовательно выполняются процедуры просеивания, очистки и усиления секретности квантовых ключей, в результате чего формируются секретные квантовые ключи (далее – квантовые ключи, или КК), случайность которых проверяется статистическими тестами.

4. ККШ взаимодействует с аппаратурой КРК по разработанному оригинальному протоколу с учетом выработки ресурса ключевой информации при шифровании потока пользовательских данных.

5. Весь пользовательский трафик шифруется ключами, полученными с помощью гибридной ключевой системы с использованием КК.

Подробное описание состава аппаратуры КРК, основных этапов работы, особенностей аутентификации, интерфейса взаимодействия, а также принципа работы физического датчика случайных чисел, входящего в состав аппаратуры КРК, приведены в статьях [1; 2; 3].

Оптическая схема передающей (Алиса) и приемной (Боб) сторон аппаратуры КРК приведена на рисунке 1.



PM – фазовый модулятор;
ATT – перестраиваемый аттенюатор;
fixed ATT – постоянный аттенюатор;
BPF – полосовой спектральный фильтр;
OI – оптический изолятор;
Powermeter PIN – детектор контроля мощности лазера;
PC – поляризационный контроллер;
SPAD – однофотонный лавинный детектор;
Guard PIN – сторожевой детектор;
Synchro APD – лавинный фотодиод синхронизации

Рис. 1. Упрощенные оптические схемы Алисы и Боба

Для реализации фазового кодирования в соответствии с применяемым протоколом на геометрически однородных когерентных состояниях [4] в схемах Алисы и Боба присутствуют интерферометры Маха – Цандера и фазовые модуляторы. Аттенюаторы служат для достижения квазиоднофотонного уровня мощности информационных импульсов. Выравнивание разностей хода интерферометров, крайне чувствительных к изменениям внешних условий, осуществляется пьезоэлементом в интерферометре Боба, управляемым пропорционально-интегрально-дифференциальным (ПИД) регулятором, исполь-

зующим в качестве сигнала ошибки значение относительной разности количества нулей и единиц в просеянном ключе [2].

Работа комплекса в лабораторных условиях

Комплекс прошел предварительные испытания на лабораторной линии длиной 100 км. Целью тестирования была проверка соответствия действительных параметров системы заявленным техническим требованиям. Все оборудование располагалось на столах в одном помещении, в котором поддерживалась комнатная температура. Проведенные измерения показали следующие результаты:

- средняя скорость выработки КК 713,7 бит/мин;
- уровень ошибки QBER 4–5 %;
- скорость генерации случайных чисел в ФДСЧ 21,6 Мбит/с в Алисе и 18,8 Мбит/с в Бобе;
- скорость передачи пользовательских данных 9,7 Гбит/с;
- параметры волоконно-оптической линии: длина 100,912 км, удельные потери 0,18 дБ/км;
- время, затрачиваемое шифратором на обработку пользовательских данных (задержка на шифраторе), 13 мкс;
- среднее число фотонов в информационных импульсах 0,3 фотон/импульс.

Измерения перечисленных параметров проводились во Всероссийском научно-исследовательском институте оптико-физических измерений (ВНИИОФИ) на поверенном измерительном оборудовании.

Испытания на городской линии ПАО «Ростелеком»

Описание площадки и линий

Испытания комплекса осуществлялись на волоконно-оптической линии связи (ВОЛС) и в помещениях, предоставленных ПАО «Ростелеком» (М10 и Сколково). Было задействовано три канала ВОЛС: транспортный, канал синхронизации аппаратуры КРК, канал передачи квантовых состояний (квантовый канал). Длина линии, использованной в качестве квантового канала, составила 57,8 км, а суммарные потери в ней – 18 дБ.

Схема стенда

Для демонстрации работы комплекса был развернут стенд (рис. 2), в состав которого входят:

1) аппаратура КРК в составе Сервера (Алисы) и Клиента (Боба);

2) два ККШ;

3) генераторы трафика (источник и приемник) для имитации потока пользовательских данных;

4) два сервисных ноутбука, один из которых использовался для управления аппаратурой КРК в сервисном режиме (для настройки оборудования), а второй – для управления генераторами трафика и проверки скорости шифрования и передачи;

5) коммутатор (SW), обеспечивающий связность аппаратуры КРК с ККШ и формирующий дополнительный канал управления, необходимый для настройки аппаратуры КРК (переключение в сервисный режим).

Пользовательские данные от источника трафика шифровались в ККШ № 2 с использованием полученного от Клиента КРК квантового ключа и уходили в транспортный канал, после прохождения которого принимались ККШ № 1, расшифровывались с использова-

нием полученного от Сервера КРК квантового ключа и принимались генератором трафика (приемником).

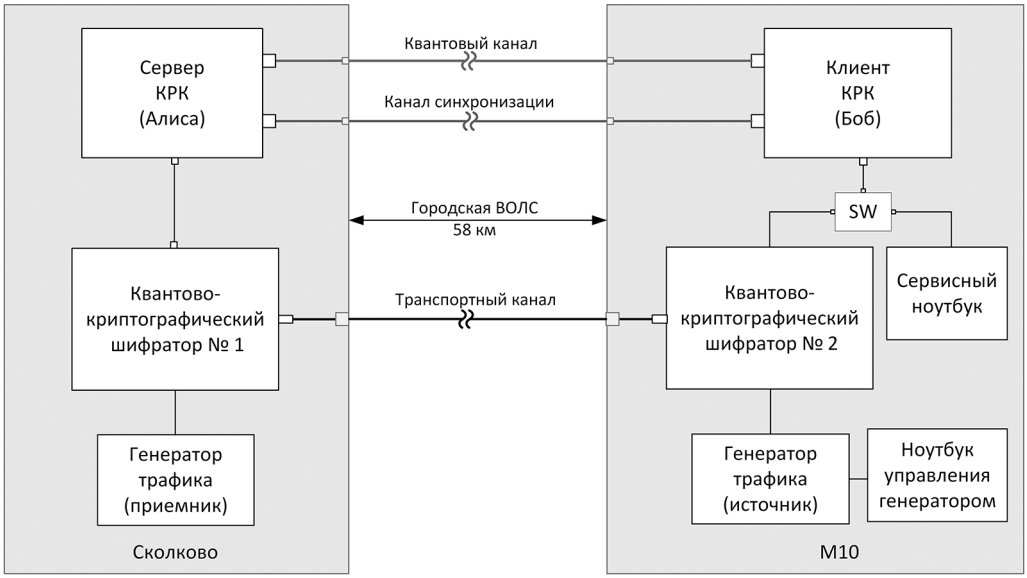


Рис. 2. Схема стенда при испытаниях на городской линии ПАО «Ростелеком»

Порядок проведения испытаний

Суммарно на проведение испытаний затрачено пять дней, четыре из которых заняла подготовка к тестированию: транспортировка и монтаж оборудования, настройка связи, наладка аппаратуры КРК на рабочую ВОЛС и настройка нагрузочных имитаторов трафика. Само испытание проводилось в течение одного дня по предложенной ПАО «Ростелеком» методике, включающей измерение потерь в линии и среднего числа фотонов в квантовом канале, наблюдение коэффициента квантовых ошибок (QBER), измерение скорости генерации КК и скорости передачи трафика по защищенной линии связи.

Описание наблюдений в процессе испытаний

Режим работы аппаратуры КРК определялся следующими основными параметрами:

- среднее число фотонов в информационных импульсах $\mu = 0{,}5$ фотон/импульс;
- частота импульсов в серии 10 МГц;
- длина серии 120 млн импульсов.

Первые 25 минут от начала испытаний КК вырабатывались нестабильно, по мере выхода на более стабильный режим работы средняя скорость выработки КК составила 390 бит/мин (рис. 3).

Скорость выработки КК зависит от уровня квантовых ошибок, так как чем выше уровень ошибки, тем больше значение квантовой утечки и, следовательно, тем большее количество бит требуется вычесть для усиления секретности ключа. QBER зависит от видности интерференции, т.е. от качества балансировки интерферометров.

Первые 20–25 минут испытаний наблюдался высокий уровень QBER – 8–10% (рис. 4-*а*) и низкая видность интерференции – менее 95% (рис. 4-*б*).

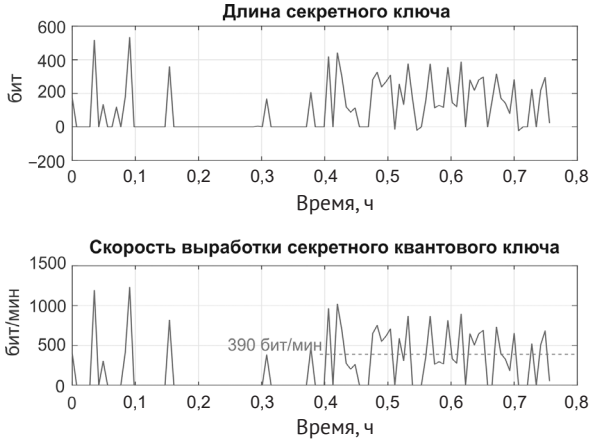


Рис. 3. Длина и скорость выработки секретного квантового ключа в зависимости от времени

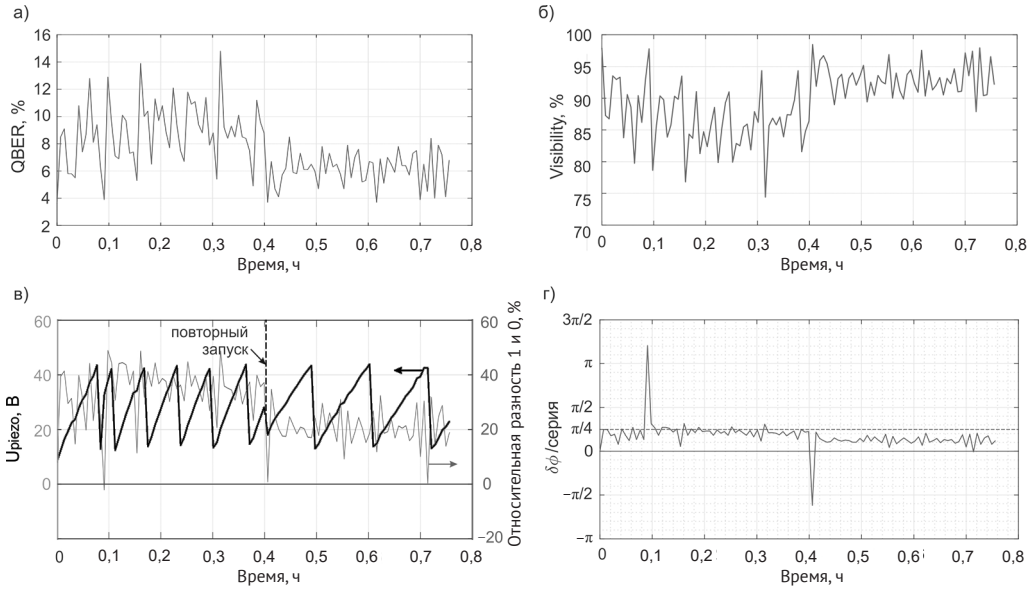


Рис. 4. Временные зависимости:
а – уровня ошибки в просеянном ключе (QBER); *б* – видности интерференционного сигнала; *в* – напряжения на пьезоэлементе и сигнала ошибки ПИД-регулятора (относительная разность количества 0 и 1 в просеяннном ключе); *г* – скорости изменения разности фаз между интерферометрами Алисы и Боба

По пилообразной функции напряжения на пьезоэлементе от времени (рис. 4-*в*, черная линия) можно сделать вывод, что величина расхождения разностей хода интерферометров Алисы и Боба быстро меняется. При скорости изменения разности фаз (рис. 4-*г*) около π/4 QBER держался на высоком уровне – 10–12% и квантовые ключи не вырабатывались. Со временем, когда скорость изменения разности фаз интерферометров снизилась примерно до уровня π/8, скорость роста напряжения на пьезоэлементе (наклон кривой) также снизилась, что привело к уменьшению величины QBER до 6% и началу выработки КК.

Описанное поведение комплекса связано с изменением температуры окружающей среды. В момент начала испытаний температура в помещении, где находилась Алиса, начала изменяться с +18 до +24 °C. Изменение было вызвано переключением режима системы кондиционирования. Так как интерферометры Алисы и Боба располагаются в отдельном термоизолирующем корпусе, то их температура меняется медленнее температуры окружающей среды. На рисунке 5 приведена временная зависимость разности температур интерферометров, при этом на момент запуска температуры считаются равными.

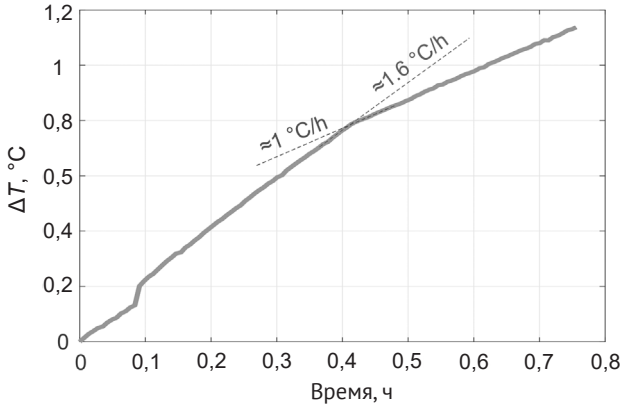


Рис. 5. Изменение разности температур интерферометров Алисы и Боба с течением времени

Таким образом, была исследована реакция системы КРК на некоторое ступенчатое изменение температуры. Поведение параметров КРК говорит о том, что оптическая разность хода интерферометра Боба не успевает подстраиваться под быстро меняющуюся разность хода интерферометра Алисы. Это связано с тем, что ПИД-регулятор является достаточно медленным элементом, а время отстрела одной серии квазиоднофотонных импульсов довольно велико (около 12 с). При этом за время отстрела серии оптические разности хода обоих интерферометров значительно расходятся, что приводит к большой относительной разности количества 0 и 1 в просеянном ключе (см. рис. 4-*в*). Поэтому при резких изменениях температуры и одновременно при длительных сериях ПИД-регулятор не успевает выдавать корректные управляющие сигналы. Для данного режима (10 МГц, 120 млн импульсов в серии) критичным градиентом разности температур внутри интерферометров можно считать 1 °C/ч.

Для повышения качества балансировки интерферометров необходимо уменьшить интервал времени между подстройками ПИД-регулятора, т.е. уменьшить длительность серии путем сокращения ее длины или повышения частоты следования импульсов. Целесообразно изменять длину серии как более гибкий параметр, при этом подстраивая коэффициенты ПИД-регулятора.

Испытания на городской линии ОАО «ИнфоТеКС» – МГУ

Для оценки параметров работы системы КРК в нестабильных условиях окружающей среды необходимо провести сравнение с аналогичными параметрами работы в более устойчивой среде. С этой целью были проведены дополнительные испытания на городской ВОЛС, связывающей здания ОАО «ИнфоТеКС» и МГУ имени М.В. Ломоносова.

Вся аппаратура КРК располагалась в одном помещении (рис. 6). Суммарная длина линии составляет 50 км, потери в линии – 11 дБ.

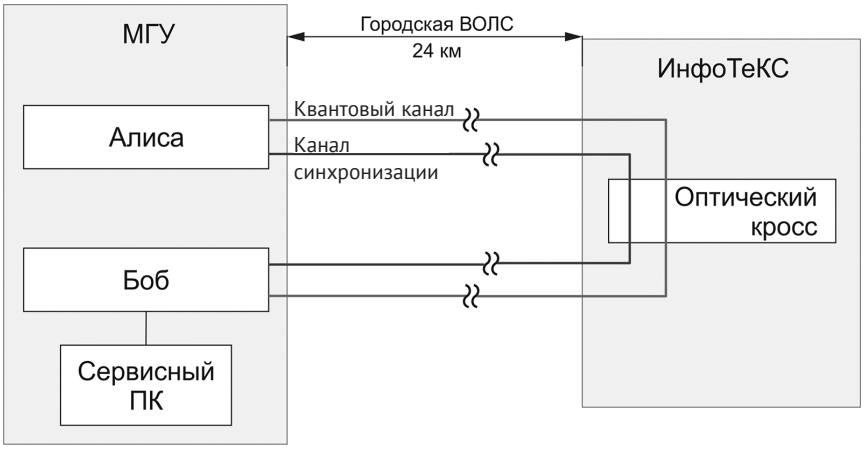


Рис. 6. Схема стенда испытаний на городской линии между МГУ и ОАО «ИнфоТеКС»

Результирующие параметры непрерывной работы системы в течение трех суток показаны на рисунке 7. Уровень QBER лежит в пределах 3–5%, что на 3% ниже ошибки на рисунке 4-*а*. Средняя скорость выработки КК составила около 2300 бит/мин. Провалы скорости совпадают со всплесками QBER и провалами видности интерференции, которые, в свою очередь, соответствуют моментам изменения напряжения пьезоэлемента на величину волнового напряжения.

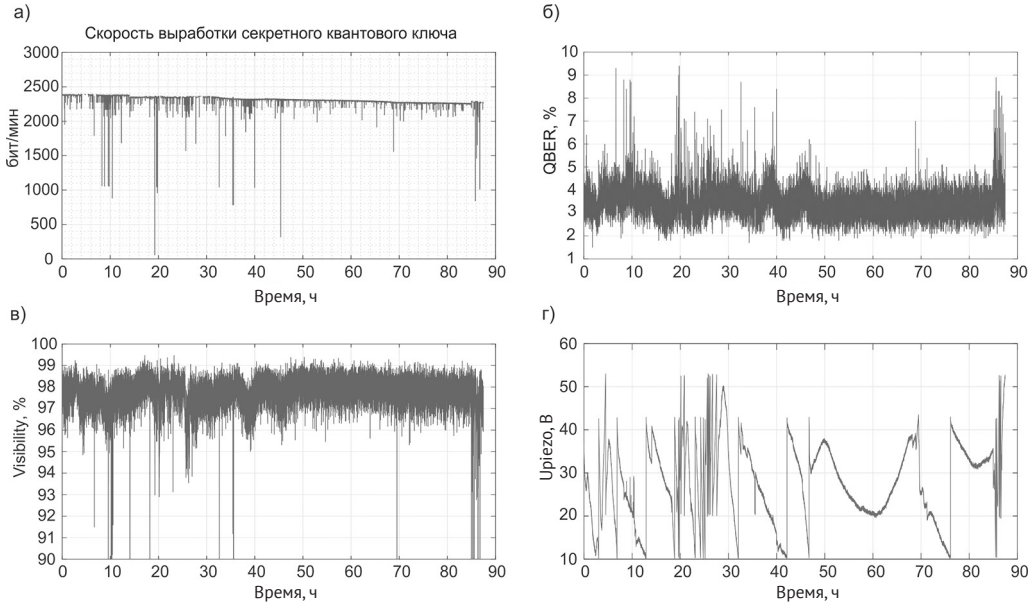


Рис. 7. Основные параметры работы системы КРК как функции времени:
а – скорость выработки квантового ключа; *б* – уровень квантовой ошибки QBER;
в – видность интерференционного сигнала; *г* – напряжение на пьезоэлементе

Результаты испытаний

Обобщая результаты проведенных испытаний, приведем сравнительную таблицу основных параметров работы комплекса квантовой криптографической аппаратуры защиты информации на городских линиях в условиях, приближенных к реальным условиям эксплуатации.

Параметры выработки квантовых ключей

Параметр	Городская ВОЛС 48 км (11 дБ), стабильные внешние условия	Городская ВОЛС 58 км (18,5 дБ), нестабильные внешние условия	100 км (18 дБ), лабораторные условия
Скорость выработки КК, бит/мин	2300	390	713
Уровень QBER, %	3–5	5–8	4–5
Скорость передачи пользовательской информации в транспортном канале данных, Гбит/с	9,7	7 (скорость была ограничена возможностями генераторов трафика)	9,7

Исходя из полученной скорости выработки 390 бит/мин и размера применяемого ключа шифрования ГОСТ Р 34.12-2015 – 256 бит, можно сделать вывод, что к аппаратуре КРК возможно подключить в среднем одну пару шифраторов (потребителей КК) при условии смены КК раз в минуту.

В процессе испытаний выявлена высокая чувствительность аппаратуры КРК к относительному изменению температуры окружающей оборудование среды. Для поддержания стабильной выработки ключей необходимы:

- уменьшение длины серии импульсов;
- увеличение частоты следования импульсов в серии (например, до 100 МГц);
- автоматическая подстройка коэффициентов ПИД-регулятора, управляющего пьезоэлементом, в зависимости от длины серии.

Кроме того, выделены направления развития комплекса и повышения качества его работы:

1. Реализация КРК в одном волокне с использованием спектрального уплотнения каналов (WDM).
2. Реализация автоматической настройки аппаратуры КРК на линию.
3. Исследование возможности применения альтернативных методов и алгоритмов балансировки интерферометров Сервера КРК и Клиента КРК, а также способов их термоизоляции.
4. Интеграция канала синхронизации с классическими каналами линии связи.

Заключение

Проведены испытания опытного образца комплекса квантовой криптографической аппаратуры защиты информации в лабораторных условиях и на реальных городских линиях. При этом даже в нестабильных внешних условиях была продемонстрирована удовлетворительная работоспособность системы. В ходе испытаний в работе аппаратуры выявлены проблемные стороны и по результатам сформулированы направления развития и совершенствования разработанного комплекса.

Авторы выражают благодарность лаборатории метрологии малоинтенсивного лазерного излучения и волоконно-оптических систем ВНИИОФИ за предоставление поверенного измерительного оборудования и помощь в проведении предварительных испытаний и ПАО «Ростелеком» за предоставление городской линии.

Литература

1. *Балыгин К.А. и др.* Активная стабилизация оптической части в волоконной квантовой криптографии // Письма в ЖЭТФ. 2016. Т. 103, № 6. С. 469–474.
2. *Балыгин К.А. и др.* Управление распределенной интерференцией в однопроходной системе квантовой криптографии // Письма ЖЭТФ. 2017. Т. 106, № 2. С. 108–114.
3. *Втюрина А.Г. и др.* Реализация средства криптографической защиты информации, использующего квантовое распределение ключей // Доклады Томского государственного университета систем управления и радиоэлектроники. 2018. Т. 21, № 2. С. 15–21.
4. *Молотков С.Н.* О геометрически однородных когерентных состояниях в квантовой криптографии // Письма в ЖЭТФ. 2012. Т. 95, № 6. С. 361–366.
5. *Bennett Ch.H., Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // Theoretical Computer Science. 2014. Vol. 560, № 12. P. 7–11.
6. *Elliott C. et al.* Current Status of the DARPA Quantum Network // Quantum Information and Computation III. 2005. Vol. 5815. P. 138–149.
7. *Fujiwara M. et al.* Photon Level Crosstalk Between Parallel Fibers Installed in Urban Area // Optics Express. 2010. Т. 18, № 21. P. 22199–22207.
8. *Kiktenko E.O. et al.* Demonstration of a Quantum Key Distribution Network in Urban Fibre-Optic Communication Lines // Quantum Electronics. 2017. Vol. 47, № 9.
9. *Lancho D. et al.* QKD in Standard Optical Telecommunications Networks // International Conference on Quantum Communication and Quantum Networking. Berlin: Springer, 2009. P. 142–149.
10. *Sasaki M. et al.* Field Test of Quantum Key Distribution in the Tokyo QKD Network // Optics Express. 2011. Vol. 19, № 11. P. 10387–10409.
11. *Wang S. et al.* Field and Long-Term Demonstration of a Wide Area Quantum Key Distribution Network // Optics Express. 2014. Vol. 22, № 18. P. 21739–21756.
12. *Xu F.X. et al.* Field Experiment on a Robust Hierarchical Metropolitan Quantum Cryptography Network // Chinese Science Bulletin. 2009. Vol. 54, № 17. P. 2991–2997.

Literatura

1. *Balygin K.A. i dr.* Aktivnaya stabilizatsiya opticheskoj chasti v volokonnoj kvantovoj kriptografii // Pis'ma v ZhETF. 2016. T. 103, № 6. S. 469–474.
2. *Balygin K.A. i dr.* Upravlenie raspredelennoj interferentsiej v odnoprokhodnoj sisteme kvantovoj kriptografii // Pis'ma ZhETF. 2017. T. 106, № 2. S. 108–114.
3. *Vtyurina A.G. i dr.* Realizatsiya sredstva kriptograficheskoj zashchity informatsii, ispol'zuyushchego kvantovoe raspredelenie klyuchej // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. 2018. T. 21, № 2. S. 15–21.
4. *Molotkov S.N.* O geometricheski odnorodnykh kogerentnykh sostoyaniyakh v kvantovoj kriptografii // Pis'ma v ZhETF. 2012. T. 95, № 6. S. 361–366.
5. *Bennett Ch.H., Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // Theoretical Computer Science. 2014. Vol. 560, № 12. P. 7–11.
6. *Elliott C. et al.* Current Status of the DARPA Quantum Network // Quantum Information and Computation III. 2005. Vol. 5815. P. 138–149.

7. *Fujiwara M. et al.* Photon Level Crosstalk Between Parallel Fibers Installed in Urban Area // Optics Express. 2010. T. 18, № 21. P. 22199–22207.
8. *Kiktenko E.O. et al.* Demonstration of a Quantum Key Distribution Network in Urban Fibre-Optic Communication Lines // Quantum Electronics. 2017. Vol. 47, № 9.
9. *Lancho D. et al.* QKD in Standard Optical Telecommunications Networks // International Conference on Quantum Communication and Quantum Networking. Berlin: Springer, 2009. P. 142–149.
10. *Sasaki M. et al.* Field Test of Quantum Key Distribution in the Tokyo QKD Network // Optics Express. 2011. Vol. 19, № 11. P. 10387–10409.
11. *Wang S. et al.* Field and Long-Term Demonstration of a Wide Area Quantum Key Distribution Network // Optics Express. 2014. Vol. 22, № 18. P. 21739–21756.
12. *Xu F.X. et al.* Field Experiment on a Robust Hierarchical Metropolitan Quantum Cryptography Network // Chinese Science Bulletin. 2009. Vol. 54, № 17. P. 2991–2997.