

09.7

Возможность построения модульной системы квантового распределения ключей в атмосфере

© А.А. Боев¹, С.С. Воробей², С.Ю. Казанцев³, М.Ю. Керносов¹, О.В. Колесников³,
С.Н. Кузнецов¹, Ю.Б. Миронов³, А.А. Паршин¹, Н.В. Рудавин²

¹ АО „Мостком“, Рязань, Россия

² ООО „КуРЭйт“, Сколково, Россия

³ Московский технический университет связи и информатики, Москва, Россия

E-mail: s.i.kazantsev@mtuci.ru

Поступило в Редакцию 17 марта 2022 г.

В окончательной редакции 9 июня 2022 г.

Принято к публикации 15 июня 2022 г.

Экспериментально показана возможность квантового распределения ключей в атмосфере посредством сопряжения выпускаемых серийно блоков квантового распределения ключей, разработанных для волоконно-оптических линий связи, с терминалами атмосферной оптической связи. Для дистанций до 3100 м получены данные о потерях в квантовом канале на оптической трассе и исследовано влияние систем интеллектуальной подстройки терминалов атмосферной связи на систему синхронизации блоков квантовой связи. Установлено, что сбои систем синхронизации при квантовом распределении ключей в атмосфере на дистанциях более 10 м обусловлены особенностями алгоритма, реализованного в блоке квантовой связи.

Ключевые слова: квантовое распределение ключей, атмосферные оптические линии связи, протокол decoy-state BB84, поляризационное кодирование.

DOI: 10.21883/PJTF.2022.15.53125.19192

В последнее время интенсивно создаются и исследуются системы квантового распределения ключа (КРК) [1,2]. Технологии КРК на физическом уровне гарантируют безопасность передачи информации, а возможность утечки данных может быть связана лишь с несовершенством конкретной реализации технологии [3,4]. Сегодня достигнуты значительные успехи в разработке серийных устройств для КРК в волоконно-оптических линиях связи (ВОЛС) [5], а установки КРК в атмосфере пока находятся на стадии демонстрационных макетов [6]. При этом терминалы для атмосферных оптических линий связи (АОЛС) уже давно доказали свою эффективность для передачи больших объемов данных [7,8]. Целью настоящей работы является анализ технической возможности построения надежных устройств КРК в атмосфере за счет сопряжения представленных на рынке модулей КРК для ВОЛС и терминалов АОЛС.

Для проведения исследований были выбраны терминалы АОЛС M1-40GE компании АО „Мостком“ [9] и блоки КРК QKD312 компании ООО „КуРЭйт“ [10]. Выбранное оборудование АОЛС позволяет с минимальными трудозатратами создавать беспроводный канал связи точка–точка и обеспечивает параллельную передачу потоков данных через интерфейсы 10GBASE(SFP+) [9]. Передача информационных сигналов терминалом АОЛС осуществляется на длинах волн 1535–1560 nm, также в нем используется лазер на длине волны 785 nm для организации служебного канала между терминалами [8].

Известно, что для КРК необходимо иметь два канала связи, первый из которых является открытым

и осуществляется штатным подключением терминалов АОЛС, описанным выше, а второй квантовый [2]. Квантовый канал связи служит для приема и передачи информации, переносимой одиночными фотонами, обычно в открытом пространстве ее кодируют поляризацией одиночного фотона [11]. Проблема создания истинных источников одиночных фотонов, соответствующих требованиям телекоммуникационной индустрии, пока не решена, поэтому в коммерческих блоках КРК применяются ослабленные лазерные импульсы [12]. Для организации квантового канала связи использовались блоки QKD312, в которых передача криптографического ключа осуществляется с использованием модифицированного протокола decoy-state BB84, а информация кодировалась поляризацией фотона [10]. Блок QKD312 был разработан для ВОЛС без сохранения поляризации, поскольку в этом блоке КРК используются специальные алгоритмы интеллектуальной настройки системы синхронизации квантового канала связи при изменении поляризации волокна [5,10]. В нашем эксперименте оптические блоки терминалов АОЛС устанавливались на крышах разных зданий так, чтобы они находились в зоне прямой видимости и были сориентированы друг на друга. Блоки КРК одномодовым оптоволоконным подключались к блокам интерфейсов терминалов АОЛС. Полная схема соединений в экспериментальном оборудовании приведена на рис. 1, на котором показаны информационный канал (IC), квантовый канал (QC), тестовый канал (TC). Возможность реализации квантового канала связи через терминалы АОЛС M1-40GE обусловлена тем, что архи-

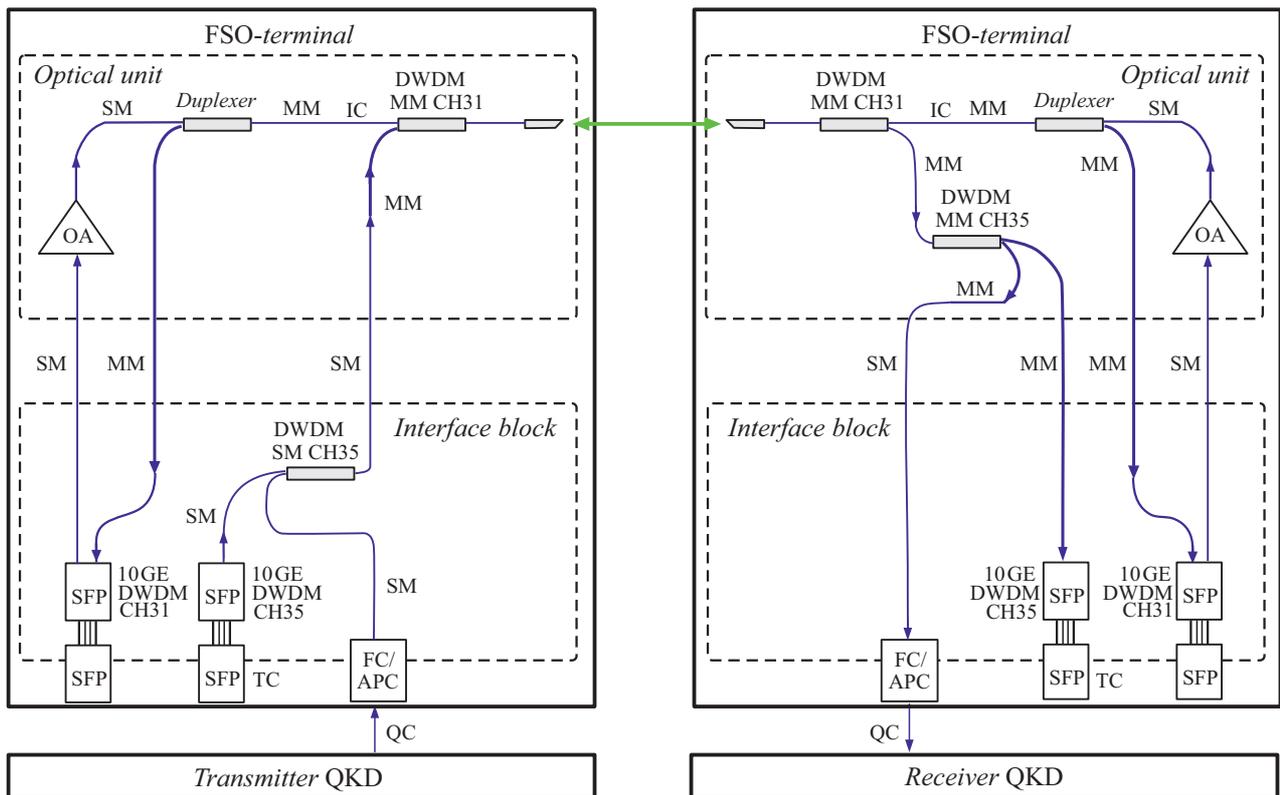


Рис. 1. Схема подключения оборудования АОЛС к блокам КРК. IC — информационный канал, QC — квантовый канал, TC — тестовый канал.

текстура данного оборудования позволяет организовать „прозрачный“ канал связи под задачи КРК без изменения конструкции, работая по принципу passive optics-active tracking, поэтому передача информационного сигнала через АОЛС осуществляется с минимумом преобразований, используется только активная система наведения. Информационные сигналы от оборудования поступают на блок интерфейсов АОЛС, который передает их в оптический блок терминала через интерфейсный кабель. Для анализа влияния пропускания атмосферы на квантовый канал (длина волны 1554.9 nm) между терминалами был организован отдельный тестовый канал связи на длине волны 1549.3 nm (35-й канал в сетке ITU DWDM с интервалом 100 GHz). Со стороны приемника КРК в приемном модуле АОЛС данный канал был подключен к приемнику, который измерял уровень принимаемой мощности P_{35} . Поскольку квантовый и тестовый каналы связи были мультиплексированы по DWDM-технологии и проходили по одному и тому же пути между терминалами, P_{35} использовался для оценки уровня потерь в квантовом канале. Одной из задач настоящей работы являлось исследование влияния активной системы наведения терминала АОЛС на синхронизацию блоков КРК. С этой целью на осциллографе Teledyne LeCroy WaveRunner 620zi, подключенном к служебным выходам блока приемника КРК, анализировались импульсы синхронизации квантового канала связи при различных

режимах работы терминалов АОЛС. Точность осциллографических измерений была не хуже 8%.

На рис. 2 показана зависимость мощности сигнала P_{35} на приемном модуле терминала АОЛС от времени для трасс длиной 3100 и 180 m. Для дистанции 3100 m видны сильные флуктуации мощности сигнала P_{35} , поскольку на пути трассы во время сеанса связи стоял густой смог от котельных, в результате этого максимальная длительность устойчивой связи, когда величина P_{35} превышала $1 \mu\text{W}$, за сеанс измерений составила всего 21 s. Максимальное значение P_{35} достигало $15 \mu\text{W}$, что при выходной мощности передатчика $1300 \mu\text{W}$ позволяет оценить минимально достижимые потери в канале синхронизации как 19 dB. С учетом геометрических потерь на данной трассе они составляют 15 dB, это хорошо согласуется с прямыми измерениями потерь в канале синхронизации, возникающих при сопряжении блока КРК с терминалом АОЛС (4.6 dB). С учетом перехода многомодовое волокно—одномодовое волокно (MM—SM) потери квантового канала превышают 34 dB. При уровне потерь в квантовом канале более 26 dB передача криптографического ключа производителем QKD312 была не предусмотрена, поэтому большая часть измерений выполнялась на дистанции 180 m. Эти исследования также проводились при неблагоприятных погодных условиях, при воздействии снегопада и ветра. Как видно из рис. 2, уровень P_{35} для дистанции 180 m за

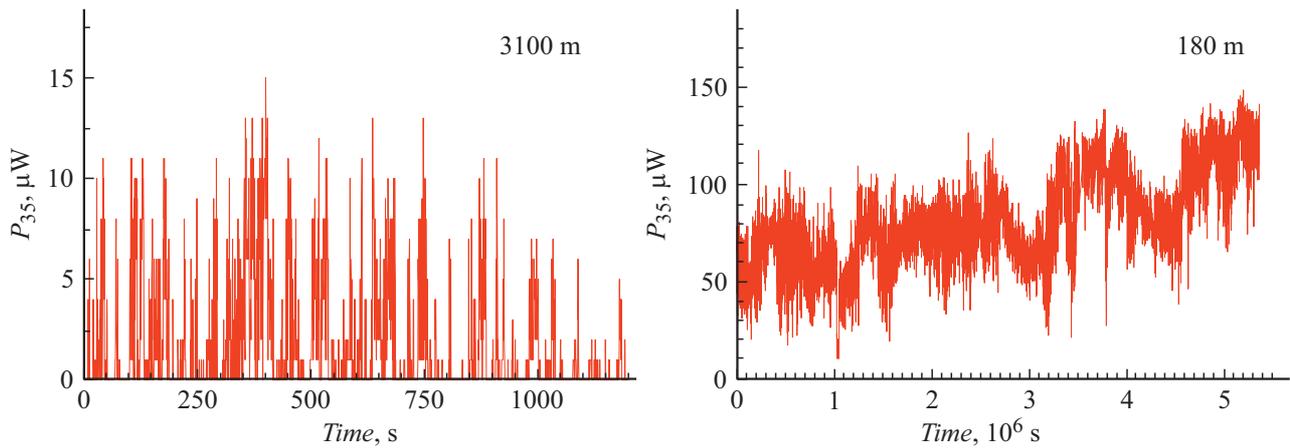


Рис. 2. Динамика мощности на приемнике терминала P_{35} на дистанциях 3100 и 180 м.

все время измерений не падал до нуля. Тренд среднего значения обусловлен изменением ослабления снегопада во время измерений. Анализ динамики мощности сигнала, регистрируемого приемником АОЛС на трассе длиной 180 м, показал, что минимально достижимые потери в канале синхронизации (без учета перехода ММ–SM) составляют 11 dB. Это значение при учете потерь 15 dB на участке сопряжения ММ–SM уже позволяет работать блокам КРК. На рис. 3 показаны типичные осциллограммы сигнальных импульсов канала синхронизации, полученные на блоке КРК. Сигналы записывались по двум каналам: 1 — сигнал детектора приемника, выработанный приемным блоком КРК по сигналу с выходного стыка квантового канала приемного терминала АОЛС; 2 — сигнал-триггер, повторяющий временной цикл работы установки КРК (начало цикла этого сигнала определяется концом детектированной пачки синхроимпульсов). Длительность пачки синхроимпульсов, выдаваемых детектором приемника КРК, составляла $16 \mu\text{s}$, а период следования пачек $\sim 3.4 \text{ ms}$. Указанные длительности полностью соответствуют параметрам излучателя канала синхронизации передающего блока КРК [10]. В процессе исследований проверялась работа АОЛС в штатном режиме, затем в режиме ручного управления отключались системы автонаведения терминалов АОЛС, регулировалась мощность излучения в служебном и информационном каналах терминалов. Отключение системы автоматической подстройки на время измерений не оказывает вредного влияния на работу синхронизации квантового канала связи. Изменение мощности лазера служебного канала (на длине волны 785 nm) в рабочем диапазоне не оказывало влияния на синхронизацию в квантовом канале. Единственным фактором, влияющим на систему синхронизации со стороны АОЛС, оказалась выходная мощность информационного канала терминала со стороны передающего блока КРК. При выходной мощности 80 mW наблюдалось устойчивое отсутствие синхроимпульсов на приемном блоке КРК. В ходе тестов периодически происходил срыв синхронизации,

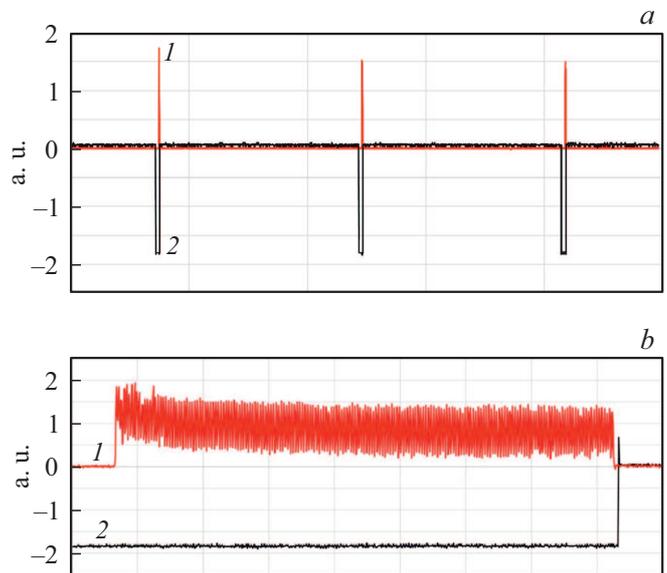


Рис. 3. Осциллограммы сигнала синхронизации, полученные на блоке КРК. 1 — сигнал детектора приемника, 2 — сигнал-триггер, повторяющий временной цикл работы установки КРК. *a* — развертка 2 ms/div, *b* — 1 μs /div.

а после срыва синхронизации в течение нескольких минут наблюдались явно выраженные отсчеты детектора квантового канала при отсутствии сигнала временного цикла блока приема КРК. Это связано с тем, что система синхронизации блоков КРК разрабатывалась в расчете на компенсацию влияния температурных воздействий на ВОЛС, вследствие которых изменяется поляризация излучения, распространяющегося в ВОЛС. Атмосфера не вносит заметных искажений в поляризацию фотонов, а изменения уровня сигнала обусловлены флуктуацией потерь в атмосферном канале, поэтому требуется доработка алгоритма синхронизации КРК.

Таким образом, в работе впервые продемонстрирована возможность построения системы КРК в атмосфере на

основе модульного принципа, когда сопрягаются серийно производимые терминалы АОЛС и блоки КРК, разработанные для ВОЛС. В реальных условиях городской атмосферы исследованы основные факторы, влияющие на работу систем синхронизации квантового канала связи. Выявлены главные причины потери синхронизации квантового канала связи, заключающиеся в высоком уровне потерь на участке сопряжения ММ–SM терминалов АОЛС с блоком КРК и в особенностях применяемых алгоритмов автоматической подстройки в блоке КРК. Устранение выявленных участков сопряжения, вносящих дополнительные потери в квантовый канал, и адаптация алгоритмов блока КРК под условия атмосферной трассы позволят разработать эффективные атмосферные системы КРК, которые могут применяться в самых разных приложениях [8].

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Список литературы

- [1] V. Martin, J.P. Brito, C. Escribano, M. Menchetti, C. White, A. Lord, D. López, EPJ Quantum Technol., **8** (1), 19 (2021). DOI: 10.1140/epjqt/s40507-021-00108-9
- [2] А.Ю. Быковский, И.Н. Компанец, Квантовая электроника, **48** (9), 777 (2018). [A.Y. Bykovsky, I.N. Kompanets, Quantum Electron., **48** (9), 777 (2018). DOI: 10.1070/QEL16732].
- [3] V. Makarov, D.R. Hjelme, J. Mod. Opt., **52** (5), 691 (2005). DOI: 10.1080/09500340410001730986
- [4] А.В. Борисова, Б.Д. Гармаев, И.Б. Бобров, С.С. Негодяев, И.В. Синильщиков, Оптика и спектроскопия, **128** (11), 1758 (2020). DOI: 10.21883/OS.2020.11.50182.4-20 [A.V. Borisova, B.D. Garmaev, I.B. Bobrov, S.S. Negodyaev, I.V. Sinil'shchikov, Opt. Spectrosc., **128** (11), 1892 (2020). DOI: 10.1134/S0030400X20110077].
- [5] Е.О. Киктенко, Н.О. Пожар, А.В. Дуплинский, А.А. Канапин, А.С. Соколов, С.С. Воробей, А.В. Миллер, В.Е. Устимчик, М.Н. Ануфриев, А.С. Трушечкин, Р.Р. Юнусов, В.Л. Курочкин, Ю.В. Курочкин, А.К. Федоров, Квантовая электроника, **47** (9), 798 (2017). [E.O. Kiktenko, N.O. Pozhar, A.V. Duplinskiy, A.A. Kanapin, A.S. Sokolov, S.S. Vorobey, A.V. Miller, V.E. Ustimchik, M.N. Anufriev, A.T. Trushechkin, R.R. Yunusov, V.L. Kurochkin, Yu.V. Kurochkin, A.K. Fedorov, Quantum Electron., **47** (9), 798 (2017). DOI: 10.1070/QEL16469].
- [6] H. Zhao, M.-S. Alouini, IEEE Trans. Commun., **69** (1), 429 (2021). DOI: 10.1109/TCOMM.2020.3030250
- [7] A.V. Raj, A.K. Majumder, IET Commun., **13** (16), 2405 (2019). DOI: 10.1049/iet-com.2019.0051
- [8] Е.Г. Чуляева, С.Н. Кузнецов, Б.И. Огнев, Науч.-техн. ведомости СПбГПУ. Физ.-мат. науки, **11** (1), 66 (2018). DOI: 10.18721/JPM.111107
- [9] <http://www.moctkom.ru/optical-ground-stations/>
- [10] A.V. Duplinskiy, E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, R.P. Ermakov, A.I. Kotov, A.V. Brodskiy, R.R. Yunusov, V.L. Kurochkin, A.K. Fedorov, Y.V. Kurochkin, J. Russ. Laser Res., **39** (2), 113 (2018). DOI: 10.1007/s10946-018-9697-1
- [11] D. Elser, T. Bartley, B. Heim, C. Wittmann, D. Sych, G. Leuchs, New J. Phys., **11** (4), 045014 (2009). DOI: 10.1088/1367-2630/11/4/045014
- [12] Ю.Б. Миронов, С.Ю. Казанцев, Р.А. Шаховой, О.В. Колесников, Л.С. Машковцева, А.И. Зайцев, А.В. Коробов, Научные технологии в космических исследованиях Земли, **13** (6), 22 (2021). DOI: 10.36724/2409-5419-2021-13-6-22-33