17. *Klyushnikov V.Yu.* Sindrom Kesslera: budet li zakryta doroga v kosmos? [Kessler syndrome: will the road to space be closed?], *VKS* [Aerospace sphere], 2021, No. 4 (109). Available at: https://cyberleninka.ru/article/n/sindrom-kesslera-budet-li-zakryta-doroga-v-kosmos (accessed 25 October 2024).
18. *Dzyuba A.P.* Perspektivy razvitiya fazirovannykh antennykh reshetok [Prospects for the development of phased antenna arrays], *Vestnik DGTU. Tekhnicheskie nauki* [Bulletin of DSTU. Technical sciences], 2013, No. 3. Available at: https://cyberleninka.ru/article/n/perspektivy-razvitiya-fazirovannyh-antennyh-reshetok (accessed 25 October 2024).
19. *Listvin A.V, Listvin V.N.* Reflektometriya opticheskikh volokon [Reflectometry of optical fibers]. Moscow: LESARart, 2005, 208 p.
20. *Aleshin V.S., Dogaev S.G.* Zaderzhki rasprostraneniya signalov v setyakh sputnikovoy svyazi [Signal propagation delays in satellite communication networks], *T-Comm,* 2019, No. 5. Available at: https://cyberleninka.ru/article/n/zaderzhki-rasprostraneniya-signalov-v-setyah-sputnikovoy-svyazi (accessed 27 October 2024).

Статью рекомендовал к опубликованию д.т.н., профессор И.И. Турулин.

Левин Илья Израилевич – Южный федеральный университет; e-mail: levin@superevm.ru; г. Таганрог, Россия; тел.: +78634612111; кафедра интеллектуальных и многопроцессорных систем, зав. кафедрой интеллектуальных и многопроцессорных систем; д.т.н.; профессор.

Буряков Дмитрий Сергеевич – e-mail: dburiakov@sfedu.ru; тел.: +79198955502; аспирант.

Levin Ilya Izrailevich – Southern Federal University; e-mail: levin@superevm.ru; Taganrog, Russia; phone: +78634612111; the Department of Intelligent and Multiprocessor Systems; head of Department; dr. of eng. sc.; professor.

Buryakov Dmitrii Sergeevich – e-mail: dburiakov@sfedu.ru; phone: +79198955502; postgraduate student.

УДК 621.396.624 DOI 10.18522/2311-3103-2024-5-254-260

А.П. Плёнкин

СПОСОБ ОБНАРУЖЕНИЯ ОПТИЧЕСКОГО СИГНАЛА В КВАНТОВЫХ СЕТЯХ

Приводится способ обнаружения оптического сигнала синхронизации для участка сети квантовых коммуникаций. Целью статьи является представление варианта реализации городской квантовой сети. В работе рассматривается решение задачи конфигурации канала синхронизации для систем квантовой связи нестандартной топологии. Описывается обобщенный принцип работы системы квантового распределения ключей с фазовым кодированием. Предлагается алгоритм синхронизации, адаптированный для конфигурации городской квантовой сети, содержащей несколько сегментов. Особенностью предлагаемой схемы является наличие одной приемо-передающей станции, с которой взаимодействуют несколько кодирующих станций. В статье приведены результаты анализа энергетической модели предлагаемого способа и расчет усредненных потерь в квантовом канале. В заключении мы рассуждаем о возможных вариантах структуры квантовых сетей и о применимости в них процессов синхронизации. Сети квантовых коммуникаций активно масштабируются и используют различные протоколы квантового распределения ключей, аутентификации и синхронизации. Квантовое распределение ключей (КРК) решает центральную проблему симметричной криптографии и представляет собой безопасную технологию генерации идентичной последовательности бит у двух удаленных пользователей. Теоретически, безопасность (стойкость) такой технологии не зависит от вычислительной мощности взломщиков, которые, например, могут обладать квантовым компьютером. Тем не менее, практическая реализация теоретических моделей все еще показывает техническое несовершенство, что позволяет злоумышленникам находить уязвимости. При исследовании и проектировании различных модификаций систем квантового распределения ключей (СКРК), необходимо уделять внимание не только вопросам стойкости квантовых протоколов, но и компонентам технической реализации аппаратуры.

Квантовые коммуникации; квантовый ключ; фотонный импульс; вероятность обнаружения; доверенные узлы.

A.P. Pljonkin

METHOD FOR DETECTING OPTICAL SIGNAL IN QUANTUM NETWORKS

The article presents a method for detecting an optical synchronization signal for a section of a quantum communications network. The objective of the article is to present a variant of implementing an urban quantum network. The paper considers a proposed solution to the problem of configuring a synchronization channel for quantum communication systems with a non-standard topology. A generalized operating principle of a quantum key distribution system with phase coding is described. A synchronization algorithm adapted for configuring an urban quantum network containing several segments is proposed. A feature of the proposed scheme is the presence of one receiving and transmitting station with which several coding stations interact. The article presents the results of analyzing the energy model of the proposed method and calculating the average losses in the quantum channel. In conclusion, we discuss possible variants of the structure of quantum networks and the applicability of synchronization processes in them. Quantum communications networks are actively scaling and use various quantum key distribution, authentication, and synchronization protocols. Quantum key distribution (QKD) solves the central problem of symmetric cryptography and is a secure technology for generating an identical bit sequence for two remote users. Theoretically, the security (resistance) of such technology does not depend on the computing power of hackers, who, for example, may have a quantum computer. However, the practical implementation of theoretical models still shows technical imperfection, which allows attackers to find vulnerabilities. When researching and designing various modifications of quantum key distribution systems (QKDS), it is necessary to pay attention not only to the issues of the stability of quantum protocols, but also to the components of the technical implementation of the equipment.

Quantum communications; quantum key; photon pulse; detection probability; trusted nodes.

Введение. В сетях квантовых коммуникаций базовой конфигурацией является топология «точка-точка», при которой квантовые секретные ключи распределяются между двумя удаленными узлами. Ограничения такой топологии заключаются, в том числе, возможным предельным расстоянием. Максимальное эффективное расстояние связано с особенностями функционирования квантовых протоколов. В подавляющем большинстве для работы протоколов квантового распределения ключей требуются ослабленные до однофотонного уровня оптические сигналы. Протяженные волоконно-оптические линии связи вносят существенное затухание и не позволяют передавать слабый оптический сигнал на большие расстояния без усиления. Смешанные топологии квантово-криптографических сетей сегодня построены на масштабировании базовой конфигурации и требуют наличия общего ключа между любой парой узлов, в том числе тех, которые не связаны непосредственно квантовым каналом связи. Задача распределения секретных ключей решается применением доверенных промежуточных узлов (ДПУ), через которые по цепочке передаются ключи к необходимым нодам сети. В Китае по такому принципу построена сложная квантовая сеть, охватывающая десятки городов и имеющая протяженность в тысячи километров [1]. В России также используют подход с ДПУ при построении сетей квантовых коммуникаций. Конструктивно ДПУ представляет собой безопасное помещение с оборудованием квантовой криптографией. В большинстве действующих протоколах квантового распределения ключей секретная последовательность формируется путем срабатывания нескольких лавинных фотодиодов (ЛФД) [2–4]. Например, срабатывание одного ЛФД интерпретируется как «0», а срабатывание другого как «1». Технической задачей при проектировании ДПУ является запрет доступа злоумышленника к оборудованию КРК, так как доступ к ЛФД позволит получить необходимую информацию о квантовой последовательности.

Известны модификации систем КРК, которые позволяют вынести ЛФД в отдельное неконтролируемое пространство. Исследования показывают, что в этом случае злоумышленник может иметь полный доступ к детекторам и это не влияет на секретность квантового протокола. Подобная модификация может быть применима лишь в отдельно взятых случаях, так как доступ к системе КРК все равно должен быть ограничен. В последнее десятилетие активно исследуются методы КРК на перепутанных парах фотонов (TF QKD) и с недоверенными промежуточными узлами (НПУ). В таких недоверенных

узлах допускается, что злоумышленник обладает всей информацией о работе аппаратуры, включая работу ЛФД. Система квантовой связи с НДУ базируется на топологии «точка-точка» с центральной недоверенной нодой. Квантовое распределение в такой сети реализуется по протоколу MDI (Measurement Device Independent).

В работе [5] описывается доказательство стойкости протокола MDI, принцип которого схож с известным BB84. Отправитель и получатель равновероятно выбирают один из базисов. Эта процедура происходит независимо друг от друга. Далее аналогично происходит выбор ортогонального состояния и присваиваются значения 0 и 1. Состояния поступают на НДУ, где производятся измерения в неполном Белловском базисе [6, 7]. Отметим, что результаты измерений на недоверенном узле общедоступны. Далее посылки, в которых использованы разные базисы, отбрасываются, а респонденты производят операции инвертации бит. В такой схеме требуется оценка вероятности ошибки, которая позволяет определить величину утечки информации к нарушителю.

Подготовительные процессы КРК. Работа квантового протокола является одной из финальных стадий в операциях систем КРК, функционирование которых невозможно без предварительных процедур настройки и согласования. Квантовые сети в базовой топологии «точка-точка» содержат три канала связи между отправителем и получателем: квантовый, синхронизации, общедоступный. Квантовый канал – это оптический тракт (оптическое волокно или оптический атмосферный канал), по которому реализуется работа квантового протокола. Канал синхронизации (или калибровки) – в большинстве случаев это отдельный волоконно-оптический канал для согласования и периодической подстройки компонентов системы КРК. Квантовый канал и синхронизация могут быть совмещены, т.е. физически реализованы в одном оптическом волокне [8]. Общедоступный канал – это сеть передачи данных, по которой осуществляются процессы аутентификации, шифрования, дешифрования.

Сегодня существует множество реализаций систем КРК, но принцип действия и ряд компонентов у всех схожий. Как правило, всегда есть ЛФД, источник оптического излучения, интерферометры, фазовые модуляторы, поляризационные фильтры. Рассмотрим двухпроходную схему реализации СКРК, в которой оптические ЛФД, источник излучения и интерферометр Маха-Цендера расположены в одной станции (Алиса) [9]. В такой системе станции Алиса и Боб соединены одним оптическим волокном, по которому реализуется синхронизация и работа квантового протокола. Удобство такой схемы заключается в том, что все технологически сложные элементы расположены в одном модуле (корпусе). При построении квантовых сетей такая конфигурация может быть востребована, когда требуется распределять ключи между базовой станцией и пользователями (рис. 1). В подобных схемах наиболее эффективным является использование квантового протокола BB84 и его модификаций с фазовым или поляризационным кодированием.

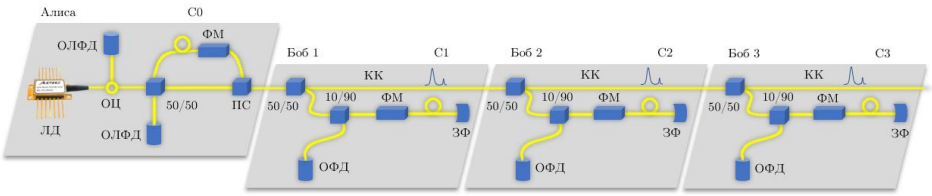

Рис. 1. Схема сети квантовых коммуникаций

Предположим, что в нашем распоряжении есть «темное» оптическое волокно, расположенное вдоль всех сегментов сети. Такое волокно служит как для передачи квантовых сигналов (КК), так и для синхронизации. Перед началом работы и в процессе функционирования квантового протокола системе КРК необходима калибровка. Так как схема двухпроходная, то оптическим сигналам необходимо пройти путь от источника излучения (ЛД) до вращающего поляризацию зеркала Фарадея (ЗФ) и обратно в станцию Алиса к ОЛФД. Отметим, что практическая реализация двухпроходной схемы имеет сущест-

венные ограничения по расстоянию, но вполне применима для городских задач с дистанцией в 50-70 км. Рассмотрим процесс калибровки, задача которого заключается в определении точного расстояния от ЛД до фазового модулятора и ОЛФД. Системе КРК необходимо понимать, в какой момент времени прикладывать электрическое напряжение к ФМ (Боб 1) и в какой момент времени подавать сигнал на ОЛФД. Наиболее распространенный процесс измерения расстояния через обнаружение оптического синхросигнала описан в [10]. В двухпроходных системах КРК данный метод применяется с небольшими модификациями.

Периодическая последовательность оптических импульсов (*1550 нм*) следует на делитель мощности (50/50) через циркулятор (ОЦ) и распределяется по плечам интерферометра. Каждый импульс последовательности разделяется на два с временной задержкой, равной длине отрезка волокна перед фазовым модулятором (ФМ) в плече интерферометра. Далее поляризационный сплиттер направляет сигналы в квантовый канал. По достижению первого сегмента квантовой сети, часть каждого импульса отводится через делитель мощности в станцию Боб 1. Здесь, пройдя ряд волоконно-оптических элементов, сигналы фиксируются классическим детектором (ОФД) и отражаются от ЗФ, изменяя поляризацию на ортогональную. При обратном распространении синхросигналы интерферируют на светоделителе и фиксируются ОЛФД.

Часть сигналов минует сегмент «Боб 1» и направляется по каналу к следующему сегменту «Боб 2», где происходит подобная (как в Боб 1) операция с последовательностью импульсов. Аналогичный процесс применим к последующим сегментам. Так как в процессе синхронизации ОЛФД работают в линейном режиме, то им не требуется время для восстановления работоспособности после детектирования. При расчете числа сегментов сети следует учитывать максимальный период следования импульсов таким образом, чтобы отраженный в последнем модуле оптический синхроимпульс мог вернуться в станцию отправителя и не пересечься по пути с встречным импульсом. В реализованных система КРК период следования тактовых импульсов равен *1.2 мс*. Такой период рассчитан, исходя из максимально возможного расстояния между удаленными станциями (рис. 2).

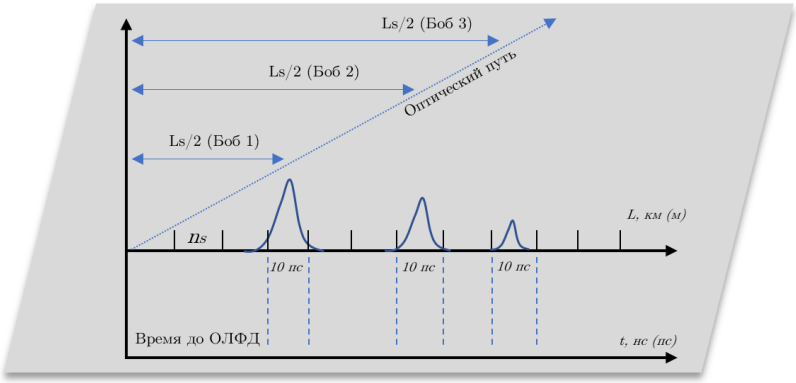

Рис. 2. Пространственно-временной поиск оптического сигнала

Обнаружение оптического синхросигнала осуществляется последовательным анализом временных интервалов *ns.* После каждой посылки импульса ОЛФД станции Алиса настраиваются на приём сигнала через заданные временные интервалы. Результаты срабатываний фиксируются. Детально процесс обнаружения для топологии «точка-точка» описан в работах [8, 9]. В нашем случае (рис. 1) результатом синхронизации будут считаться обнаруженные сигнальные интервалы и их интерпретация во временные данные. Так, станция Алиса будет знать в какой момент времени необходимо активировать ОЛФД для каждого сегмента (С1, С2 и С3 на рис. 1), а электроника станций Боб 1, Боб 2, Боб 3 будет обладать информацией в какой момент времени прикладывать напряжение на ФМ. Отличительной особенностью описываемой схемы является наличие трех вре-

менных интервалов и трех пространственных отрезков, соответствующих расстояниям до сегментов Боб 1 – Боб 3. *Технически мы не видим препятствий использования одной базовой станции (одного ЛД и двух ОЛФД) для осуществления синхронизации с тремя удаленными станциями. Естественно, с точки зрения работы квантового протокола, все станции должны быть связаны аутентичным общедоступным каналом, но для процесса калибровки этого не требуется.*

Проведем усредненный анализ потерь оптического сигнала, не учитывающий возможные дестабилизирующие факторы, способные повлиять на КК. Пусть расстояние от станции *C0* до *C1* равно *10 км*, от *C1* до *C2 – 15 км*, от *C2* до *C3* составляет *20 км*. Таким образом, максимальное расстояние от источника излучения до ЗФ *C3* и обратно до ОЛФД *C0* равно *90 км*. Собственные потери в КК для одномодового волокна и потери на разъемных соединениях *(lf)* принимаем равными *0.2 дБ/км.* Потери на сварных соединениях *(lw) – 0.05 дБ*. Суммарные потери в сегменте *lc – 10 дБ.*

$$L\text{сумм для С1} = 0.2[lf \text{ в ВОЛС}] * 10 + 0.2[lf] * 8 + 0.05\,[lw] * 28 + 10[lc] = 15 \text{ дБ}$$

$$L\text{сумм для С2} = 0.2[lf \text{ в ВОЛС}] * 25 + 0.2[lf] * 8 + 0.05\,[lw] * 62 + 10[lc] = 19.7 \text{ дБ}$$

$$L\text{сумм для С3} = 0.2[lf \text{ в ВОЛС}] * 45 + 0.2[lf] * 8 + 0.05\,[lw] * 98 + 10[lc] = 25.5 \text{ дБ}$$

Следует обратить внимание на то, что приведенные потери справедливы только для прямого направления, т.е. при построении энергетической модели системы КРК и расчете мощности оптического импульса, вносимого аттенюатором затухания, необходимо учитывать обратный путь от каждого сегмента.

Выводы и дискуссия. В статье рассмотрен способ обнаружения оптического сигнала синхронизации для участка сети квантовых коммуникаций, особенностью которого является наличие одной приемо-передающей станции и нескольких кодирующих станций. Описан принцип работы системы квантового распределения ключей с фазовым кодированием и предложена концепция алгоритма, адаптированного для предлагаемой конфигурации городской квантовой сети, содержащей несколько последовательных сегментов. Приведен расчет усредненных потерь в квантовом канале для наглядного понимания вносимых затуханий.

Переходя к дискуссии, можно выделить несколько актуальных проблем по мнению автора при технической реализации квантовых сетей: защищенность каналов аутентификации (как обеспечить безусловную защищенность не только квантового протокола, но и процесса аутентификации? Можно ли обойтись без классической криптографии при первичной аутентификации? Насколько безопасно использовать системы КРК, если злоумышленник имеет доступ к каналу синхронизации, аутентификации?) [11–16]; безопасная реализация самих ДПУ (вероятность НСД к аппаратуре в ДПУ больше вероятности атак на квантовый канал между ДПУ? Как обеспечить доставку квантовых ключей конечному пользователю?); однофотонность при формировании ключей (насколько реально добиться однофотонной передачи на расстоянии, например, 40 км в городских условиях? Какой протокол с доказанной стойкостью можно использовать в реальных условиях эксплуатации?) [17–20].

Автор статьи благодарен читателю и приглашает дать обратную связь по приведенным вопросам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Chen Y.A. et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres // Nature. – 2021. – Vol. 589, No. 7841. – P. 214-219.
2. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, No. 1. – P. 145-195.
3. *Bennett C.H., Brassard G., & Ekert A.K.* Quantum Cryptography // Scientific American. – 1992. – 267 (4). – P. 50-57. – http://www.jstor.org/stable/24939253.
4. *Кулик С.* Квантовая криптография // Фотоника. – 2010. – №. 2. – С. 36-41.
5. *Кулик С.П., Молотков С.Н.* MDI–Measurement Device Independent квантового распределения ключей // Письма в Журнал экспериментальной и теоретической физики. – 2023. – Т. 118, № 1. – С. 62-70.

6. *Lo H.K., Curty M., Qi B.* Measurement-device-independent quantum key distribution // Physical review letters. – 2012. – Vol. 108, No. 13. – P. 130503.
7. *Bouwmeester D. et al.* Experimental quantum teleportation // Nature. – 1997. – Vol. 390, No. 6660. – P. 575-579.
8. *Pljonkin A., Rumyantsev, K., Singh, P.K.* Synchronization in quantum key distribution systems // Cryptography. – 2017, 1, 18. – DOI: 10.3390/cryptography1030018.
9. *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.
10. *Гальярди Р.М., Карп Ш.* Оптическая связь: пер. с англ. / под ред. А.Г. Шереметьева. – М.: Связь, 1978. – 424 с.
11. *Deng F.G., & Long G.L.* Secure direct communication with a quantum one-time pad // Physical Review A. – 2004. – 69 (5). – 052319.
12. *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.
13. *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.
14. *Makarov V., & Hjelme D.R.* Faked states attack on quantum cryptosystems // Journal of Modern Optics. – 2005. – 52 (5). – P. 691-705.
15. *Сабанов А.Г., Шелупанов А.А.* Идентификация и аутентификация в цифровом мире. – М.: Горячая Линия–Телеком, 2022.
16. *Кравцов К.С. и др.* Система релятивистской квантовой криптографии. – 2018.
17. *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. – Springer Berlin Heidelberg, 2008. – P. 29-39.
18. *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. – P. 13-13.
19. *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. – P. 143-145.
20. *Поздняков А.М.* Способ передачи сообщения через вычислительную сеть с применением аппаратуры квантового распределения ключей. – 2019.

REFERENCES

1. *Chen Y.A. et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres, *Nature,* 2021, Vol. 589, No. 7841, pp. 214-219.
2. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography, *Reviews of Modern Physics,* 2002, Vol. 74, No. 1, pp. 145-195.
3. *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.
4. *Kulik S.* Kvantovaya kriptografiya [Quantum cryptography], *Fotonika* [Photonics], 2010, No. 2, pp. 36-41.
5. *Kulik S.P., Molotkov S.N.* MDI–Measurement Device Independent kvantovogo raspredeleniya klyuchey [MDI-Measurement Device Independent of quantum key distribution], *Pis'ma v Zhurnal eksperimental'noy i teoreticheskoy fiziki* [Letters to the Journal of Experimental and Theoretical Physics], 2023, Vol. 118, No. 1, pp. 62-70.
6. *Lo H.K., Curty M., Qi B.* Measurement-device-independent quantum key distribution, *Physical review letters,* 2012, Vol. 108, No. 13, pp. 130503.
7. *Bouwmeester D. et al.* Experimental quantum teleportation, *Nature,* 1997, Vol. 390, No. 6660, pp. 575-579.
8. *Pljonkin A., Rumyantsev, K., Singh, P.K.* Synchronization in quantum key distribution systems, *Cryptography,* 2017, 1, 18. DOI: 10.3390/cryptography1030018.
9. *Rumyantsev K.E., Plenkin A.P.* Sinkhronizatsiya sistemy kvantovogo raspredeleniya klyucha pri ispol'zovanii fotonnykh impul'sov dlya povysheniya zashchishchennosti [Synchronization of the quantum key distribution system using photon pulses to increase security], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8, pp. 81-96.
10. *Gal'yardi R.M., Karp Sh.* Opticheskaya svyaz' [Optical communication]: trans. from engl., ed. by A.G. Sheremet'eva. Moscow: Svyaz', 1978, 424 p.

11. *Deng F.G., & Long G.L.* Secure direct communication with a quantum one-time pad, *Physical Review A,* 2004, 69 (5), 052319.
12. *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.
13. *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.
14. *Makarov V., & Hjelme D.R.* Faked states attack on quantum cryptosystems, *Journal of Modern Optics,* 2005, 52 (5), pp. 691-705.
15. *Sabanov A.G., Shelupanov A.A.* Identifikatsiya i autentifikatsiya v tsifrovom mire [Identification and authentication in the digital world]. Moscow: Goryachaya Liniya–Telekom, 2022.
16. *Kravtsov K.S. i dr.* Sistema relyativistskoy kvantovoy kriptografii [The system of relativistic quantum cryptography], 2018.
17. *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*. Springer Berlin Heidelberg, 2008, pp. 29-39.
18. *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.
19. *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.
20. *Pozdnyakov A.M.* Sposob peredachi soobshcheniya cherez vychislitel'nuyu set' s primeneniem apparatury kvantovogo raspredeleniya klyuchey [Method for transmitting messages through a computing network using quantum key distribution equipment], 2019.

Статью рекомендовал к опубликованию д.т.н., профессор И.И. Турулин.

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; cand. of eng. sc.; associate professor.

УДК 621.396.67 DOI 10.18522/2311-3103-2024-5-260-270

А.В. Геворкян, В.С. Савостин

СВЕРХШИРОКОПОЛОСНЫЕ РЕШЁТКИ АНТЕНН ВИВАЛЬДИ С ТЕМ-РУПОРОМ

Приведены конструкции и характеристики антенных решёток на основе антиподного излучателя Вивальди. Исследуются антенные решётки с ТЕМ-рупорами линейного и эллиптического профиля. Проведена оптимизация параметров рупоров. Характеристики исследовались в диапазоне частот от 4 до 12 ГГц. Антенная решётка с ТЕМ-рупором линейного профиля имеет лучший КСВН в диапазоне от 4 до 5 ГГц (для крайних излучателей максимум равен 4,75, а для остальных – 3,33). Рабочая полоса частот антенной решётки находится в диапазоне от 4,90 до 12,00 ГГц (коэффициент перекрытия $k_п$=2,45). Частотная характеристика реализованного коэффициента усиления (КУ) имеет провалы. Антенная решётка с ТЕМ-рупор эллиптического профиля с узким основанием имеет минимальную рабочую полосу частот (от 7,06 до 12,00 ГГц ($k_п$=1,70)) и плавную характеристику реализованного КУ. Антенная решётка с увеличенной шириной основания ТЕМ-рупора эллиптического профиля имеет лучший КСВН в диапазоне от 5,3 до 12,0 ГГц (для крайних излучателей максимум равен 2,51, а для остальных – 2,15), но характеристика реализованного КУ плавная только до 9 ГГц. Рабочая полоса частот антенной решётки находится в диапазоне от 4,84 до 12,00 ГГц ($k_п$=2,48). Лучшие характеристики у антенной решётки с ТЕМ-рупором эллиптического профиля с расширенным основанием и увеличенной высотой. Увеличение высоты рупора приводит к увеличению значений реализованного КУ на частотах более 9,25 ГГц, где были провалы. Рабочая полоса частот находится в диапазоне от 4,72 до 12,00 ГГц