7. Bappy D.M., Jeon I. Combination of hybrid median filter and total variation minimisation for medical X-ray image restoration. *IET Image Processing*, 2016, vol. 10, no. 4, pp. 261-271. doi: 10.1049/iet-ipr.2015.0054
8. Mikolajczak G., Peksinski J. Estimation of the variance of noise in digital images using a median filter. *Telecommunications and Signal Processing (TSP)*, *2016 39th International Conference on*, IEEE, 2016, pp. 489-492. doi: 10.1109/TSP.2016.7760927.
9. Subbuthai P., Muruganand S. Restoration of retina images using extended median filter algorithm. *Signal Processing and Integrated Networks (SPIN), 2015 2nd International Conference on,* IEEE, 2015, pp. 131-138. doi: 10.1109/SPIN.2015.7095378.
10. Khatri S., Kasturiwale H. Quality assessment of Median filtering techniques for impulse noise removal from digital images. *Advanced Computing and Communication Systems (ICACCS), 2016 3rd International Conference on*, IEEE, 2016, vol. 1, pp. 1-4. doi: 10.1109/ICACCS.2016.7586331
11. Ko S.J., Lee Y.H. Center weighted median filters and their applications to image enhancement. *IEEE transactions on circuits and systems*, 1991, vol. 38, no. 9, pp. 984-993. doi: 10.1109/31.83870.
12. Bovik A.C. *Handbook of image and video processing.* Academic press, 2010. 974 p.
13. Gonzalez R.C., Woods R.E. *Digital image processing*. Moscow, Technosfera Publ., 2012. 1104 p. (In Russian).
14. Huang T.S., *Two-dimensional digital signal processing II: transforms and median filters*, New York, Springer-Verlag, 1981. 224 p.

Received 10.09.2017

ТЕХНОЛОГИИ ТЕЛЕКОММУНИКАЦИЙ

УДК 681.7.068

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО КАНАЛА ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ВОЛОКОННО-ОПТИЧЕСКОГО ЛИНЕЙНОГО ТРАКТА

Бурдин А.В., Губарева О.Ю., Пашин С.С., Пугин В.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: bourdine@yandex.ru

Предложен альтернативный способ реализации защищенного на физическом уровне канала передачи конфиденциальной информации сегмента «первая/последняя миля» внутрикорпоративной сети на базе специализированного волоконно-оптического линейного тракта. Решение базируется на применении в соединительных кабельных линиях специализированных кварцевых волоконных световодов, функционирующих в маломодовом режиме передачи оптического сигнала, который достигается за счет совместного использования когерентных источников оптического излучения (лазеров), являющихся основой приемо-передающих модулей активного оборудования мультигигабитных сетей передачи данных, и предлагаемых специализированных оптических волокон с увеличенным диаметром сердцевины, поддерживающих в маломодовом режиме распространение ограниченного набора модовых составляющих. В качестве второй дополнительной степени защиты канала передачи КИ предлагается использовать элементы технологии модового мультиплексирования.

Ключевые слова: оптические волокна, маломодовый режим, управление дифференциальной модовой задержкой, профиль показателя преломления, модовый состав, модовое мультиплексирование, связь мод, условия ввода оптического сигнала с выхода лазера, оптические крипто-волокна, конфиденциальная информация, защита информации, канал передачи

Введение

В настоящее время деятельность практически любого предприятия или организации сопровождается необходимостью передачи и последующей обработки конфиденциальной информации (КИ), которая может представлять собой, например, персональные данные сотрудников или клиентов, а также документы, составляющие коммерческую, а в ряде случаев – и государственную тайну [1-2; 45-48].

В отдельную группу проблем, связанных с обработкой КИ, как правило, выделяют вопросы обработки и передачи персональных данных в многочисленных многофункциональных центрах по

предоставлению услуг населению. Очевидно, что несанкционированный доступ, снятие/кража КИ так или иначе негативно влияют на ключевые показатели бизнес-процессов [3-7; 22].

Подавляющее большинство систем защиты (как в случае представленных на отечественном и мировом рынках информационной безопасности коммерческих систем, так и отдельных проприетарных решений) базируется на компьютерной безопасности и антивирусной защите от хакерских атак [3-9]. Основной акцент делается на аппаратно-программных комплексах защиты от утечки КИ в точках консолидации внутрикорпоративной и глобальной сетей [4-9]. В то время как подкластерам уровня «первая/последняя миля», находящимся внутри «периметра» корпоративной сети, соответствующее внимание практически не уделяется, не говоря уже о том, что в данном сегменте сети защита транслируемых данных на физическом уровне в подавляющем большинстве случаев просто не предполагается.

В данной работе представлен альтернативный подход для решения описанной задачи, который предлагается реализовать непосредственно с помощью специализированного волоконно-оптического линейного тракта.

Обзор решений съема КИ по ОВ

Описанный выше кластер «первой/последней мили» внутрикорпоративных сетей, в целом, отличается малой протяженностью соединительных кабельных линий: от десятков метров – например в случае структурированных кабельных систем (СКС) центров обработки данных, до одного-двух километров, соответствующих «кампусным» СКС, например объединенной группы зданий (производственные цеха, технологические площадки и административные помещения предприятия). Для этого сегмента сетей также характерно увеличенное, по сравнению с сетями передачи данных общего пользования, количество информационных портов. В данном случае удобно воспользоваться термином «компактные многопортовые сети», к которым относятся внутриобъектовые СКС бизнес-центров, внутрикорпоративные сети промышленных предприятий, упомянутые СКС центров обработки данных, сетей хранения данных, вычислительных центров и др.

В целом, как известно [10-12], СКС представляет собой универсальную кабельную систему отдельного здания/помещения или группы зданий. Универсальность СКС подразумевает использование ее для различных систем, таких как: компьютерная сеть, телефонная сеть, охранная система, пожарная сигнализация и др. СКС охватывает все пространство здания и соединяет точки средств передачи информации, которые обеспечиваются индивидуальной точкой входа в общую систему здания. Кабельные соединительные линии горизонтальной подсистемы, индивидуальные для каждой информационной розетки, связывают точки входа с коммутационным центром этажа, образуя горизонтальную кабельную подсистему. Этажные коммутационные узлы с помощью магистральных кабелей вертикальной подсистемы объединяются в центре коммутации здания. Сюда же подводятся внешние кабели для подключения здания к глобальным информационным ресурсам, таким как телефония, интернет и т.п. Описанная топология позволяет надежно управлять всей системой здания, обеспечивает гибкость и простоту системы, а также ее унифицируемость и масштабируемость.

В настоящее время как минимум вертикальные подсистемы современных СКС реализуются на базе волоконно-оптических кабелей (ОК) с применением технологии FTTE («Fiber-To-The-Enclosure» – «волокно до конструктива») [12]. Однако нередко в условиях повышенных требований к пропускной способности соответствующего подкластера сети, объединяющего выделенную группу пользователей, используется технология FTTD («Fiber-To-The-Desk» – «волокно до рабочего места»), и в этом случае горизонтальная подсистема СКС также представляет собой совокупность ОК.

Следует отметить, что в качестве одного из ключевых преимуществ перехода на ОК отмечается высокая степень защиты сети непосредственно на физическом уровне по сравнению с подсистемами СКС, реализованными на базе витой пары или коаксиального кабеля [12]. Безусловно, по сравнению с последними общее число способов съема/кражи КИ с ОВ намного меньше. Однако на сегодняшний день известен целый ряд каналов утечки КИ в волоконно-оптических линиях передачи (ВОЛП), подробно описанных в работах отечественных и зарубежных авторов [13-16], на основе которых предлагаются различные способы и методики активных и пассивных способов защиты от утечки КИ в ВОЛП [17-26].

Наибольшие количество атак на КИ в ВОЛП реализовано по акусто-опто-волоконным каналам утечки речевой информации. На сегодняшней день известны способы нейтрализации воздействия акустических полей на ОВ кабеля путем специальной звукоизолирующей оболочки волокна и кабеля, которая понижает влияние вибраций и звука на параметры света в волоконно-оптических линиях связи [13-17]. Более того, в соответствии с «Правилами применения оптических кабелей связи, пассивных оптических устройств и устройств для сварки оптических волокон», утвер-

жденными приказом Министерства информационных технологий и связи Российской Федерации от 19.04.2006, №47, от производителей кабеля требуется стойкость оптического кабеля к вибрационным нагрузкам с ускорением до 40 м/с^2 в диапазоне частот от 10 до 200 Гц. Однако и это не обеспечивает полной защиты от акусто-опто-волоконного канала утечки речевой информации, что связано с возможностью создать акустический контакт с кабелем как непреднамеренно при монтаже и эксплуатации, так и специально нарушителем [18-19, 21-22].

Также известны способы нейтрализации локального влияния акустических полей на ОВ кабеля путем включения в линейный тракт ВОЛП специального оборудования, восстанавливающего параметры оптических импульсов, в том числе повторителей и (или) фирегенераторов сигналов [19, 27-33]. В качестве примера можно привести опто-электронное развязывающее устройство (ОРУ) на один порт SC ОРУ-1 или на два порта SC ОРУ-2. Здесь принцип работы основан на преобразовании оптического сигнала в электрический и последующем преобразовании в оптический сигнал, очищенный от шумов, в том числе и акустической природы. Более того, в принципе любое активное оборудование ВОЛП неизбежно разрушает акусто-опто-волоконный канал утечки, так как в нем восстанавливается исходная цифровая модуляция и шумовые воздействия исчезают.

В то же время применение как специального, так и типового активного оборудования не исключает опасности формирования утечки КИ [4-8]. В результате требуется проведение целого ряда дополнительных мероприятий по обслуживанию, размещению рядом с защищаемым помещением в специализированном шкафу, регламентированных проверок функционирования и т.д. Кроме того, такое оборудование требует дополнительной защиты от утечки по побочным электромагнитным излучениям и наводкам, что связано с электронными составляющими оборудования с цепями электрического питания от сети [13; 16].

На сегодняшний день разработан целый ряд различных способов, методов и устройств защиты КИ, передаваемой по ВОЛП [27-33], но ни один из них не гарантирует полной защиты КИ.

Так, согласно [27], «Способ защиты акустической речевой информации от сопутствующей передачи по оптическим линиям связи, заключающийся в том, что производят регистрацию с демодуляцией на акустических частотах параметров оптического излучения, проходящего через элементы волоконно-оптические телекоммуникации выделенных помещений, и определяют утечку акустической речевой информации, отличающийся тем, что при определении утечки акустической речевой информации в выделенном помещении изменяют режим работы источника оптического излучения – лазера…» – то есть режим работы источника оптического излучения меняется только при фиксации (определении) факта утечки КИ, что, с точки зрения защиты информации, является не вполне корректным. КИ в момент передачи по сети всегда должна быть защищена вне зависимости, знает ли служба безопасности о планируем или происходящем факте ее кражи. В настоящий момент ведутся разработки по внедрению методов с использованием режима динамического хаоса, который позволяет обеспечить передачу информационных сигналов в виде псевдохаотических колебаний частоты и амплитуды оптической несущей [15; 18]. Наложение на такой сигнал, снимаемый с боковой поверхности волокна, шумового сигнала, который обязательно будет присутствовать, сильно затрудняет несанкционированный доступ. Следует отметить, что данный подход может быть использован в комбинации с предлагаемым в данной работе методе защиты КИ, передаваемой в ВОЛП.

Направление разработки способов, методов и устройств защиты КИ от утечки ВОЛП развивается достаточно давно. Одними из первых этим вопросом заинтересовались специалисты компании Hughes Aircraft (США): в 1991 г. была разработана система защиты IDOC (Intrusion Detection Optical Communications System) – это первая некриптографическая система защиты КИ в ВОЛП, которая была сертифицирована АНБ США и положена в основу доктрины по безопасности для ОВ [34]. Однако данная технология не пригодна для передачи КИ на дальние расстояния, так как метод не предполагает использование одномодового волокна.

Как было отмечено выше, подавляющее большинство известных решений описанной проблемы непосредственно в оптическом интерфейсе ориентировано на применение квантовой криптографии [35-37]. Практическая реализация данного направления требует использования дорогостоящего оборудования, отдельные известные опытные образцы которого на сегодняшний день находятся в опытной (лабораторной) эксплуатации в рамках государственных проектов по организации региональных квантовых центров [38-41]. В качестве отдельной группы также следует выделить работы, посвященные сочетанию элементов теории квантовой криптографии с технологиями модового мультиплексирования и кодирования, например, с помощью дифракционных оптических элементов, оптических вихревых пучков (вортексов) [42-44] и др. Однако и здесь предполагается использование сложной эле-

ментной базы, а успешно реализованные эксперименты и представленные в открытых публикациях результаты по ним ограничены лабораторными испытаниями с применением специализированного оборудования, в то время как реальные волоконно-оптические тракты отличаются от модельных линий целым набором дополнительных негативных факторов искажения транслируемых оптических сигналов.

Таким образом, следует отметить, что разработка универсального метода, способа или технологии по защите КИ в ВОЛП по-прежнему является актуальной задачей. Более того, любая технология, разрабатываемая для внедрения на территории РФ, должна соответствовать не только руководящим документам в области защиты информации международных организаций в области связи ISO и ITU, но в первую очередь – отечественным стандартам [45-49].

Описание предлагаемого решения

Для реализации защиты сегмента «первая/последняя миля» внутрикорпоративной сети авторы предлагают реализовать защищенный на физическом уровне канал передачи КИ с применением специализированного волоконно-оптического линейного тракта. Данное решение базируется на применении в соединительных кабельных линиях специализированных кварцевых волоконных световодов, функционирующих в маломодовом режиме передачи оптического сигнала, который достигается за счет совместного использования когерентных источников оптического излучения (лазеров), являющихся основой приемо-передающих модулей активного оборудования мультигигабитных сетей передачи данных, и предлагаемых специализированных оптических ОВ с увеличенным диаметром сердцевины, поддерживающих в маломодовом режиме распространение ограниченного набора модовых составляющих [50].

Геометрия ОВ остается традиционной и представляет собой классическую коаксиальную конструкцию в виде легированной соответствующими редкоземельными примесями кварцевой сердцевины, окруженной одной внешней сплошной оболочкой из чистого кварца. Однако при этом специализированная форма профиля показателя преломления таких ОВ обеспечивает усиленное проявление заданного характера эффекта дифференциальной модовой задержки (ДМЗ), уникальное для того или иного световода. В результате такое ОВ на всем протяжении линии является шифратором, а форма его специализированного профиля показателя преломления выполняет роль ключа. Таким образом, транслируемый сильно искаженный за счет ДМЗ трафик становится невозможно разобрать без соответствующего дешифратора.

Диаметр сердцевины предлагаемого ОВ увеличен по сравнению с одномодовыми ОВ и в общем случае может выбираться таким образом, чтобы обеспечивать выполнение условия отсечки заданному количеству направляемых мод искомых порядков. Для унификации и возможности сочетания таких ОВ с типовыми конструктивами пассивных устройств коммутации, волоконно-оптическими коннекторами и адаптерами, а также классическими технологиями полевого монтажа и сращивания кварцевых ОВ предлагается ограничить диаметр оболочки ОВ 125 мкм в соответствии с ратифицированными категориями ОВ TIA и ISO [10-12]. Формально диаметр сердцевины предлагаемых ОВ может быть также выбран идентичным номенклатурным значениям: 50 мкм или 62,5 мкм.

Маломодовый режим передачи оптического сигнала формируется за счет возбуждения ОВ с увеличенным диаметром сердцевины когерентным источником оптического излучения – лазером – например, типовыми лазерным диодом или VCSEL (спецификации LX или SX, соответственно, серии стандартов IEEE 802.3), которые, в частности, также традиционно используются в оптических приемо-передающих модулях (трансиверах) активного оборудования мультигигабитных сетей [10-12; 50]. Сочетание когерентного источника излучения и ОВ с увеличенным диаметром сердцевины приводит к тому, что сигнал переносится в таком световоде ограниченным числом модовых составляющих, число которых в первую очередь определяется исходным модовым составом излучения, генерируемого лазером, условиями ввода самого сигнала в торец сердцевины ОВ и геометрией/параметрами последнего. Отличительной особенностью передачи оптического сигнала по ОВ в маломодовом режиме является непосредственно эффект ДМЗ, который проявляется в виде разделения оптического импульса на отдельные компоненты неодинаковой амплитуды и разбросом по времени поступления на приемную сторону [50]. При этом огибающая оптического импульса, традиционно имеющая квазигауссовскую форму, не сохраняется и приобретает форму «перчатки». Степень и характер проявления эффекта ДМЗ для разных сочетаний «лазер – ОВ» может проявляться по-разному. Более того, этот эффект может проявляться и для одной и той же пары «лазер – ОВ» при неконтролируемых условиях ввода.

Безусловно, с точки зрения традиционных мультигигабитных инфокоммуникационных сетей ДМЗ

является негативным эффектом, сильно искажающим форму оптического импульса, который является ключевым фактором, ограничивающим пропускную способность волоконно-оптических линий передачи для таких приложений ратифицированных сетевых стандартов IEEE, регламентирующих передачу оптических сигналов когерентных источников по многомодовым ОВ на жестко ограниченные (буквально десятками и сотнями метров) расстояния со скоростью 1/10/40/100 Гбит/с [12; 50]. В этом смысле известно достаточно большое количество работ, направленных на разработку аппаратных средств и самой конструкции ОВ для уменьшения ДМЗ в линейном тракте, детальный обзор которых представлен в монографии [51].

Напротив, в рамках данного проекта, с точки зрения защиты конфиденциальных данных на физическом уровне, при передаче последних по волоконно-оптическим линиям СКС внутрикорпоративной сети предлагается использовать кварцевые ОВ с уникальным, специальным образом выбранным профилем показателя преломления, за счет которого обеспечивалось бы усиленное проявление эффекта ДМЗ уже буквально на первых метрах линии. Фактически такое ОВ на всем протяжении линии является шифратором, а форма его специализированного профиля показателя преломления выполняет роль ключа. Таким образом, транслируемый сильно искаженный за счет ДМЗ трафик становится невозможно разобрать без соответствующего дешифратора. Вышесказанное делает бесполезной подсоединение волоконно-оптического снифера, включение вставки с волоконно-оптическим разветвителем для отвода/перехвата сигнала или прямой врезки в канал передачи, что непосредственно исключает MITM-атаки (Man-in-the-Middle – «человек посередине»).

Очевидно, что степень защиты КИ на основе предложенного подхода может быть увеличена за счет каскадного включения крипто-волокон с отличающимися профилями показателя преломления, обеспечивающих разные степень и характер усиленного проявления ДМЗ.

На рис. 1 представлена типовая структурная схема СКС класса «зоны распределения», реализуемой на базе технологии FTTD. В этом случае на все трех сегментах кабельной системы – магистральном ОК вертикальной подсистемы и двух сегментах горизонтальной подсистемы (распределительный и абонентский ОК) могут быть последовательно скоммутированы в соответствующих кроссах или сплайс-боксах указанные ОВ. Альтернативным решением в этом смысле является инсталляция кабеля с крипто-волокном с изменяющимся вдоль длины профилем показателя преломления, также обеспечивающим усиленное проявление ДМЗ, степень и характер которого будет также изменяться соответствующим образом вдоль длины ОВ.

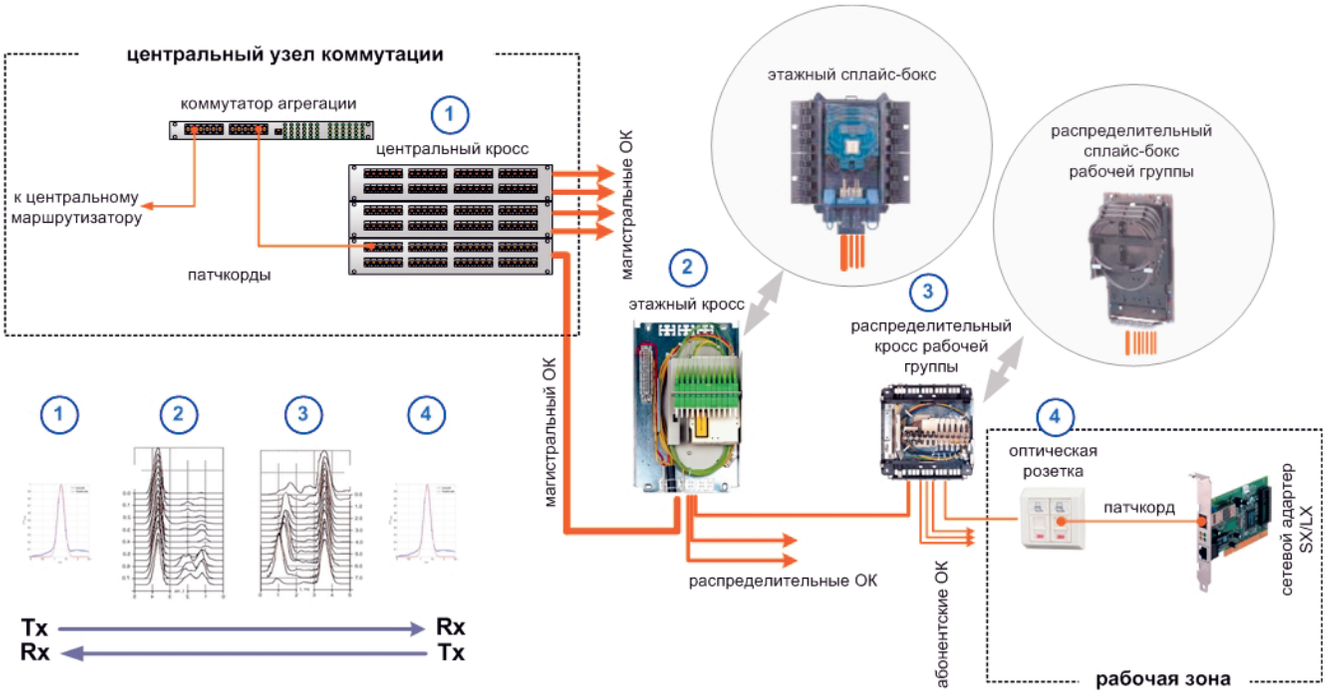

Рис. 1. Структурная схема СКС внутрикорпоративной сети передачи данных, реализованной на базе технологии FTTD с использованием оптических крипто-волокон

Предложенный подход может также использоваться и уже на инсталлированных СКС с волоконно-оптическими подсистемами с многомодовыми ОВ. В этом случае в локациях размещения устройств коммутации (см. рис. 1), например, центральном узле коммутации, этажных распределительных кроссах, а также кроссах рабочих групп между коммутируемыми ОВ подсистем СКС, включаются предлагаемые ОВ с сильным проявлением ДМЗ, длина которых выбирается исходя из протяженности сегментов волоконно-оптического линейного тракта. В этом случае крипто-волокна, уложенные в компактные бухты, могут непосредственно размещаться в устройствах коммутации (кроссах и сплайс-боксах) либо в 1/2U контейнерах и устанавливаться в конструктив.

В качестве второй дополнительной степени защиты канала передачи КИ предлагается использовать элементы технологии модового мультиплексирования. Однако в отличие от известных решений, предполагающих применение данной техники, с точки зрения уплотнения каналов и увеличения пропускной способности сети в целом, в данной работе предлагается использовать только определенную модовую компоненту заданного порядка (или группу мод) для передачи полезного информационного сигнала. При этом в течение заранее определенного интервала времени (например, через 12, 16 или иное задаваемое непосредственно оператором или взаимодействующими сторонами число часов) система передачи самостоятельно определяет, какая из мод будет использоваться в данный период времени, при этом могут использоваться различные алгоритмы генерации случайных чисел, побитовое сложение по модулю два и т.п. Благодаря этому из цикла работы будут исключены как непосредственно клиент, так и клиентские станции и в результате будут минимизированные дополнительные каналы утечки информации. Таким образом, закрытые сеансовые ключи предаются по защищенному каналу без участия пользователя информационной системы, устраняя тем самым возможность применения методов социальной инженерии. Такая технология, особенно в сочетании с представленными выше крипто-волокнами, является намного более надежной по сравнению с организацией туннелирования и передачей информации по открытым каналам сети доступа.

Ключевой проблемой, с точки зрения практической реализации данного решения, является волокно-оптическая структура, обеспечивающая селективное возбуждение модового состава ОВ. В данном случае в качестве одного из возможных решений указанной проблемы можно рассмотреть фотонные лантерны [52-53], известные аналоги которых представлены на рынке фотоники и волоконной оптики, обеспечивают ввод до 12, а некоторые модели и больше, модовых каналов. Однако здесь необходимо проведение дополнительных теоретических исследований, в частности вычислительных экспериментов, направленных на разработку методик расчета параметров схемы прецизионного пространственного позиционирования каналов системы модового мультиплексирования выхода (входа) модовых мультиплексора (демультиплексора) на торце как традиционного многомодового ОВ соответствующей категории ISO/TIA, так и предлагаемых крипто-волокон.

В зависимости от структуры и состояния сегмента сети строятся различные конфигурации построения линейного тракта ВОЛП на основе крипто-волокон и смены селективного модового канала.

Заключение

Разработка научно-технических основ функционирования предложенного подхода организации защищенного на физическом уровне канала передачи КИ на базе специализированного волоконно-оптического линейного тракта невозможна без соответствующего математического аппарата с применением ранее разработанных методов расчета параметров передачи модового состава волоконных световодов сложной конструкции и методов анализа процессов распространения оптических сигналов, возбуждаемых когерентными источниками оптического излучения по ОВ с увеличенным диаметром сердцевины в маломодовом режиме, адаптированных на рассматриваемый случай, в том числе и для решения задачи синтеза профиля показателя преломления искомой формы, обеспечивающего заданное управление ДМЗ.

В маломодовом режиме на передний план выходит необходимость «индивидуальной» оценки параметров передачи направляемых мод заданного порядка, участвующих в переносе мощности оптического сигнала по многомодовому ОВ заданной конструкции. Модовый состав излучения лазера и условия ввода определяют исходный набор модовых компонентов и значения их амплитуд непосредственно на передающей стороне многомодовой ВОЛП. К основным факторам искажения относятся ДМЗ, а также хроматическая дисперсия основной моды и мод высших порядков. При распространении маломодовых сигналов в сильно нерегулярных волокнах взаимодействие и смешение мод может оказывать существенное влияние на проявление ДМЗ за счет возникновения новых или, напротив, снижения мощности исходных модовых составля-

ющих сигнала. В результате требуется разработка следующих теоретических методов:

– метод анализа волоконного световода, обеспечивающий возможность оценки параметров передачи направляемых мод произвольного порядка, распространяющихся в ОВ с увеличенным диаметром сердцевины с произвольным профилем показателя преломления;

– метод анализа распространения маломодовых оптических сигналов по ОВ в режиме управления ДМЗ;

– метод синтеза профиля показателя крипто-ОВ заданной конструкции, обеспечивающего проявление эффекта ДМЗ заданной степени и характера.

Литература

1. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (в ред. Федеральных законов от 02.02.2006 № 19-ФЗ, от 18.12.2006 № 231-ФЗ, от 24.07.2007 № 214-ФЗ). – 7 с.
2. Шестакова Е. Перечень конфиденциальной информации. 2012 год // URL: http://www.hr-portal.ru/article/perechen-konfidencialnoy-informacii (д.о. 01.07.2017)
3. Шередин Р.В. О проблеме защиты персональных данных / Инфофорум-Гонконг-2012. 23. 10. 2013 // URL: http://pd.rkn.gov.ru/press-service/subject4/news3007/ (д.о. 01.07.2017)
4. Ульянов В. Утечки конфиденциальной информации. Итоги 2013 г. Материалы аналитического центра Zecurion // URL: http://d-russia.ru/wp-content/uploads/2014/03/Zecurion_Data_leaks_2014.pdf (д.о. 01.07.2017)
5. Ходаковский К. Самые громкие утечки информации 2014 года // URL: https://3dnews.ru/907353 д.о. 01.07.2017)
6. Утечки конфиденциальной информации (итоги 2013 года) Новостной блог banki.ru // URL: http://www.banki.ru/news/research/?id=6242078 (д.о. 01.07.2017)
7. DLP: Громкие утечки информации / Официальный сайт TADVISER SUMMIT // URL: http://www.tadviser.ru/index.php (д.о. 01.07.2017)
8. Михайлова А. Основные каналы утечки информации на предприятии / Anti-Malware.ru Интернет-журн. 21.08.17 // URL: https://www.anti-malware.ru/analytics/Threats_Analysis/main-channels-information-leakage-in-enterprise (д.о. 22.08.2017 г.)
9. Панасенко А. Конфиденциальные данные продолжают утекать / Anti-Malware.ru Интернет-журнал, 08.10.15 // URL: https:// www.anti-malware.ru/analytics/Threats_ Analysis / Sensitive_data_continue_leak (д.о. 01.07.2017)
10. Семенов А.Б., Стрижаков С.К., Сунчелей И.Р. Структурированные кабельные системы. М.: ДМК Пресс, 2002. – 640 с.
11. Смирнов И.Г. Структурированные кабельные системы – проектирование, монтаж, сертификация. М.: AESP, 2007. – 348 с.
12. Семенов А.Б. Волоконно-оптические подсистемы современных СКС. М.: Академия АйТи; ДМК Пресс, 2007. – 632 с.
13. Гришачев В.В., Кабашкин В.Н., Фролов А.Д. Анализ каналов утечки информации в волоконно-оптических линиях связи: нарушение полного внутреннего отражения // Информационное противодействие угрозам терроризма. №4, 2005. – С. 194-205.
14. Федоров И.С., Орехов И.Н., Красноборько Э.В. Особенности утечки информации по акустическим и виброакустическим каналам // Безопасность информационных технологий. №1, 2004. – С. 114-118.
15. Гришачев В.В., Халяпин Д.Б., Шевченко Н.А., Мерзликин В.Г. Новые каналы утечки конфиденциальной речевой информации через волоконно-оптические подсистемы СКС // Техника для спецслужб. Статьи. Средства оценки и анализа оптического канала утечки информации, 2011 // URL: http://www.bnti.ru /showart.asp?aid=944&lvl=04.02.04. (д.о. 01.07.2017)
16. Филатенков А. Доказательства уязвимости ВОЛС // Сети Network World. № 09, 2008 // URL: http://www.osp.ru/nets/2008/09/5300705/ (д.о. 01.07.2017)
17. Гришачев В.В., Косенко О.А., Халяпин Д.Б. Методы активного противодействия утечке речевой информации по акусто-опто-волоконным каналам акустическим зашумлением // Специальная техника. №3, 2010. – С. 49-62.
18. Яковлев А.В. Волоконно-оптическая система передачи конфиденциальной информации // Электросвязь. №10, 1994. – С. 227.
19. Свинцов А.Г. Оптимизация параметров оптического рефлектометра для обнаружения неоднородности при попытке несанкционированного доступа в ВОСП // Фотон-Экспресс. №6, 2006. – С. 56-71.
20. Терентьев Е.Б., Халяпин Д.Б. Защита речевой информации от утечки через извещатели охранно-пожарной сигнализации // Технологии техносферной безопасности. №5, 2007 // URL: http://www.ipb.mos.ru/ttb/2007-5/2007-5.html (д.о. 28.06.2017)

21. Манько А., Каток В., Задорожний М. Защита информации на волоконно-оптических линиях связи от несанкционированного доступа // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. № 2, 2001. – С. 249-255.
22. Боос А.В., Шухардин О.Н. Анализ проблем обеспечения безопасности информации, передаваемой по оптическим каналам связи, и пути их решения // Информационное противодействие угрозам терроризма. №5, 2007. – С. 162.
23. Townsend P.D., Rarity J.G., Tapster P.R. Single photon interference in a 10 km long optical fibre interferometer // Electronics Letters. №29, 1993. – С. 634.
24. Townsend P.D., Rarity J.G., Tapster P.R. Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel // Electronics Letters. №29, 1993. – С. 1291.
25. Шапкин А.В. К вопросу о способах защиты информации при ее передаче в волоконно-оптических линиях связи // Информационные технологии, связь и защита информации МВД России. Часть 1, 2011. – С. 52-53.
26. Глущенко А.В., Глущенко Л.А., Тупота В.И. Математическая модель получения информации об акустическом сигнале по отраженному лазерному излучению // Сб. докладов 20-ой МНТК «Лазеры. Измерения. Информация-2010», Т.1. Санкт-Петербург, 2010. – С. 209-220.
27. Алисевич Е.А., Иванов Н.А., Иванов С.А. и др. Способ защиты акустической речевой информации от сопутствующей передачи по оптическим линиям связи. Патент RU 2609893C1 от 07.02.2017. Бюл. № 4.
28. Ивченко С.Н., Шубин В.В. Способ защиты информации от несанкционированного доступа в волоконно-оптических линиях связи. Патент RU 2110894 от 10.05.1998.
29. Гришачев В.В. Волоконно-оптический детектор угроз утечки речевой информации через волоконно-оптические коммуникации. Патент RU 2428798 от 20.03.2011.
30. Healey P., Sikora Edmund S.R. Communicating or reproducing an audible sound. Patent US 8000609, 16.08.2011.
31. Гришачев В.В., Халяпин Д.Б., Шевченко Н.А. Способы и устройства активной защиты речевой информации от прослушивания по акусто-опто-волоконному каналу утечки. Патент RU 2416166C2 от 10.04.2011. Бюл. №10.
32. Трещиков В.Н., Наний О.Е. Распределенный датчик акустических и вибрационных воздействий. Патент RU 2532562C1 от 10.11.2014. Бюл. №31.
33. Гришачев В.В., Халяпин Д.Б., Шевченко Н.А. Способ и устройство активной защиты конфиденциальной речевой информации от утечки по акусто-опто-волоконному каналу на основе внешнего оптического зашумления. Патент RU 2416167 от 10.04.2011. Бюл. №10.
34. Operational Security Doctrine for the Fiber Alarmed Modem (FAM)-131 Intrusion Detection Optical Communications System (IDOCS) / NSTISSI №3015 от 28.02.1991. – DOCID: 3353807. – 11 p.
35. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир, 2006. – 824 с.
36. Килин С.Я. Квантовая криптография – идеи практика. Минск: Белорусская наука, 2007. – 260 с.
37. Bernstein D.J. Introduction to quantum cryptography // New York: Springer, 2009. DOI https://doi.org/10.1007/978-3-540-88702-7_1.
38. Российский Квантовый Центр // Интернет-журнал, 2013-2017 // URL: http://www.rqc.ru/publications/articles/ (д.о. 01.07.2017)
39. Kazan Quantum Center // Интернет-журнал, 2014-2017 // URL: https://kazanqc.org/ru/pubs// (д.о. 01.07.2017).
40. Пресс-служба Университета ИТМО. Запущена единственная в СНГ многоузловая квантовая сеть // URL: http://technopark.ifmo.ru/zapushhena-edinstvennaya-v-sng-mnogouzlovaya-kvantovaya-set/ (д.о. 01.07.2017)
41. Шмыров В.В. В России научились ставить квантовую защиту на действующие линии связи // CNews Media Интернет-журнал, 23.05.17 // URL: http://www.cnews.ru /news/top/2017-05-23_v_rossii_nauchilis_pri menyat_kvantovuyu_zashchitu (д.о. 01.07.2017)
42. Carpenter J., Xiong Ch., Collins M.J. e. a. Mode multiplexed single-photon and classical channels in a few-mode fiber // Optics Express. Vol. 21, No. 23, 2013. – P. 28794-28800.
43. Mirhosseini M., Magaña-Loaiza O.S., O'Sullivan M.N. e. a. High-Dimensional Quantum Cryptography with Twisted Light // New Journal of Physics. Vol. 17, 2015. – P. 033033-1-033033-12.
44. Ndagano B., Nape I., Cox M.A. e. a. Creation and Characterization of Vector Vortex Modes for

Classical and Quantum Communication // arXiv.org. – 2017 (preprint).
45. ГОСТ Р 50.1.056-2005. Техническая защита информации. Основные термины и определения, от 29.12.2005 // URL: http://www. consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=396925#0 (д.о. 03.07.2017)
46. Указ Президента РФ от 12.05.2009 № 537 (ред. от 01.07.2014) «О Стратегии национальной безопасности Российской Федерации до 2020 года». – 25 с.
47. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации. Положение о лицензировании деятельности по технической защите конфиденциальной информации» // URL: http://ivo.garant.ru/# /document/71556224/paragraph/1:0 (д.о. 03.07.2017)
48. Руководящий документ Гостехкомиссии России «СВТ. Защита от НСД к информации. Показатели защищенности от НСД» // Гостехкомиссия России, 1992.
49. Хорев А.А. Средства акустической разведки: проводные микрофонные системы и электронные стетоскопы // Спецтехника и связь. №2, 2008. – С. 36-42.
50. Bottacchi S. Multi-Gigabit transmission over multimode optical fibre. Theory and design methods for 10GbE systems. West Sussex: John Wiley & Sons Ltd., 2006. – 654 p.
51. Бурдин А.В. Маломодовый режим передачи оптических сигналов по многомодовым волокнам: приложения в современных инфокоммуникациях. Самара: Изд-во ПГУТИ, 2011. – 274 с.
52. Noordegraaf D., Skovgaard P.M., Nielsen M.D. e. a. Efficient multi-mode to single-mode coupling in a photonic lantern // Optics Express. Vol. 17(3), 2009. – P. 1988-1994.
53. Leon-Saval S.G., Argyros A., Bland-Hawthorn J. Photonic lanterns: a study of light propagation in multimode to single-mode converters // Optics Express. Vol. 18(8), 2010. – P. 8430-8439.

Получено 25.09.2017

Бурдин Антон Владимирович, д.т.н., доцент, профессор Кафедры линий связи и измерений в технике связи» (ЛС и ИТС) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. (8-846) 332-21-61. E-mail: bourdine@yandex.ru

Губарева Ольга Юрьевна, зам. начальника НИО, ассистент Кафедры мультисервисных сетей и информационной безопасности ПГУТИ. Тел. (8-846) 332-21-61. E-mail: o.gubareva@psuti.ru

Пашин Станислав Сергеевич, аспирант Кафедры ЛС и ИТС ПГУТИ. Тел. 8-987-438-71-55. E-mail: pashinstanislav@outlook.com

Пугин Владимир Владимирович, к.т.н., доцент, декан Факультета заочного обучения ПГУТИ. Тел. 8-(846) 332-61-99. E-mail: pugin@psuti.ru

SECURE DATA TRANSMISSION OVER SPECIALIZED FIBER-OPTIC LINK

Bourdine A.V., Gubareva O.Yu., Pashin S.S., Pugin V.V.
Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation
E-mail: bourdine@yandex.ru

In this article we present an alternative method of secure data transmission over physical layer for the “first/last mile” segment of intra-corporate network implemented with specialized fiber-optic link. Proposed solution is based on using few-mode optical fibers with specific refractive index profile as an «encryptor», which creates unique distortions in accordance with its unique differential mode delay. Therefore, transmitted traffic becomes strongly distorted and cannot be processed without corresponding «decryptor» which might be either another optical fiber with «inversed» refractive index profile in relation to the «encryptor» - fiber or electronic dispersion compensator device modified for such an application. We also propose to utilize elements of mode division multiplexing technique as an additional protection for secure data channel. Such an approach is based on using only one particular mode (or modes) for secure data transmission, which is changed with certain time interval according to the privacy key. This work presents configurations of proposed «crypto-fiber-optic» link as well as the list of problems which require a solution for designing, developing and implementing the presented approach.

Keywords: optical fiber, few-mode regime, differential mode delay management, refractive index profile, mode staff, mode division multiplexing, laser-generated optical signal input conditions, optical crypto-fibers

DOI: 10.18469/ikt.2017.15.4.04

Bourdine Anton Vladimirovich, Povolzhskiy State University of Telecommunications and Informatics, 77 Moskovskoe shosse, Samara 443090, Russian Federation; Professor of the Department of Communication Lines; Doctor of Technical Science, Associated Professor. Tel.: +78463322161. E-mail: bourdine@psuti.ru

Gubareva Olga Yurevna, Povolzhskiy State University of Telecommunications and Informatics, 23 L. Tolstoy, Samara, 443010, Russian Federation; Deputy Head of the Science and Research Department, Assistant of the Department of Multiservice Networks and Information Security. Tel.: +79277321211. E-mail: o.gubareva@psuti.ru

Pashin Stanislav Sergeevich, Povolzhskiy State University of Telecommunications and Informatics, 77, Moscovskoe shosse, Samara 443090, Russian Federation; post-graduate student of the of the Department of Communication Lines. Tel.: +79874387155; E-mail: pashinstanislav@outlook.com

Pugin Vladimir Vladimirovich, Povolzhskiy State University of Telecommunications and Informatics, 23 L. Tolstoy, Samara, 443010, Russian Federation; Dean of the Distance Learning Faculty, Associate Professor of the Department of Multiservice Networks and Information Security; PhD in Technical Science, Associate Professor. Tel.: +79272033000. E-mail: pugin@psuti.ru

References

1. National law 29.07.2004 № 98-FZ «O kommercheskoj tajne» [For commercial secret]. 7 p.
2. Shestakova E. *Perechen' konfidencial'noj informacii* [Summary confidential information]. 2012. Available at: http://www.hr-portal.ru/article/perechen-konfidencialnoy-informacii (accessed 01.07.2017).
3. Sheredin R.V. O probleme zashchity personal'nyh dannyh [About the problem protection of personal data]. *Infoforum-Gonkong-2012*. Available at: http://pd.rkn.gov.ru/press-service/subject4/news3007/ (accessed 01.07.2017).
4. Ul'yanov V. Utechki konfidencial'noj informacii. Itogi 2013 goda [The security leakage. The 2013 results]. *Materialy analiticheskogo centra Zecurion*. Available at: http://d-russia.ru/wp-content/uploads/2014/03/Zecurion_Data_leaks_2014.pdf (accessed 01.07.2017).
5. Hodakovskij K. *Samye gromkie utechki informacii 2014 goda* [The same high-profile giveaway the 2014s]. Available at: https://3dnews.ru/907353 (accessed 01.07.2017).
6. Utechki konfidencial'noj informacii (itogi 2013 goda) [Security leakage. The 2013 results]. Available at: http://www.banki.ru/news/research/?id=6242078 (accessed 01.07.2017).
7. DLP: gromkie utechki informacii [DLP: high-profile giveaway]. Available at: http://www.tadviser.ru/index.php (accessed 01.07.2017).
8. Mihajlova A. Osnovnye kanaly utechki informacii na predpriyatii [The giveaway main canal at the company]. *Anti-Malware*. Available at: https://www.anti-malware.ru/analytics/Threats_Analysis/main-channels-information-leakage-in-enterprise (accessed 22.08.2017).
9. Panasenko A. Konfidencial'nye dannye prodolzhayut utekat' [The inside intelligence continues to flow away]. *Anti-Malware*. Available at: https://www.anti-malware.ru/analytics/Threats_Analysis/Sensitive_data_continue_leak (accessed 01.07.2017).
10. Semenov A.B., Strizhakov S.K., Sunchelej I.R. *Strukturirovannye kabel'nye sistemy* [The structured cabling system]. Moscow, DMK Press Publ., 2002. 640 p.
11. Smirnov I.G. *Strukturirovannye kabel'nye sistemy – proektirovanie, montazh, sertifikaciya* [The structured cabling system – design work, jointing, certification]. Moscow, AESP Press Publ., 2007. 348 p.
12. Semenov A.B. *Volokonno-opticheskie podsistemy sovremennyh SKS* [Fiber-optical subsystems of modern structured cabling structures]. Moscow, the Academy IT, DMK Press Publ., 2007. 632 p.
13. Grishachev V.V., Kabashkin V.N., Frolov A.D. Analiz kanalov utechki informacii v volokonno-opticheskih liniyah svyazi: narushenie polnogo vnutrennego otrazheniya [Analysis of information leakage channels in fiber-optic communication lines: violation of total internal reflection]. *Informacionnoe protivodejstvie ugrozam terrorizma*, 2005, no. 4, pp. 194-205.

14. Fedorov I.S., Orekhov I.N., Krasnoborod'ko Eh.V. Osobennosti utechki informacii po akusticheskim i vibroakusticheskim kanalam [Features of leakage of information on acoustic and vibroacoustic channels]. *Bezopasnost' informacionnyh tehnologij*, 2004, no. 1, pp. 114-118.
15. Grishachev V.V., Halyapin D.B., Shevchenko N.A., Merzlikin V.G. Novye kanaly utechki konfidencial'noj rechevoj informacii cherez volokonno-opticheskie podsistemy SKS [New channels of leakage of confidential voice information through fiber-optic subsystems of structural cable structures]. 2011. Available at: http://www.bnti.ru/showart.asp?aid=944&lvl=04.02.04. (accessed 01.07.2017).
16. Filatenkov A. Dokazatel'stva uyazvimosti VOLS [Evidence of vulnerability of fiber-optic communication line]. *Seti Network World*, 2008, no. 09. Available at: http://www.osp.ru/nets/2008/09/5300705/ (accessed 01.07.2017).
17. Grishachev V.V., Kosenko O.A., Halyapin D.B. Metody aktivnogo protivodejstviya utechke rechevoj informacii po akusto-optovolokonnym kanalam akusticheskim zashumleniem [Methods of active counteraction to leakage of speech information on acousto-optic-fiber channels by acoustic noise]. *Special'naja tehnika*, 2010, no. 3, pp. 49-62.
18. Yakovlev A.V. Volokonno-opticheskaya sistema peredachi konfidencial'noj informacii [Fiber-Optic Transmission System for Confidential Information]. *Electrosvyaz*, 1994, no. 10, p. 227.
19. Svincov. A.G. Optimizaciya parametrov opticheskogo reflektometra dlya obnaruzheniya neodnorodnosti pri popytke nesankcionirovannogo dostupa v VOSP [Optimization of parameters of an optical reflectometer for detecting inhomogeneity in an attempt to unauthorized access in a fiber-optic transmission system], *Foton-Express*, 2006, no. 6, pp. 56-71.
20. Terent'ev E.B., Halyapin D.B. Zashchita rechevoj informacii ot utechki cherez izveshchateli ohranno-pozharnoj signalizacii [The protection of voice information from leakage through fire alarms]. *Tekhnologii tekhnosfernoj bezopasnosti*, 2007, no. 5. Available at: http://www.ipb.mos.ru/ttb/2007-5/2007-5.html (accessed 28.06.2017).
21. Man'ko A., Katok V., Zadorozhnij M. Zashchita informacii na volokonno-opticheskih liniyah svyazi ot nesankcionirovannogo dostupa [Protection of information on fiber-optic communication lines from unauthorized access]. *Pravove, normativne ta metrologichne zabezpechennya sistemi zahistu informacii v Ukraïni*, 2001, no. 2, pp. 249-255. (In Ukrainian).
22. Boos A.V., Spuhardin O.N. Analiz problem obespecheniya bezopasnosti informacii, peredavaemoj po opticheskim kanalam svyazi, i puti ih resheniya [Analysis of problems of ensuring the security of information transmitted through optical communication channels and ways to solve them]. *Informacionnoe protivodejstvie ugrozam terrorizma*, 2005, no. 5, pp. 162-169.
23. Townsend P.D., Rarity J.G., Tapster P.R. Single photon interference in a 10 km long optical fibre interferometer. *Electronics Letters*, 1993, no. 29, p. 634.
24. Townsend P.D., Rarity J.G., Tapster P.R. Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel. *Electronics Letters*, 1993, no. 29, p. 1291.
25. Shapkin A.V. K voprosu o sposobah zashchity informacii pri eyo peredache v volokonno-opticheskih liniyah svyazi [On the issue of ways to protect information when it is transmitted in fiber-optic communication lines]. *Informacionnye tekhnologii, svyaz' i zashchita informacii MVD Rossii. Part 1*. 2011, pp. 52-53.
26. Glushchenko A.V., Glushchenko L.A., Tupota V.I. Matematicheskaya model' polucheniya informacii ob akusticheskom signale po otrazhennomu lazernomu izlucheniyu [Mathematical model of obtaining information about an acoustic signal by reflected laser radiation]. *Sbornik dokladov 20-oj mezhdunarodnoj konferencii «Lazery. Izmereniya. Informaciya-2010»* [Proc. 6th Int. Conference Lasers. Measurements. Information-2010"]. Part 1. St. Petersburg. 2010, pp. 209-220.
27. Alisevich E.A., Ivanov N.A., Ivanov S.A., Krasnov V.A., Starodubcev P.YU., Starodubcev Yu.I. Sposob zashchity akusticheskoj rechevoj informacii ot soputstvuyushchej peredachi po opticheskim liniyam svyazi [The method of protecting acoustic voice information from the accompanying transmission over optical links]. Patent RF, no. 2609893C1. 2017.
28. Ivchenko S.N., Shubin V.V. Sposob zashchity informacii ot nesankcionirovannogo dostupa v volokonno-opticheskih liniyah svyazi [The way to protect information from unauthorized access in fiber-optic communication lines]. Patent RF, no. 2110894. 1998.
29. Grishachev V.V. Volokonno-opticheskij detektor ugroz utechki rechevoj informacii cherez volokonno-opticheskie kommunikacii [Fiber-optical detector of threats of leakage of voice information through fiber-optic communications]. Patent RF, no. 2428798. 2011.

30. Healey P., Sikora Edmund S.R. Communicating or reproducing an audible sound. Patent US, no. 8000609. 2011.
31. Grishachev V.V., Halyapin D.B., Shevchenko N.A. Sposoby i ustrojstva aktivnoj zashchity rechevoj informacii ot proslushivaniya po akusto-opto-volokonnomu kanalu utechki [Methods and devices for active protection of voice information from listening to an acousto-optic-fiber leakage channel]. Patent RF, no. 2416166C2. 2011.
32. Treshchikov V.N., Nanij O.E. Raspredelennyj datchik akusticheskih i vibracionnyh vozdejstvij [Distributed sensor for acoustic and vibration effects]. Patent RF, no. 2532562C1, 2014.
33. Grishachev V.V., Halyapin D.B., SHevchenko N.A. Sposob i ustrojstvo aktivnoj zashchity konfidencial'noj rechevoj informacii ot utechki po akusto-opto-volokonnomu kanalu na osnove vneshnego opticheskogo zashumleniya [A method and device for actively protecting confidential voice information from leakage through an acousto-optic-fiber channel based on external optical noise]. Patent RF, no. 2416167. 2011.
34. Operational security doctrine for the fiber alarmed modem (FAM)-131 intrusion detection optical communications system (IDOCS). 28.02.1991. NSTISSI №3015. DOCID: 3353807. 11 P.
35. Nil'sen M., Chang I. *Kvantovye vychislpeniya i kvantovaya informaciya* [The quantum vychislpeniye and quantum information]. Moscow, Mir Publ., 2007. 824 p.
36. Kilin S.Ya. *Kvantovaya kriptografiya – idei praktika* [The quantum cryptography – the ideas of the practician]. Minsk, Belorusskaya nauka Publ., 2007. (in Belarusian).
37. Bernstein D.J. *Introduction to quantum cryptography*. New York: Springer. 2009. DOI https://doi.org/10.1007/978-3-540-88702-7_1
38. Russian Quantum Center Available at: http://www.rqc.ru/publications/articles/ (accessed 01.07.2017). (In Russ.)
39. Kazan Quantum Center Available at: https://kazanqc.org/ru/pubs// (accessed 01.07.2017). (In Russ.)
40. Zapushchena edinstvennaya v SNG mnogouzlovaya kvantovaya set' [The only multinodal quantum network in the CIS is started]. Available at: http://technopark.ifmo.ru/zapushhena-edinstvennaya-v-sng-mnogouzlovaya-kvantovaya-set/ (accessed 01.07.2017).
41. Shmyrov V.V. Rossii nauchilis' stavit' kvantovuyu zashchitu na dejstvuyushchie linii svyazi [Russia learned to put quantum protection on the operating communication lines]. CNews Media Available at: http://www.cnews.ru/news/top/2017-05-23_v_rossii_nauchilis_primenyat _kvantovuyu_zashchitu (accessed 01.07.2017).
42. Carpenter J., Xiong Ch., Collins M.J., Juntao Li J., Krauss T.F., Eggleton B.J., Clark A.S, Schröder J. Mode multiplexed single-photon and classical channels in a few-mode fiber. Optics Ex-press, 2013, vol. 21, no. 23, pp. 28794 – 28800.
43. Mirhosseini M., Magaña-Loaiza O.S., O'Sullivan M.N., Rodenburg B., Malik M., Lavery M. P.-J., Padgett M.J., Gauthier D.J., Boyd R.W. High-dimensional quantum cryptography with twisted light. *New Journal of Physics*, 2015, vol. 17, 033033. doi: 10.1088/1367-2630/17/3/033033.
44. Ndagano B., Nape I., Cox M.A., Rosales-Guzman C., Forbes A. Creation and characterization of vector vortex modes for classical and quantum communication. arXiv.org. 2017 (preprint).
45. GOST R 50.1.056 - 2005 «Tekhnicheskaya zashchita informacii. Osnovnye terminy i opredeleniya» ot 29 dekabrya 2005 g. [Technical information security. Main terms and definitions].
46. Edict of the President of the Russian Federation 12.05.2009 N 537, last updated 01.07.2014 «O Strategii nacional'noj bezopasnosti Rossijskoj Federacii do 2020 goda» [About the Strategy of national security of the Russian Federation till 2020]. 25 p.
47. Edict of the President of the Russian Federation 05.12.2016 N 646 «Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii» Polozhenie o licenzirovanii deyatel'nosti po tekhnicheskoj zashchite konfidencial'noj informacii [«About the approval of the Doctrine of infor-mation security of the Russian Federation» the Provision on licensing of activities for technical protection of confidential information]. Available at: http://ivo.garant.ru/#/document/71556224/paragraph/1:0 (accessed 03.07.2017).
48. Directive document Federal Service for Technical and Export Control of the Russian Federation «SVT. Zashchita ot NSD k informacii. Pokazateli zashchishchennosti ot NSD» [Computer aids. Protection against unauthorized access to information. Security indicators from unauthorized access]. 1992.
49. Horev A.A. Sredstva akusticheskoj razvedki: provodnye mikrofonnye sistemy i ehlektronnye stetoskopy [Means of acoustic investigation: wire microphone systems and electronic stethoscopes]. Spectekhnika i svyaz', 2008. no. 2, 36-42 pp.

50. Bottacchi S. *Multi-Gigabit transmission over multimode optical fibre. Theory and design methods for 10GbE systems.* West Sussex: John Wiley & Sons Ltd. 2006. 654 p.
51. Burdin A.V. *Malomodovyj rezhim peredachi opticheskih signalov po mnogomodovym voloknam: prilozheniya v sovremennyh infokommunikaciyah* [The Malomodovy mode of transfer of optical signals on multimode fibers: applications in modern infokommunikation]. Samara, PSUTI Publ., 2011. 274 p.
52. Noordegraaf D. P.M. Skovgaard, M.D. Nielsen, J. Bland-Hawthorn Efficient multi-mode to single-mode coupling in a photonic lantern. *Optics Express*. 2009. vol. 17. no. 3. pp. 1988 – 1994. doi: 10.1364/OE.17.001988
53. Leon-Saval S.G., Argyros A., Bland-Hawthorn J. Bland-Hawthorn Photonic lanterns: a study of light propagation in multimode to single-mode converters. Bland-Hawthorn. *Optics Express*. 2010. vol. 18. no. 8. pp. 8430 – 8439. doi: 10.1364/OE.18.008430.

Received 25.09.2017

УДК 621.39

ОЦЕНКА ВОЗМОЖНОЙ ЭКОНОМИИ ЭНЕРГИИ В ПАССИВНОЙ ОПТИЧЕСКОЙ СЕТИ TDM-PON

Росляков А.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: arosl@mail.ru

Одной из главных целей создания сетей будущего (Future Networks) является снижение энергозатрат на их функционирование за счет использования различных энергосберегающих технологий. Важнейшими компонентами настоящих и будущих сетей являются пассивные оптические сети (Passive Optical Network), которые широко используются для построения широкополосных сетей доступа. В статье рассмотрена методика измерения энергопотребления оборудования пассивных оптических сетей с мультиплексированием с временным разделением каналов, основанная на материалах рекомендаций Международного союза электросвязи Y.3021 и Y.3022. Получены оценки возможной экономии энергопотребления в пассивной оптической сети на базе оборудования российской компании Eltex при использовании дремлющего режима и режима циклического сна.

Ключевые слова: будущие сети, пассивная оптическая сеть TDM-PON, энергопотребление, энергосбережение, дремлющий режим, режим циклического сна

Введение

Экологические аспекты являются одним из четырех целевых сегментов, учитываемых при разработке концепции будущих сетей (Future Networks) [1], активно разрабатываемой Международным союзом электросвязи (МСЭ) [2]. Вклад телекоммуникационных технологий в снижение негативного воздействия будущих сетей на окружающую среду может быть реализован прежде всего через энергосбережение [3-5]. Но прежде чем определять пути и методы энергосбережения в будущих сетях, нужно знать величину энергии, потребляемой соответствующим телекоммуникационным оборудованием, и от чего она зависит. На этапах разработки, внедрения и последующей эксплуатации будущих сетей необходимо учитывать три уровня, каждому из которых соответствует своя технология энергосбережения [6]:

– уровень устройств: технологии, которые применяются для электронных устройств, таких как большие интегральные схемы и запоминающие устройства;

– уровень оборудования: технологии, которые применяются к одной единице оборудования (набору устройств), например маршрутизатору или коммутатору;

– уровень сети: технологии, которые применяются к оборудованию в рамках всей сети (например протокол маршрутизации, применяемый к нескольким маршрутизаторам).

Будущие сети должны задействовать эти технологии и обладать гибкостью при внедрении результатов их развития и эволюции в целях повышения эффективности энергосбережения.

На основе комбинации указанных технологий могут быть определены два основных пути энергосбережения в будущих сетях (см. рис. 1).