УДК 621.383:004.721

ЗАЩИТА ИНФОРМАЦИИ ЗА ПРЕДЕЛАМИ КОНТРОЛИРУЕМОЙ ЗОНЫ В ВОЛОКОННО-ОПТИЧЕСКИХ СЕТЯХ

В. В. Шубин
(ФГУП "РФЯЦ-ВНИИЭФ", г. Саров Нижегородской области)

Представлены подходы к защите информации за пределами контролируемой зоны в волоконно-оптических сетях. Дана классификация сетей и приведены три способа их защиты: традиционная и квантовая криптография, а также технические средства. Показаны особенности высокоскоростных волоконно-оптических систем: разреженное и плотное волновое уплотнение, фазовая манипуляция, упреждающая коррекция ошибок и многофункциональность. Дано описание традиционной и квантовой криптографии с точки зрения соответствия современным волоконно-оптическим системам и защите передаваемой информации. Представлен подход РФЯЦ-ВНИИЭФ к защите передаваемой информации по волоконно-оптическим сетям с помощью технических средств и их сравнение с другими вариантами.

Ключевые слова: защита информации, контролируемая зона, волоконно-оптическая система передачи, традиционная и квантовая криптография, техническая защита информации.

Введение

Информация, передаваемая по волоконно-оптическим сетям, за пределами контролируемой зоны (КЗ) присутствует в виде модулированного оптического сигнала, сосредоточенного преимущественно в сердцевине волокна. Безопасность информации — это конфиденциальность, доступность и целостность [1]. Обеспечить безопасность информации за пределами КЗ, где доступ нарушителя возможен с применением любых технических средств неограниченное время и в любой момент, в общем случае затруднительно. Но обеспечить конфиденциальность (защиту) информации в течение всего времени эксплуатации возможно.

Защита информации — деятельность, направленная на предотвращение утечки информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [1].

Все информационные сети делятся на две категории:

– сети общего пользования с коммутацией каналов (преимущественно телефония, телевидение, интернет и др.). Количество абонентов переменно и неизвестно, линии связи не определены и могут быть различными;
– выделенные сети с коммутацией пакетов (преимущественно распределенные автоматизированные системы). Количество абонентов строго фиксировано, линии связи определены.

Сети общего пользования подвержены сетевым атакам. Сетевая атака — это действия с использованием протоколов сетевого взаимодействия, направленные на получение несанкционированного доступа в операционную среду компьютера или на нарушение функционирования аппаратных или программных средств компьютера [2] в случае внешнего воздействия. Место, время и технические средства атаки неизвестны. Об этом можно только предполагать, исходя из стоимости информации.

Выделенные сети не подвержены сетевым атакам, так как нет доступа к сети (в случае невозможности внешних атак) от внешних ресурсов.

Вся информация делится на две категории: составляющая государственную тайну (ГТ) и информация, которая ГТ не является (персональные данные, промышленная и коммерче-

ская тайны, информация для служебного пользования и т. д.). Подход к защите двух категорий информации также различен, он зависит от стоимости последней и статуса предприятия (государственное или частное), которому эта информация принадлежит.

Государственные предприятия и организации должны подчиняться федеральным документам по защите информации. Техническую защиту информации регламентирует Федеральная служба по техническому и экспортному контролю (ФСТЭК) России. Криптографической и технической защитой информации для высших эшелонов власти занимается Федеральная служба безопасности (ФСБ) России. Частные предприятия и организации, которые являются владельцами информации, как правило, не составляющей ГТ, защищают ее по своему усмотрению. За пределами КЗ информация существует в виде сигналов передачи, которые соответствуют цифровым протоколам сетей.

Сегодня лучшими проводными каналами для информационных сетей, предназначенных для передачи на дальние расстояния, являются волоконно-оптические системы передачи (ВОСП). Современные системы и сети независимо от количества пользователей, назначения и стандарта передачи (вычислительные, телевидение, интернет, телефон, интегрированные и т. д.) делятся на три класса:

1) внутриобъектовые и бортовые сети, сети доступа (Access, WAN);
2) межобъектовые, городские сети (Metropolitan, MAN);
3) зоновые и магистральные, транспортные сети (Long-Haul, LAN).

С увеличением скорости в настоящее время системы первого класса с гибридной сети (волокно/электрокабель — HFC (hybrid fiber/coax)) переходят на полностью волоконную сеть: FTTC, FTTO, FTTH и FHHD (fiber to the curd, office, home and desk — "волокно в шкаф, офис, дом, рабочее место") [3]. Но в первом классе до сих пор присутствуют системы, относящиеся к сетям общего пользования, основанные на электрических соединениях (коаксиальные кабели и витая пара и т. д.).

По требованию сектора телекоммуникаций Международного союза электросвязи (МСЭ-Т, или в англоязычной версии ITU-T) вероятность ошибки для первого класса ВОСП должна быть не более чем 10^{-10}, для второго и третьего классов — не более 10^{-12}.

Скорость передачи и дальность для современных линий связи также зависят от класса системы: для первого класса скорость 0,1—1 Гбит/с, дальность 0,1—10 км; для второго класса скорость 1—10 Гбит/с, дальность 1—100 км; для третьего класса скорость 10—100 Гбит/с, дальность от 10 до 10 000 км и выше. Деление это весьма условно и с течением времени меняется в сторону увеличения скорости передачи.

В дальнейшем скорости передачи будут только повышаться — до 1 Тбит/с на канал и выше за счет поляризации, фазовой манипуляции, разреженного (грубого, CWDM — Coarse Wavelength Division Multiplexing) и плотного (DWDM — Dense Wavelength Division Multiplexing) волнового уплотнения в ВОСП [4, 5]. Для третьего и второго классов уже стандартизована технология оптических транспортных сетей (OTN — Optical Transport Networks). Системы третьего класса отличаются от систем второго класса большими расстояниями и, как следствие, многократным восстановлением амплитуды, формы и синхронизации сигналов (регенерация сигналов) без их преобразования в электрические (полностью оптические сети, AON — All Optical Network) [6].

Защита информации, передаваемой за пределами КЗ, возможна тремя способами: с помощью традиционной и квантовой криптографии, а также техническими средствами. Прежде чем подробнее рассмотреть защиту информации в ВОСП, необходимо указать особенности передачи для современных высокоскоростных систем.

Краткая характеристика высокоскоростных ВОСП

Уже были отмечены общие особенности современных ВОСП: они разделены на три класса независимо от количества пользователей и назначения; все ВОСП — цифровые со скоростями от 0,1 Гбит/с до 1 Тбит/с на канал и выше, с вероятностью ошибки не более 10^{-10} — 10^{-12} и дальностью от 0,1 до 10 000 км и выше.

Но есть особенности, характерные только для высокоскоростных ВОСП второго и третьего классов:

– волновое уплотнение;
– фазовая манипуляция;
– упреждающая коррекция ошибок;

– многофункциональность оптической транспортной сети.

В дальнейшем именно такие системы вытеснят ВОСП первого класса.

Волновое уплотнение. Разреженное (грубое) волновое уплотнение (разреженное мультиплексирование по длинам волн), характерное для ВОСП второго класса, применяется к O-, E-, S-, C-, L-диапазонам длин волн (1 270—1 630 нм) с шагом между каналами 20 нм и насчитывает до 19 каналов. Параметры CWDM регламентированы рекомендациями МСЭ-Т [5]. На рис. 1 показаны затухание для современных одномодовых волокон и диапазоны длин волн (обозначены цифрами и буквами).

Плотное волновое уплотнение (более плотное по сравнению с CWDM мультиплексирование по длинам волн) характерно для ВОСП третьего класса. Уплотнение информации DWDM применяется к C-диапазону длин волн (1 530—1 565 нм) или L-диапазону (1 570—1 625 нм).

Количество каналов в ВОСП зависит от шага между канальными частотами. Соотношения между шагом по длине волны (в скобках указан шаг между несущими частотами) и типовым количеством каналов следующие:

1,76 нм (200 ГГц) — до 20 каналов;
0,88 нм (100 ГГц) — до 40 каналов;
0,44 нм (50 ГГц) — до 80 каналов;
0,22 нм (25 ГГц) — до 160 каналов;
0,11 нм (12,5 ГГц) — до 320 каналов.

Параметры DWDM-систем также регламентированы рекомендациями МСЭ-Т [5].

Первый диапазон (длина волны 800—900 нм — см. рис. 1) характерен для многомодовых волокон и в настоящее время применяется только для ВОСП первого класса. При увеличении абонентских скоростей передачи данный класс ВОСП станет не нужен. Типовая ширина спектра многомодовых волокон — 600 МГц/км (не считая быстродействия передатчика и приемника ВОСП); для скорости 100 Мбит/с дальность передачи составляет максимум 2—3 км, а для скорости передачи 1 Гбит/с — сотни метров.

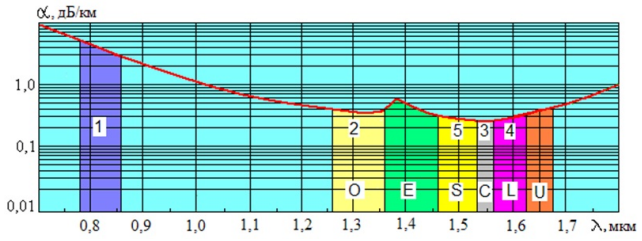


Рис. 1. Затухание для современных волокон и диапазоны длин волн [7]

Фазовая манипуляция. С увеличением скорости передачи ВОСП выше 40 Гбит/с вместо традиционной амплитудной манипуляции (ASK) применяется фазовая манипуляция (PSK). При достижении частот 40—50 ГГц электронные средства (а не оптические, что принципиально) не выдерживают передачи сигналов. Поэтому для повышения скорости передачи в канале используется фазовая манипуляция.

На рис. 2 показаны количество каналов, вид манипуляции и скорость передачи по годам для ВОСП третьего класса. Например, при скорости передачи 40 Гбит/с используется фазовая манипуляция DPSK (Dual Phase Shift Keying) — задействуются два канала по 27,8 Гбит/с (или четыре канала по 10,3 Гбит/с). Для скорости 100 Гбит/с применяется фазовая манипуляция DP-QPSK (Dual Polarization — Quarter Phase Shift Keying), в которой используются четыре канала по 27,8 Гбит/с.

Системы позволяют использовать все четыре степени свободы электромагнитного поля: амплитуду и фазу в каждой из двух поляризаций. Это позволяет в формате DP-QPSK передавать восемь битов информации из двух позиций, используя всего один уровень мощности. Таким образом, увеличивается объем передаваемой информации. Подробнее о фазовой манипуляции можно прочитать, например, в работах [9—11].

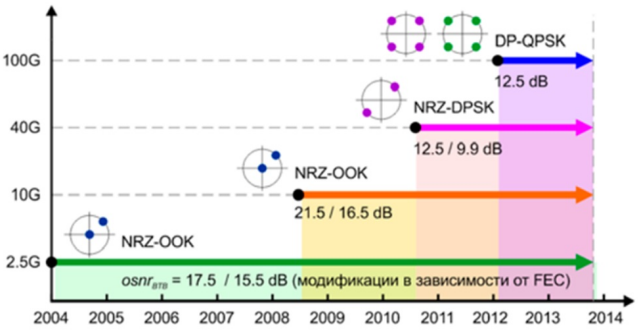


Рис. 2. Количество каналов, вид манипуляции и скорость передачи для ВОСП [8]: NRZ — кодирование без возврата к нулю; OOK (On/Off Key) — переключение включено/выключено; FEC — упреждающая коррекция ошибок; *osnr* — отношение сигнал/шум

Упреждающая коррекция ошибок. Современные ВОСП характеризуются упреждающей коррекцией ошибок (FEC — Forward Error Correction), которая позволяет автоматически обнаруживать и исправлять ошибки при передаче за счет введения избыточной информации в передаваемый сигнал. Для этого используются, например, специализированные коды Рида—Соломона (RS). Хотя такой подход требует дополнительной перекодировки сигнала на передатчике и приемнике, скорость передачи увеличивается на 7—25 %.

Параметры FEC приведены в рекомендациях МСЭ-Т [12, 13].

На рис. 3 показаны зависимости выходного коэффициента ошибок (Output BER) от входного (Input BER) для ВОСП без использования FEC (Uncoded) и с FEC (RS (255, 239), Super FEC). Видно, что при входном коэффициенте ошибок BER $= 10^{-2}$ применение FEC не имеет смысла, так как выходной и входной коэффициенты ошибок равны.

Многофункциональность оптической транспортной сети. Многофункциональность OTN заключается в том, что сеть позволяет передавать любые сигналы трех классов: плезиохронной цифровой иерархии (PDH) — E1, E2, E3, E4; синхронной цифровой иерархии (SDH) — STM-N, VC-4/VC-3; ячейки ATM, вычислительных сетей — Ethernet, пакеты IP и т. д. На рис. 4 показана структура сигнала OTN.

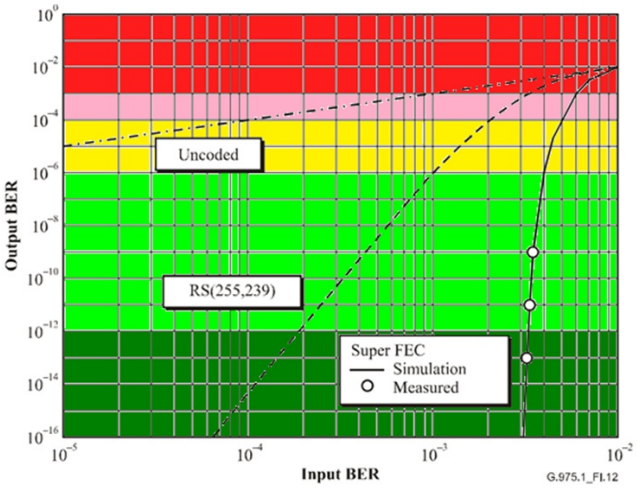


Рис. 3. Зависимости выходного BER от входного для различных систем [13]

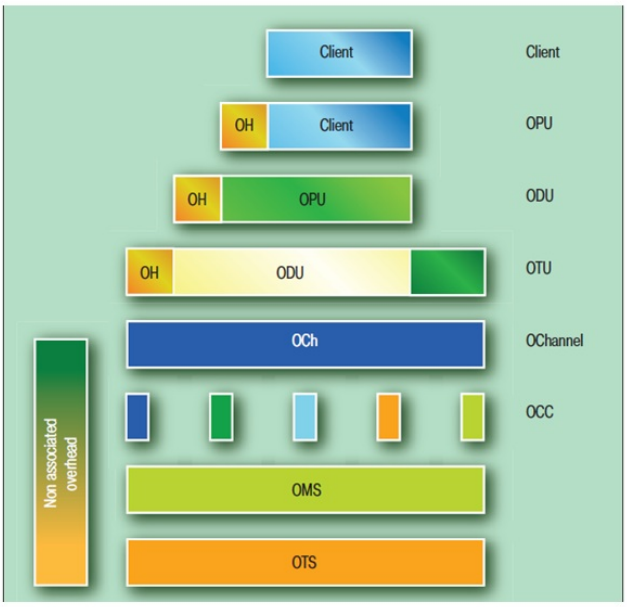


Рис. 4. Структура сигнала OTN [14]: Client — клиентская нагрузка; OH — заголовки; OPU — единица нагрузки; ODU — единица данных; FEC — модуль FEC; OTU — транспортная единица; Och — оптический канал; OCC — маркировка цветом; OMS — секция мультиплексирования; OTS — секция передачи

OTN, характерная для ВОСП второго и третьего классов, включает в себя все особенности, перечисленные выше. Контроль канала может быть осуществлен по среднему значению информационных сигналов, что предусмотрено интерфейсом OTN, фазовой манипуляцией и волновым мультиплексированием [14]. Система мониторинга методом обратного рассеивания, уже встроенная в ВОСП OTN, основана на использовании сервисного канала на одной из длин волн DWDM [14].

Устройство съема информации усложняется из-за протокола OTN, волнового мультиплексирования DWDM, использования FEC, увеличения скорости передачи на 7—25 %. Надо не просто перехватить сигнал, но и извлечь из него информацию.

В настоящее время для систем первого класса OTN, как правило, не применяется, а применяются традиционные криптографические средства защиты информации.

Защита информации с помощью традиционной криптографии

Традиционная криптография пришла в ВОСП от электрических систем, которые излучают в окружающее пространство электромагнитное поле, несущее информацию. Другого способа защиты, как шифровать саму информацию, не было, при этом вычислительная техника, с помощью которой информация расшифровывалась, находилась в зачаточном состоянии. Криптография (информационный уровень) предполагает абсолютную доступность канала передачи для нарушителя, а защита информации основана на использовании ключей, от которых полностью зависит секретность сообщения.

Клод Шеннон показал [15], что если ключ является действительно случайным, если он такой же или большей длины, что и само сообщение, и если он никогда не используется повторно, то одноразовая передача сообщения абсолютно защищена. Но на практике это далеко не так: все три условия нарушены.

Традиционная криптография предполагает, что время расшифровки информации с помощью программного обеспечения ЭВМ (задается разработчиком кода) превышает время актуальности информации. С появлением квантового компьютера и соответствующих алгоритмов расшифровки это время сократилось с нескольких лет до нескольких минут [16].

В 1994 г. П. Шором был разработан квантовый алгоритм [17], который позволяет найти за конечное и приемлемое время все простые множители больших чисел (характерно, что для всех несимметричных кодов) и, как следствие, взломать шифры, например RSA. На рис. 5 изображены длина ключа (в битах) шифра RSA, год расшифровки и предположительное время расшифровки информации с помощью ЭВМ (в годах) в сравнении со временем расшифровки с применением алгоритма П. Шора на квантовом компьютере (в часах).

RSA	cracked in	CPU years	Shor
453 bits	1999	10	1 hour
768 bits	2009	2000	5 hours
1024 bits		1000000	10 hours

Рис. 5. П. Шор и результаты расшифровки ключей шифра RSA с применением его алгоритма и без него [16]

На рис. 6 показано, что увеличение длины ключа в традиционной криптографии увеличивает время расшифровки информации с использованием ЭВМ на несколько порядков. С помощью квантового компьютера с алгоритмом П. Шора увеличение длины кода влияет на время расшифровки почти незаметно (в пределах одного порядка). То есть увеличение ключа в традиционной криптографии против алгоритма П. Шора практически ничего не дает [18]. Это означает, что при наличии квантового компьютера из 3 000 кубитов криптографическая система RSA с ключом длиной 2 048 битов может быть эффективно взломана за время, лишь ненамного превышающее время для зашифровывания. Аналогично могут быть взломаны другие криптографические асимметричные системы (алгоритмы DSA, EdDSA, El Hamal, ГОСТ Р 34.10-2012 и др.).

Отметим, что на стойкость симметричных шифров алгоритм П. Шора не распространяется. Для них применяются другие, не столь эффективные алгоритмы (метод Гровера, Саймона, BHT и др.), успешная защита от которых достигается увеличением размера параметров в 2-3 раза [19].

В 1996 г. американский математик Л. Гровер предложил другой квантовый алгоритм, основанный на методе перебора чисел. Этот алгоритм квантовые компьютеры смогут использовать для взлома систем симметричного шифрования (алгоритмы DES, 3DES, AES, BlowFish, RC2, RC4, CAST, IDEA, ГОСТ 28147-89, ГОСТ

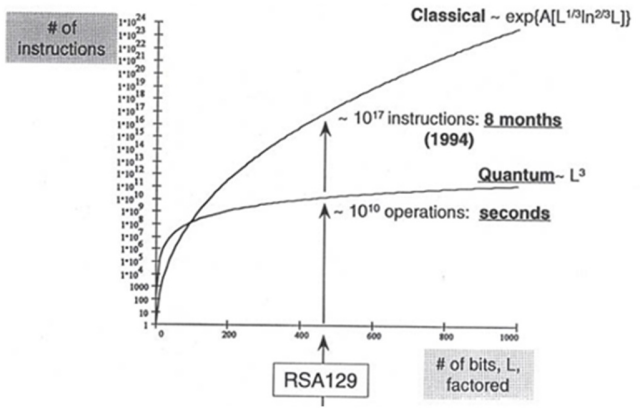


Рис. 6. Зависимость времени расшифровки от длины кода для шифра RSA [18]

Р 34.12-2015 и др.). Чтобы сохранить текущий уровень безопасности, потребуется удвоить размер ключей.

Появление квантовых вычислений неизбежно приведет к изменениям в методах шифрования. В противном случае практически все существующие системы будут достаточно быстро взломаны [20].

В России для государственных предприятий и организаций разрешено использовать только средства криптографической защиты отечественного производства [21], а алгоритм шифрования должен соответствовать документу [22]. В табл. 1 представлены некоторые устройства традиционной криптографии, их изготовители (поставщики), физический интерфейс с сетью, максимальная скорость шифрования и номера сертификатов ФСБ и ФСТЭК России.

Таким образом, средства традиционной криптографической защиты информации имеют следующие недостатки: низкая скорость передачи информации, высокая стоимость оборудования и внедрения, уязвимость информации. С появлением квантового компьютера и алгоритмов расшифровки информация, составляющая ГТ, не защищена от доступа. Традиционная криптография ориентирована на сети первого класса и стандарты вычислительных сетей (выделенные сети).

Таблица 1

Средства криптографической защиты информации, выпускаемые в России

Средство криптографической защиты информации	Разработчик, поставщик изготовитель	Физический стык с сетью	Максимальная скорость шифрования	Сертификат ФСБ, ФСТЭК
IP-шифратор "Заслон" (М-543, М-543К)	ЗАО "Голлард"	100Base-FX	Полный дуплекс 90 Мбит/с	СФ/024-2803 (ГТ) СФ/124-2804 (ДСП)
Аппаратура КЗИ "Швейцар-Я"	АО "ПНИЭИ"	100Base-TX	Менее 100 Мбит/с	СФ/124-2877 (ДСП)
Криптомаршрутизатор DPS-4024	"Фактор-ТС"	10/100/1000 Base-T; SFP (1000 Base-SX/LX); SFP (10G Base-SR/LR)	2,5 Гбит/с	СФ/124-2275 (ДСП) № 2852
Криптомаршрутизатор М479-Р2	"Фактор-ТС"	10/100/1000 Base-TX; SFP (1000 Base-SX/LX); SFP + (10G Base-SR/LR)	До 14 Гбит/с (по данным авторов)	СФ/024-3085 (ГТ)
Программно-аппаратный комплекс VIPNet Coordinator HW2000	ОАО "ИнфоТеКС"	2x10/100/1000 Base-T; 4xSFP + (10G Base-SR/LR)	До 2,7 Гбит/с	СФ/124-2606 СФ/124-2933 (ДСП)
АПКШ "Континент 3М", платформа IPC-1000F	НИП "Информ-защита"	2x10/100/1000 Base-T; 2xSFP (1000 Base-X)	До 800 Мбит/с	СФ/525-2741 № 1804 (ДСП)
АПКШ "Континент 3.7", платформа IPC-3000F	НИП "Информ-защита"	10x10/100/1000 Base-T; 4xSFP + (10G)	До 2,5 Гбит/с	СФ/124-2617 СФ/124-2871 СФ/124-2918 СФ/124-2919 СФ/124-2921 № 3007 № 3008 (ДСП)

Преимущества традиционной криптографии проявляются при ее применении для защиты информации в сетях общего пользования (независимость от среды передачи: оптическое волокно, коаксиальный кабель, спутниковая связь и т. д.). Также к преимуществам можно отнести наличие государственной нормативно-методическаой документации (НМД).

Стоит обратить внимание, что в главе 3.5 НМД по AON, действующей в США [6], нет даже упоминаний о традиционной криптографии как методе защиты информации в волоконно-оптических сетях. Исходя из недостатков, разработчики и пользователи средств защиты информации обратили внимание на новую область техники — квантовую криптографию.

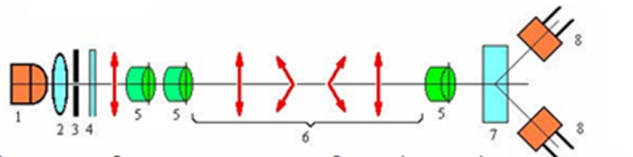
Защита информации в оптическом волокне с помощью квантовой криптографии

Теоретически с помощью квантовой криптографии информация полностью защищена от несанкционированного доступа нарушителя. Невозможность доступа к информации базируется на двух принципах квантовой криптографии:

- невозможность клонирования (копирования) неизвестного квантового состояния без изменений в самой системе (принцип неопределенности Гейзенберга);
- эффект квантового перепутывания, который заключается в том, что две и более квантовые системы могут находиться в состоянии взаимной корреляции и влиять друг на друга.

На основе этих двух принципов создано несколько протоколов квантовой криптографии (BB84, B92, BB84(4+2), E91, Гольденберга—Вайдмана, Коаши—Имото и др.). Первый оптический протокол BB84 (остальные протоколы, кроме E91, являются его модификациями) представлен на рис. 7. Ч. Беннет и Ж. Брассард провели свой опыт на *оптической скамье* (длина оптического пути 32 см) с поляризацией единичных фотонов [23] и создали протокол BB84, который в квантовой криптографии до сих пор является основным.

К сожалению, на практике при переходе от оптической скамьи к протяженной волоконно-оптической линии в квантово-криптографических системах возникают



1 – источник 2 – оптическая система 3 – диафрагма 4 – поляризатор
5 – ячейка Поккельса 6 – воздух 7 – кальциадная призма 8 - ФЭУ

Пример протокола передачи квантовой криптографии

Передаваемый бит	1	0	1	0	0	1	0	0
Плоскость поляризации, град.	45	0	45	0	135	45	135	90
Поляризация приема	Д	О	О	Д	О	О	Д	Д
Принимаемый бит	1	0	0	1	1	0	0	1
Результат приема	+	+	–	–	–	–	+	–

Примечание: О – ортогональная, Д – диагональная плоскость поляризации.

Рис. 7. Схема реализации протокола BB84 [23]

неразрешимые проблемы, с которыми разработчики этих систем борются и в настоящее время. Эти проблемы приводят к тому, что параметры ВОСП не обеспечивают защиту информации. Как результат — несоответствие устройств квантовой криптографии параметрам современных ВОСП: низкая скорость передачи ключа (несколько десятков-сотен кбит/с), высокая вероятность ошибки (единицы-десятки процентов), дальность в пределах одного пролета ВОСП, возможность выведения системы из строя и формирование сигнала квантового ключа со стороны (уязвимость защиты информации).

Чтобы соответствовать показателям ВОСП, с помощью квантовой криптографии формируется только ключ, а передача информации выполняется с применением традиционной криптографии. В отличие от традиционной криптографии, где ключ формируется математически, квантово-криптографическим путем ключ формируется на меньшее время. На рис. 8 показана схема такого использования ключа [24], называемого квантовым распределением ключей (КРК, или в англоязычной версии QKD — Quantum Key Distribution).

Существуют различные схемы формирования оптического квантового ключа: с кодированием по положению плоскости поляризации [25], фазы излучения [26], на временных сдвигах [27], на боковых частотах [28]. Например, схема формирования квантового ключа (по положению фазы излучения) в системе ID Clavis^2 за два прохода излучения показана на рис. 9.

Аппаратура для квантовых систем ВОСП выпускается во всем мире [29—33]. В России квантовым центром КНИТУ-КАИ им. А. Н. Туполева (г. Казань) совместно с квантовой лаборато-

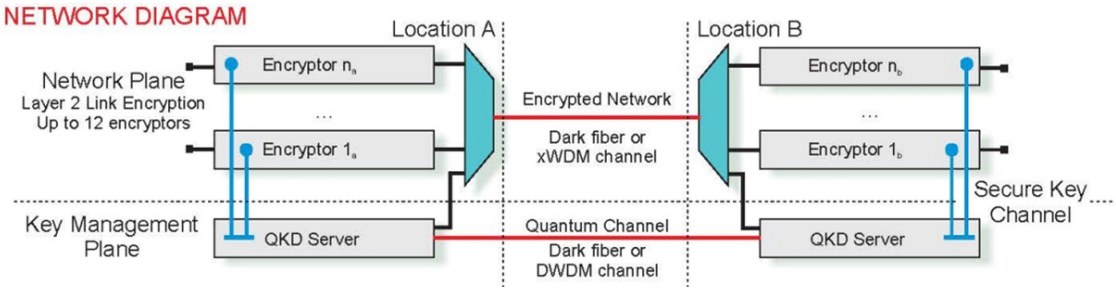


Рис. 8. Схема квантового распределения ключей [24]

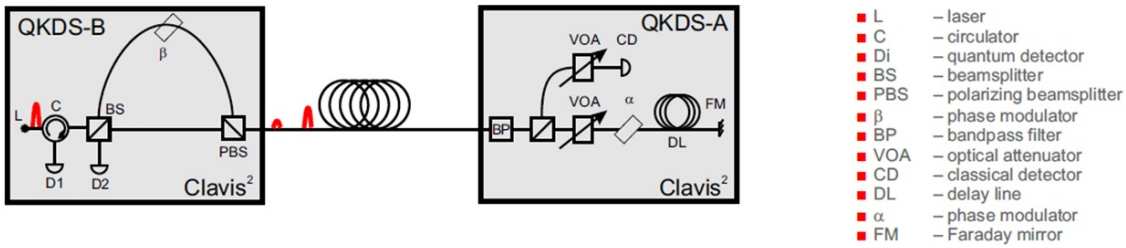


Рис. 9. Схема формирования квантового ключа в системе ID Clavis^2 [28]

рией университета ИТМО (г. Санкт-Петербург) создана аппаратура ВОСП на основе КРК на боковых частотах [28], которая там же и тестируется.

В табл. 2 представлены характеристики некоторых квантово-криптографических систем.

Криптоанализ оптической серийной аппаратуры практически показал уязвимость защиты информации в квантово-криптографических системах. В этих системах разделяются *некогерентная* (однофотонная) атака [34], *когерентная* (совместная) [35] и *коллективная* [36] атаки.

Таблица 2

Основные параметры некоторых квантово-криптографических систем

Производитель	Система	Протоколы (кол-во бит в ключе)	Дальность передачи, км	Скорость передачи ключа, кбит/с	Спектральная эффективность (предел), %	Цена, тыс. евро
ID Quantique (Швейцария)	ID 500, Clavis	BB84, SARG04	Нет данных	1,28—2,56	Нет данных	Нет данных
	Clavis^{23}	Нет данных	100	1	4	90
	Cerberis	BB84, SARG04, AES (256 бит)	50	Нет данных	Нет данных	70
MagiQ Technologies (США)	QPN 8505	BB84, DES (112 бит) AES (256 бит)	140	0,1	Нет данных	80
Smart Quantum (Франция)	SQ Box	Нет данных	140	0,023	4	Нет данных
SeQureNet	Cygnus	Нет данных	Нет данных	0,1	4	Нет данных
ИТМО, КНИТУ–КАИ (Россия)	SCW-QC	BB84	250	10	40—50	Нет данных

Основой этих атак является открытый доступ к волокну и срабатывание системы контроля не по чувствительному параметру, а по коэффициенту ошибок [37]. То есть контроль слишком грубый.

Таким образом, можно сказать, что квантово-криптографические системы для ВОСП по сравнению с устройствами традиционной криптографии в большей части обладают недостатками. Это:

- уязвимость по защите информации в волокне ВОСП (нет защиты информации, заявленной теоретически);
- низкая скорость передачи информации (даже при КРК), копирование ключей квантовой криптографии только на одном пролете;
- отсутствие НМД (многообразие систем квантовой криптографии и атак на эти системы);
- высокая стоимость оборудования;
- привязка к волокну (нет независимости передачи от среды).

Криптография (как традиционная, так и квантовая) основана на полном доступе к волокну в течение неограниченного времени, а защита информации строится на незнании ключа нарушителем. Нельзя за пределами КЗ закрыть доступ к волокну. Но можно быстро отключить передачу сигналов и не допустить утечки передаваемой информации с помощью технических средств.

Технические средства защиты информации в оптическом волокне

Техническая защита информации от возможности доступа за пределами КЗ основана на защите волоконного канала передачи, а не самой информации. Техническая защита предусматривает быстрое отключение (переключение) передачи информационных сигналов в случае обнаружения непредвиденных локальных потерь в волокне.

Средства нарушителя используют как *неинтрузивные* (без вторжения в волокно), так и *интрузивные* (с вторжением в волокно) методы. Способы основаны на извлечении мощности информационного сигнала из волокна (*активные* способы) либо на извлечении и возвращении мощности в волокно (*компенсационные* способы) [38].

В случае любого вторжения в волокно мощность W_0 информационного сигнала в волокне ограничена, а порог $A_д$ срабатывания системы защиты (при заданных вероятности обнаружения и среднего времени наработки системы на ложную тревогу) определяется применяемой аппаратурой защиты информации [39]. Мощность информационного сигнала в самом критическом случае (устройство съема находится у передатчика ВОСП) составит

$$W_0 = W_п - A(\mathrm{BER}) - \\ - 10\lg\left(K_п(1-10^{-0{,}1A_д})\right)\ [\text{дБм}],$$

где $W_п$ [дБм] — предельная чувствительность оптического приемника информации (на канал) нарушителя при коэффициенте ошибок $\mathrm{BER} = 10^{-9}$; $A(\mathrm{BER})$ [дБ] — поправка чувствительности приемника нарушителя при переходе BER с 10^{-9} на 10^{-2}; $K_п$ [отн. ед.] — коэффициент передачи излучения через боковую поверхность волокна; $A_д$ [дБ] — порог срабатывания системы защиты ВОСП (при заданных вероятности обнаружения нарушения и среднего времени наработки системы защиты на ложную тревогу).

В случае компенсационного вторжения при совпадении других параметров (мощности, длины волны (волн), фазы, длительности и т. д.) время между выводом и вводом излучения составляет несколько десятых долей секунды [20].

На этих принципах построена НМД ФСТЭК России по технической защите информации, как составляющей ГТ [40], так и ее не содержащей [20]. Требования ФСБ России к ВОСП по защите информации содержатся в документе [19].

В 2007—2014 гг. в РФЯЦ-ВНИИЭФ были разработаны, а затем сертифицированы ФСТЭК России [41] устройства защиты информации в волокне ВОСП — конверторы среды FOBOS-100M (S.L, F, FL и m) с контролем мощности по среднему информационному сигналу (метод прямого доступа). В конверторах для защиты информации применялось специально разработанное программное обеспечение, которое было основано на теории обнаружения сигналов на фоне случайных помех [42—44]. Такое программное средство позволило повысить чувствительность системы защиты волокна на два порядка.

Носителем программного обеспечения является встроенный в устройство PIC микроконтроллер. Конверторы среды FOBOS-100M (S.L, F, FL и m) применялись только для стандарта "Fast Ethernet" [45, 46] (вычислительные сети, ВОСП первого класса) и были внедрены как в серийное

производство (выпущено около 500 штук), так и эксплуатацию в составе ВОСП. Устройства неоднократно экспонировались на выставках "Технологии безопасности" (2012—2014 гг.) и др., защищены несколькими патентами на изобретения.

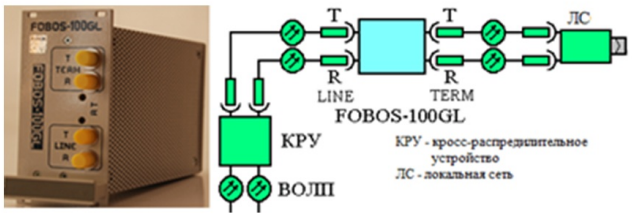
На тех же принципах в 2015—2020 гг. в РФЯЦ-ВНИИЭФ были разработаны, поставлены на производство и сертифицированы ФСТЭК России [47] (дано положительное заключение ФСБ России) универсальные средства защиты информации — контроллеры FOBOS-100GL (10GS, GE) (ВОСП первого и второго класса). Это устройства с оптическим входом и выходом информации, не имеющие ограничений по скорости, типу протоколов и количеству каналов (в пределах установленной мощности передачи информации).

На рис. 10 показаны внешний вид, основные параметры контроллера FOBOS-100GL и одна из схем его включения в локальную сеть [7]. Внешний вид конверторов среды FOBOS-100L, S, M [7] показан на рис. 11.

В 2016—2018 гг. контроллеры не раз экспонировались на выставках "Технологии безопасности" и др., награждены дипломами, признаны победителями конкурса "100 лучших товаров" в Нижегородской области и России, устройства и программа защищены в России несколькими патентами на изобретения.

В обоих устройствах применен метод прямого детектирования (контролируется разность мощности между передачей и приемом информации, т. е. коэффициент передачи между полюсами). Это косвенное измерение локальных потерь в волокне.

Метод обратного рассеяния основан на временной рефлектометрии (OTDR — Optical Time



Пропускная способность от 100 Мбит на канал
Стандарт передачи и тип оптического кабеля – любой
Дальность передачи: до 100 км
Порог отключения передачи информации 0,02 дБ
Время реакции на отключение передачи менее 0,2 с

Рис. 10. Внешний вид контроллера FOBOS-100GL, его основные параметры и пример схемы включения

Рис. 11. Внешний вид конверторов среды FOBOS-100L, S, M

Domain Reflectometer) и измеряет локальные потери, т. е. контролирует непосредственно отвод мощности из волокна. Он имеет преимущество по сравнению с методом прямого детектирования по основным параметрам — точности, времени наблюдения и мониторингу. Исключение составляют время реакции (необходима обработка сигнала) и применимости (необходима отдельная длина волны для рефлектометрии волокна).

Таким образом, оптимальным является сочетание применения обоих методов в одном устройстве системы контроля: метода обратного рассеяния, характеризуемого точностью измерения, и метода прямого детектирования, обеспечивающего быстроту реакции.

Впервые в России в РФЯЦ-ВНИИЭФ в 2018—2020 гг. был разработан комплексный контроллер защиты, основанный на двух методах — прямого детектирования и обратного рассеивания [48]. На рис. 12 показаны внешний вид платы устройства, осциллограмма подключения устройства нарушения, полученная методом обратного рассеяния, и экспериментальная установка для тестирования платы.

Методы защиты данного устройства для AON описаны в зарубежной НМД [16] и хорошо соответствуют отечественной приемопередающей аппаратуре ВОСП [50], предназначенной для сетей второго и третьего класса. Устройство экспонировалось на выставках и защищено несколькими патентами на изобретения.

Таким образом, научно-технический задел РФЯЦ-ВНИИЭФ по техническим средствам за-

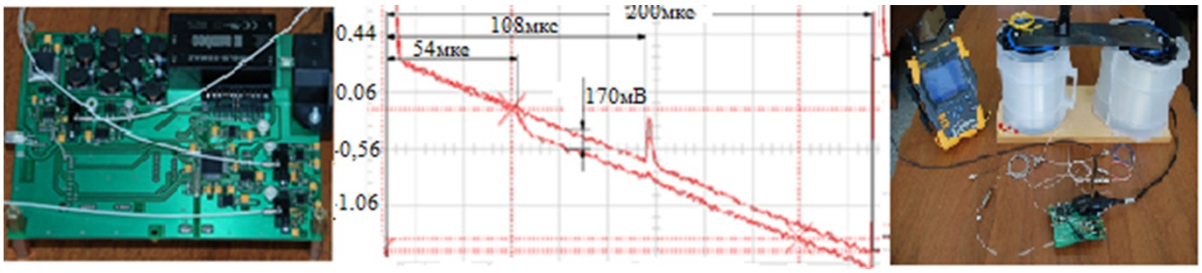


Рис. 12. Внешний вид платы, осциллограмма подключения устройства нарушения и экспериментальная установка для тестирования [49]

щиты позволяет разрабатывать, сертифицировать и серийно производить новые устройства, основанные на двух методах технической защиты информации.

Сравнение способов защиты информации в оптических волокнах

Сравнение способов защиты информации, передаваемой за пределами КЗ по оптическому волокну, основанных на традиционной и квантовой криптографии, а также технических средствах, представлено в табл. 3. Прокомментируем приведенные в ней данные.

Область применения. Традиционная криптография не зависит от среды передачи и может применяться в любой сети, чего нельзя сказать о квантовой криптографии и технических средствах защиты, которые "привязаны" к оптическому волокну, применяемому только в ВОСП.

Степень защищенности информации. Этот показатель зависит от того, какие средства перехвата использует нарушитель, а они, в свою очередь, — от стоимости и принадлежности информации. При перехвате информации, составляющей ГТ, спецслужбами зарубежных стран используются все возможные средства.

Таблица 3

Сравнение способов защиты информации в оптическом волокне

Способ защиты информации	Область применения	Степень защищенности информации	Скорость передачи информации на канал, Гбит/с	Тип манипуляции	Максимальная дальность связи, км	Универсальность к протоколам передачи	Наличие НМД	Стоимость аппаратуры защиты информации, тыс. руб.
Традиционная криптография	Сети общего пользования, выделенные сети	Средняя	До 10	Амплитудная	Нет ограничений	Нет	Есть	$2\,000N^*$
Квантовая криптография	Выделенные сети с оптическим волокном	Средняя	До 10 (при КРК)	Амплитудная	Один пролет для квантового ключа	Нет	Нет	$8\,000+$ $+\,2\,000N$
Технические средства	Выделенные сети с оптическим волокном	Высокая	Нет ограничений	Нет ограничений	Нет данных	Да	Есть	400

$^*N$ — число каналов

Для информации, не содержащей ГТ, частные лица используют средства, которые существуют в свободной продаже. Поэтому можно считать информацию, для которой применяется традиционная и квантовая криптография, недостаточно защищенной от спецслужб иностранных государств. Техническая защита определяется предельными возможностями средств нарушения оптических волокон, используемых в ВОСП.

Скорость передачи информации на канал. Как в традиционной, так и квантовой криптографии (при КРК) скорость передачи информации определяется скоростью в устройствах традиционной криптографии (на сегодняшний день до 10 Гбит/с). При использовании технических средств защиты информации скорость передачи не ограничена.

Тип манипуляции. В криптографии используется только амплитудная манипуляция (это связано, вероятно, со скоростью передачи). Технические средства защиты информации не зависят от типа манипуляции (амплитудная, фазовая и т. д.).

Дальность связи. В традиционной криптографии она не ограничена. В квантовой криптографии передача привязана к оптическому волокну, а передача квантового кода — к одному пролету ВОСП. Для технической защиты нет принципиальных ограничений в дальности связи, но она не определена экспериментально.

Универсальность к протоколам передачи. Криптографические средства связаны с определенным протоколом передачи, а технические средства, которые используют пилот-сигнал и среднюю мощность при передаче, открыты для любых сигналов (в том числе для CWDM и DWDM в любом диапазоне).

Наличие НМД. Для внедрения в эксплуатацию устройств традиционной криптографии и технических средств, предназначенных для передачи информации разного характера, есть НМД. Для средств квантовой криптографии такой документации нет (по крайней мере, о ее наличии автору не известно).

Стоимость аппаратуры защиты информации. Технические средства стоят в среднем в 5 раз дешевле устройств традиционной криптографии и в 20 раз дешевле устройств формирования квантового ключа (без учета КРК).

При увеличении числа каналов в технических средствах защиты информации устройства традиционной криптографии не добавляются, а к квантовому каналу (при КРК) добавляются, что соответственно влияет на стоимость аппаратуры.

Заключение

По всем выбранным показателям для ВОСП технические средства защиты информации имеют преимущества перед устройствами традиционной и квантовой криптографии. Устройства технической защиты должны быть универсальны по отношению к протоколам и скорости передачи информации и построены для ВОСП всех классов. В технических средствах защиты рекомендуется использовать пилот-сигналы и строить их на основе двух методов — прямого детектирования и обратного рассеяния.

Традиционная криптография не зависит от среды передачи и защищает информацию, не составляющую ГТ, от обычных пользователей в сетях общего пользования. Традиционная криптография является единственным средством защиты для гибридных систем первого класса (основанных не на ВОСП).

При переходе систем первого класса полностью на ВОСП, доступности квантового компьютера и алгоритма П. Шора для широкого пользования квантовая криптография полностью заменит традиционную криптографию. По крайней мере, так думают многие пользователи.

Однако для сетей второго и третьего классов квантовая криптография не соответствует требованиям ВОСП по основным параметрам (скорости, дальности, вероятности ошибки) и стоимости.

Технические средства защиты РФЯЦ-ВНИИЭФ в состоянии обеспечить защиту информации ВОСП всех трех классов независимо от характера информации.

Список литературы

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
   GOST R 50922-2006. Zashchita informatsii. Osnovnye terminy i opredeleniya.
2. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Термины и определения.
   GOST R 53114-2008. Zashchita informatsii. Obespechenie informatsionnoy bezopasnosti v organizatsii. Terminy i opredeleniya.
3. *Шубин В. В.* Волоконно-оптические системы и информационная безопасность. С.-Пб.: ИВА, 2006.

Shubin V. V. Volokonno-opticheskiye sistemy i informatsionnaya bezopasnost. S.-Pb.: IVA, 2006.

4. ITU-T. G.694.1. Spectral grids for WDM applications: DWDM frequency grid.
5. ITU-T. G.694.2. Spectral grids for WDM applications: CWDM wavelength grid.
6. All-optical network (AON). National communications system. NCS TIB 00-7. 2000.
7. *Шубин В. В.* Информационная безопасность волоконно-оптических систем. Саров: РФЯЦ-ВНИИЭФ, 2015.
   Shubin V. V. Informatsionnaya bezopasnost volokonno-opticheskikh system. Sarov: RFYaTs-VNIIEF, 2015.
8. *Трещиков В. Н., Наний О. Е.* Новое поколение DWDM — систем связи // Фотон-экспресс. 2014. № 4 (116). С. 18—23.
   Treshchikov V. N., Naniy O. E. Novoe pokolenie DWDM — system svyazi // Foton-ekspress. 2014. № 4 (116). S. 18—23.
9. *Наний О. Е., Трещиков В. Н.* Российское оборудование 40 Гбит/с — реальность! // Там же. 2010. № 5 (85). С. 28—30.
   Naniy O. E., Treshchikov V. N. Rossiyskoe oborudovanie 40 Gbit/s — realnost! // Tam zhe. 2010. № 5 (85). S. 28—30.
10. *Гуркин Н. В., Капин Ю. А., Павлов В. Н., Плаксин С. О., Трещиков В. Н.* Характеристики однопролетной системы DWDM с каналами 40 Гбит/с DPSK в сетке 50 ГГц // Электросвязь. 2012. № 1. www: t8.ru/?p=1777.
    Gurkin N. V., Kapin Yu. A., Pavlov V. N., Plaksin S. O., Treshchikov V. N. Kharakteristiki odnoprolyetnoy sistemy DWDM s kanalami 40 Gbit/s DPSK v setke 50 GGts // Elektrosvyaz. 2012. № 1. www: t8.ru/?p=1777.
11. *Гуркин Н. В., Трещиков В. Н., Наний О. Е.* Оптические когерентные DWDM системы связи с канальной скоростью 100 Гбит/с // Фотон-экспресс. 2014. № 4. С. 24—27.
    Gurkin N. V., Treshchikov V. N., Naniy O. E. Opticheskie kogerentnye DWDM sistemy Svyazi c kanalnoy skorostyu 100 Gbit/s // Foton-ekspress. 2014. № 4. S. 24—27.
12. ITU-T. G.975. Forward error correction for submarine systems.
13. ITU-T. G.975.1. Forward error correction for high bit-rate DWDM submarine systems.
14. ITU-T. G.709. Interfaces for the optical transport network.
15. *Shannon C. E.* Communication theory of secrecy systems. https://archive.org.
16. *Страхова С. И.* Философия квантовых вычислений. "Квантовая механика наноразмерных структур". https://nuclphys.sinp.msu.ru/qmns/8-9.pdf.
    Strakhova S. I. Filosofiya kvantovykh vychisleniy. "Kvantovaya mekhanika nanorazmernykh struktur". https://nuclphys.sinp.msu.ru/qmns/8-9.pdf.
17. *Shor P.* Algorithms for quantum computation: discrete logarithms and factoring // Proc. 35th Annual Symposium on Foundations of Computer Science. Los Alamitos: IEEE Computer Society, 1994. P. 124.
18. Основы квантовых вычислений. https://gerdt.
    Osnovy kvanovykh vychisleniy. https://gerdt.
19. Общие специальные требования для волоконно-оптических систем передачи. ФСБ России, 2012.
    Obshchie spetsialnye trebovaniya dlya volokonno-opticheskikh system peredachi. FSB Rossii, 2012.
20. Сборник методических документов по технической защите информации, не содержащей сведения составляющих государственную тайну, в волоконно-оптических системах передачи информации. ФСТЭК России, 2012.
    Sbornik metodicheskikh dokumentov po tekhnicheskoy zashchite informatsii, ne soderzhashchey cvedeniya, sostavlyayushchie gosudarstvennuyu taynu, v volokonno-opticheskikh sistemakh peredachi informatsii. FSTEK Rossii, 2012.
21. Положение о сертификации средств защиты информации. Постановление Правительства РФ от 26 июня 1995 г. № 608 (с изменениями и дополнениями от 23 апреля 1996 г. № 509; от 29 марта 1999 г. № 342; от 17 декабря 2004 г. № 808).
    Polozhenie o sertifikatsii sredstv zashchity informatsii. Postanovlenie Pravitelstva RF ot 26 iyunya 1995 g. № 608 (s izmeneniyami i

dopolneniyami ot 23 aprelya 1996 g. № 509; ot 29 marta 1999 g. № 342; ot 17 dekabrya 2004 g. № 808).

22. ГОСТ 28147-87. Система обработки информации, защищенной криптографией. Алгоритм криптографического преобразования.
GOST 28147-87. Sistema obrabotki informatsii, zashchishchyennoy kriptografiey. Algoritm kriptograficheskogo preobrazovaniya.

23. *Bennett C., Brassard G.* Quantum cryptography: Public key distribution and coin tossing // Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing. N.-Y., 1984. P. 175—179.

24. Redefining Security Cerberis the Best of Classical and Quantum Worlds. Geneva: ID Quantique SA, 2012. www:idquantique.com.

25. *Muller A., Breguet J., Gisin N.* Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km // Europhysics Lett. 1993. Vol. 23. P. 383—388.

26. *Bennett C. H.* Quantum cryptography using any two non-orthogonal states // Phys. Rev. Lett. 1992. Vol. 68. P. 3121—3124.

27. *Молотков С. Н.* Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы // Письма в ЖЭТФ. Т. 79, вып. 11. С. 691—704.
Molotkov S. N. Ob integrirovanii kvanovykh system zasekrechennoy svyazi (kvantovoy kriptografii) v optovolokonnye telekommunikatsionnye sistemy // Pisma v ZhETF. T. 79, vyp. 11. S. 691—704.

28. *Gleim A. V., Egorov V. I., Nazarov Y. V. и др.* Secure polarization — independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference // Optical express. 2016. Vol. 24, No 3. P. 2619—2633.

29. *Gobby C., Yuan Z., Shields A.* Quantum key distribution over 122 km of standard telecom fiber // Appl. Phys. Lett. 2004. Vol. 84. P. 3762—3764.

30. *Corndorf E., Liang C., Kanter G. S., Kumar P., Yuen H. P.* Quantum-noise randomized data-encryption for WDM fiber-optic networks // Physical Review A. 2005. Vol. 71(6). Paper 062326.

31. *Takesue H., Diamanti E., Honjo T., Langrock C., Fejer M. M., Inoue K., Yamamoto Y.* Differential phase shift quantum key distribution experiment over 105 km fiber // New J. Phys. 2005. Vol. 7. P. 232.

32. *Kimura T., Nambu Y., Hatanaka T., Tomita A., Kosaka H., Nakamura K.* Single-photon interference over 150 km transmission using silica-based integrated optic interferometers for quantum cryptography // Jpn. J. Appl. Phys. 2004. Vol. 43. P. L1217—L1219.

33. *Hughes R., Morgan G., Peterson C.* Practical quantum key distribution over a 48 km optical fiber network // J. Mod. Opt. 2000. Vol. 47. P. 533—547.

34. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography // Rev. Modern Phys. 2002. Vol. 74(1). P. 145.

35. *Mayers D.* Unconditional sequrity in quantum cryptographi // Quant-Ph. 1998. Paper 9802025.

36. *Biham E., Boyer M., Brassard G., J. Van de Graaf, Mor T.* Security of quantum key distribution against all collective attacks // Ibid. 1998. Paper 9801022.

37. *Кронберг Д. А., Ожигов Ю. И., Черняевский А. Ю.* Квантовая криптография. Учеб. пособие. М.: МГУ им. М. В. Ломоносова. http://sqi.cs.msu.su/store/storage/ss8dw5n_quantum_cryptography.pdf.
Kronberg D. A., Ozhigov Yu. I., Chernyavskiy A. Yu. Kvanovaya kriptografiya. Ucheb. posobie. M.: MGU im. M. V. Lomonosova. http://sqi.cs.msu.su/store/storage/ss8dw5n_quantum_cryptography.pdf.

38. *Волков А. П., Зайцев А. Л., Ивченко С. Н., Кращенко И. А., Курило А. П., Попов С. Н., Шубин В. В.* Исходные данные для построения модели съема информации, передаваемой по волоконно-оптическому тракту // Вопросы защиты информации. 1989. № 1(24). С. 43—48.
Volkov A. P., Zaytsev A. L., Ivchenko S. N., Krashchenko I. A., Kurilo A. P., Popov S. N., Shubin V. V. Iskhodnye dannye dlya postroeniya modeli syema informatsii, peredavaemoy po volokonno-opticheskomu

traktu // Voprosy zashchity informatsii. 1989. № 1(24). S. 43—48.

39. *Волков А. П., Зайцев А. Л., Ивченко С. Н., Кращенко И. А., Курило А. П., Попов С. Н., Шубин В. В.* О защите информации в волоконно-оптических системах // Там же. С. 37—42.
Volkov A. P., Zaytsev A. L., Ivchenko S. N., Krashchenko I. A., Kurilo A. P., Popov S. N., Shubin V. V. O zashchite informatsii v volokonno-opticheskikh sistemakh // Tam zhe. S. 37—42.

40. Сборник нормативно-методических документов по технической защите информации, содержащей сведения составляющих государственную тайну, в волоконно-оптических системах передачи информации. ФСТЭК России. 2006.
Sbornik normativno-metodicheskikh dokumentov po tekhnicheskoy zashchite informatsii, soderzhashchey svedeniya, sostavlyayushchie gosudarstvennuyu taynu, v volokonno-opticheskikh sistemakh peredachi informatsii. FSTEK Rossii. 2006.

41. Система сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00. Сертификат соответствия № 1520 от 04 декабря 2007. www.fstec.ru.
Sistema sertifikatsii sredstv zashchity informatsii po trebovaniyam bezopasnosti informatsii № ROSS RU.0001.01BI00. Sertifikat sootvetstviya № 1520 ot 04 dekabya 2007. www.fstec.ru.

42. Патент на изобретение № 2349039. Способ повышения вероятности обнаружения вывода излучения из оптического волокна / В. В. Шубин, С. И. Овечкин, С. Н. Ивченко. 10.03.2009.
Patent na izobretenie № 2349039. Sposob povysheniya veroyatnosti obnaruzheniya vyvoda izlucheniya iz opticheskogo volokna / V V. Shubin, S. I. Ovechkin, S. N. Ivchenko. 10.03.2009.

43. Патент на изобретение № 2350018. Способ обнаружения вывода излучения с боковой поверхности оптического волокна / В. В. Шубин. 20.03.2009.
Patent na izobretenie № 2350018. Sposob obnaruzheniya vyvoda izlucheniya s bokovoy poverkhnosti opticheskogo volokna / V. V. Shubin. 20.03.2009.

44. Патент на изобретение № 2350019. Способ устранения ложных срабатываний при включении защищенных волоконно-оптических систем / В. В. Шубин, С. И. Овечкин. 20.03.2009. www:patents.google.com/patent/RU2350019C2/ru.
Patent na izobretenie № 2350019. Sposob ustraneniya lozhnykh srabatyvaniy pri vklyuchenii zashchishchyennykh volokonno-opticheskikh system / V V. Shubin, S. I. Ovechkin. 20.03.2009. www:patents.google.com/patent/RU2350019C2/ru.

45. Патент на изобретение № 2297102. Приемопередающее устройство защищенной волоконно-оптической системы передачи информации ограниченного доступа / В. В. Шубин, С. Н. Ивченко, С. И. Овечкин. 19.04.2007.
Patent na izobretenie № 2297102. Priyemo-peredayushchee ustroystvo zashchishchyennoy volokonno-opticheskoy sistemy peredachi informatsii ogranichennogo dostupa / V. V. Shubin, S. N. Ivchenko, S. I. Ovechkin. 19.04.2007.

46. Патент на изобретение № 2301497. Способ обнаружения доступа к оптическому сигналу при передаче по волоконно-оптическим линиям / В. В. Шубин, С. Н. Ивченко, С. И. Овечкин. 20.06.2007.
Patent na izobretenie № 2301497. Sposob obnaruzheniya dostupa k opticheskomu signalu pri peredache po volokonno-opticheskim liniyam / V V. Shubin, S. N. Ivchenko, S. I. Ovechkin. 20.06.2007.

47. Система сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00. Сертификат соответствия № 3329 от 30 декабря 2014.
Sistema sertifikatsii sredstv zashchity informatsii po trebovaniyam bezopasnosti informatsii № ROSS RU.0001.01BI00. Sertifikat sootvetstviya № 3329 ot 30 dekabrya 2014.

48. Патент на изобретение № 2611588. Устройство комплексного контроля волоконно-оптической линии / К. И. Балашов, В. В. Шубин. 28.02.2017.

Patent na izobretenie № 2611588. Ustroystvo kompleksnogo kontrolya volokonno-opticheskoy linii / K. I. Balashov, V. V. Shubin. 28.02.2017.

49. Основные достижения РФЯЦ-ВНИИЭФ 2020. Саров: РФЯЦ-ВНИИЭФ, 2021. С. 17. Osnovnye dostizheniya RFYaTs-VNIIEF 2020. Sarov: RFYaTs-VNIIEF, 2021. S. 17.
50. T8. DWDM системы "Волга". Объединяем Россию. Разработка, производство, проектирование, инсталляция. https://T8-80000km-ru.
T8. DWDM sistemy "Volga". Obedinyaem Rossiyu. Razrabotka, proizvodstvo, proektirovanie, installyatsiya. https://T8-80000km-ru.

Статья поступила в редакцию 21.12.21.