Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
Vol. 4, Is. 2, pp. 55-60, 2015

DOI: 10.13187/vesp.2015.4.55
www.ejournal21.com

UDC 004.056.53

Cryptographic and Other Security Methods FOL

[1]Artem A. Gonchar
[2] Xenia A. Kudryavtseva

[1] St. Petersburg University of the Russian Interior Ministry, Russian Federation
198206, St. Petersburg, str. Flyer Pilyutova, 1
PhD (Military Science), Major of the police
E-mail: gonchar.tema@yandex.ru
[2] ITMO University, Russian Federation
197101, Saint-Petersburg, Kronverkskiy prospekt, 49
E-mail: kudriavtseva.ksyu@yandex.ru

Abstract

This article describes the ways in which can be achieved integrity of information transmitted over fiber optic cables, ranging from monitoring for cable and ending with the advantages of single-mode fiber, as well as disassembled encryption methods for the transmission in fiber-optic lines and the latest developments in this area.

Keywords: information security, optical signal, the optovolokonnaya line of communications, cryptography, protection from the threats.

Введение

Сегодня ни для кого не секрет, что информация, передаваемая от ее источника адресату, всегда подвержена риску утечки. При этом для каждого из способов ее передачи, будь то использование радиоканала или проводных линий, существуют вполне определенные методы перехвата. Все виды связи, известные на данный момент, находят себе применение в деятельности органов внутренних дел. Не стоит лишний раз напоминать о важности и, зачастую, конфиденциальности информации, которой обмениваются сотрудники, используя средства связи. [1]

Волоконно-оптическая связь на сегодня является основным видом высокоскоростных коммуникаций на длинные и сверхдлинные дистанции, при этом обеспечивается быстрая доставка большого объема данных любого характера. Стационарное оборудование ВОЛС обычно размещается на сертифицированных объектах, которые находятся под постоянным наблюдением специалистов, служб безопасности и охраны. Доступ к элементам линейного тракта намного проще. Ранее было принято считать, что волоконно-оптические линии связи обладают повышенной устойчивостью к несанкционированному доступу, тем не менее существует принципиальная возможность съема информации, передаваемой по оптическим каналам связи. [2] В связи с этим встает вопрос о защищенности ВОЛС. Данная статья посвящена описанию некоторых методов их защиты. Несомненно, в условиях непрерывного информационного противостояния эта тема весьма актуальна, в частности применительно к деятельности органов внутренних дел.

Обсуждение

У оптоволоконных кабелей есть масса преимуществ перед традиционными медными кабелями. Во-первых, это скорость передачи данных и ничтожные потери. За счет этого появляется возможность прокладки оптоволоконных систем на большие расстояния. Во-вторых – безопасность, которая в оптоволоконных сетях оказывается значительно выше. До недавнего времени считалось, что подключится постороннему человеку к нему практически невозможно. [2, 3]

В волоконно-оптических линиях связи, предназначенных для передачи конфиденциальной информации, должна быть сформирована надежная, защищенная инфраструктура с использованием всех доступных средств и способов информационной защиты. Информационная безопасность объектов сети и линий связи включает:

- защищенность от случайных воздействий нарушителя;
- защищенность от преднамеренных воздействий нарушителя;
- защищенность от угроз безопасности.

Что касается безопасности станционного оборудования ВОЛС, то оно, как правило, размещается на сертифицированном объекте, где проводится полный цикл организационно-технических мероприятий по комплексной информационной безопасности. Однако важным условием информационной безопасности ВОЛС является закупка сертифицированного по этому показателю телекоммуникационного оборудования. Это связано с тем, что в некоторых зарубежных образцах аппаратуры обнаруживались «закладки» в тех ее частях, которые напрямую связаны с информационной безопасностью оборудования. [3]

Результаты

В настоящее время разработано и используется несколько групп способов борьбы с незаконным подключением к оптоволоконной линии связи. [3, 4]

Первая группа, включающая в себя принципы, исключающие или сводящие до минимума возможность влияния посторонних подключений, – наблюдение за оптоволоконным кабелем и его мониторинг. Более подробно рассматривают:

1. Мониторинг сигналов вблизи волокна.

Этот метод подразумевает производство оптоволокна с дополнительными волокнами, по которым передается специальный сигнал мониторинга. Использование такого метода увеличит стоимость кабеля, но любая попытка согнуть кабель вызывает потерю сигнала мониторинга, и вызывает срабатывание сигнала тревоги.

2. Электрические проводники

Метод состоит в интегрировании электрических проводников в кабель, и если оболочка кабеля нарушена, то изменяется емкость между электрическими проводниками и это может использоваться для срабатывания тревоги.

3. Мониторинг мощности мод.

Этот метод применим к мультимодовому волокну, в котором затухание – это функция от моды, в которой распространяется свет. Подсоединение влияет на определенные моды, но при этом затрагивает и другие моды. Это приводит к перераспределению энергии от проводящих мод к непроводящим, что меняет соотношение энергии в ядре волокна и его оболочке. Изменение энергии в модах может быть обнаружено на принимающей стороне соответствующим измерением, что будет являться информацией для принятия решения – есть подключение к кабелю или нет.

4. Измерение оптически значимой мощности

В волокне может осуществляться мониторинг уровня оптически значимой мощности. В том случае, если она отличается от установленного значения, срабатывает сигнал. Но это требует соответствующей кодировки сигнала так, чтобы в волокне присутствовал постоянный уровень сигнала, не зависящий от наличия передаваемой информации.

5. Оптические рефлектометры

Поскольку подсоединение к волокну забирает часть оптического сигнала, для обнаружения подключений могут использоваться оптические рефлектометры. С их помощью можно установить расстояние по трассе, на котором обнаруживается падение уровня сигнала (Схема 2).

6. Методы с использованием пилотного тона

Пилотные тоны проходят по волокну также как и коммуникационные данные. Они используются для обнаружения перерывов в передаче. Пилотные тоны могут использоваться для обнаружения атак, связанных с постановкой помех, но если несущие волновые частоты пилотных тонов не затрагиваются, то данный метод не является эффективным при обнаружении такого рода атак. О наличии подключения можно судить только по существенному уменьшению уровня сигнала пилотного тона.

Вторым методом борьбы с несанкционированным подключением в ОВ линии связи считается использование одномодового оптоволокна, называемым «сильногнущимся». Эти виды волокна защищают сеть передачи данных, ограничивая высокие потери, возникающие при прокалывании волокна или его сгибании. Кроме того, для светового потока становятся менее повреждающими такие факторы как вытягивание, перекручивание и другие физические манипуляции с волокном [5].

Третий метод не защищает волокно от незаконного присоединения, но делает малополезной информацию, полученную злоумышленником, – это шифрование.

Оно делится на 2 вида – канальное и сквозное.

При канальном шифровании зашифровываются абсолютно все данные, проходящие по каждому каналу связи, включая открытый текст сообщения, а также информацию о его маршрутизации. Однако в этом случае любой интеллектуальный сетевой узел (например, коммутатор) будет вынужден расшифровывать входящий поток данных, чтобы соответствующим образом его обработать, снова зашифровать и передать на другой узел сети. Тем не менее, канальное шифрование представляет собой очень эффективное средство защиты информации в компьютерных сетях. Так как шифрованию подлежат все данные, передаваемые от одного узла сети к другому, у криптоаналитика нет никакой дополнительной информации о том, кто служит источником этих данных, кому они предназначены, какова их структура и т.д.

Кроме того, при использовании канального шифрования дополнительно потребуется защищать каждый узел компьютерной сети, по которому передаются данные. Если абоненты сети полностью доверяют друг другу и каждый ее узел размещен там, где он защищен от злоумышленников, на этот недостаток канального шифрования можно не обращать внимания. Однако на практике такое положение встречается чрезвычайно редко. Ведь в каждой фирме есть конфиденциальные данные, знакомиться с которыми могут только сотрудники одного определенного отдела, а за его пределами доступ к этим данным необходимо ограничивать до минимума. [6]

При сквозном шифровании криптографический алгоритм реализуется на одном из верхних уровней модели OSI. Шифрованию подлежит только содержательная часть сообщения, которое требуется передать по сети. После чего к ней добавляется служебная информация, необходимая для маршрутизации сообщения, и результат переправляется на более низкие уровни с целью отправки адресату. Теперь сообщение не требуется постоянно расшифровывать и зашифровывать при прохождении через каждый промежуточный узел сети связи. Сообщение остается зашифрованным на всем пути от отправителя к получателю. Основная проблема, с которой сталкиваются пользователи сетей, где применяется сквозное шифрование, связана с тем, что служебная информация, используемая для маршрутизации сообщений, передается по сети в незашифрованном виде. Здесь же криптоаналитик может извлечь для себя массу полезной информации, зная кто с кем, как долго и в какие часы общается через компьютерную сеть. Для этого ему даже не потребуется быть в курсе предмета общения. [7]

По сравнению с канальным, сквозное шифрование характеризуется более сложной работой с ключами, поскольку каждая пара пользователей компьютерной сети должна быть снабжена одинаковыми ключами, прежде чем они смогут связаться друг с другом. А поскольку криптографический алгоритм реализуется на верхних уровнях модели OSI, приходится также сталкиваться со многими существенными различиями в коммуникационных протоколах и интерфейсах в зависимости от типов сетей и объединяемых в сеть компьютеров. Все это затрудняет практическое применение сквозного шифрования. [8]

Организация шифрования на канальном уровне гарантирует безопасность передачи данных по оптоволокну и делает практически невозможным перехват критически важной информации. В исследованиях, проведенных в Технологическом институте Рочестер (Rochester Institute of Technology, RIT), было показано, что технологии шифрования на уровне 2 обеспечивают гораздо большую пропускную способность и намного меньшее время задержки, чем IPSec VPN, функционирующий на сетевом уровне. Поэтому для скоростных сетей, работающих по принципу «точка-точка», отказ от IPSec в пользу шифрования на канального уровне представляется вполне осмысленным. [8]

Дополнительные преимущества шифрования на уровне 2 включают в себя отсутствие увеличения времени задержки, работу без увеличения потерь, простоту эксплуатации (принцип «поставили и забыли», введение новых алгоритмов кодирования вроде AES 256 (алгоритм основан на нескольких заменах, подстановках и линейных преобразованиях, каждое из которых выполняется блоками по 16 байт, поэтому он называется блоковым шифром. Операции повторяются несколько раз, каждый из которых называется «раунд». В течение каждого раунда, на основе ключа шифрования вычисляется уникальный ключ раунда и встраивается в вычисления. Благодаря подобной блоковой структуре AES, изменение даже одного бита или в ключе, или в текстовом блоке приводит к полному изменению всего шифра – явное преимущество относительно традиционных потоковых шифров. [8,9]

Используя технологии, опирающиеся на последние разработки в алгоритмах кодирования, предприятия надежно защитят себя от «утечки» данных. Современные шифровальные системы постоянно производят смену ключа. Это означает, что даже если кто-то сумеет собрать информацию и подобрать ключ, расшифровать ему удастся лишь незначительный объем. Согласно последним данным, для декодирования 128-битного ключа AES с помощью специальных программ может потребоваться около 149 трлн. лет. А при использовании 256-битного ключа – и того дольше. Причем, с ростом размера ключа увеличивается и сложность алгоритма шифрования. Иными словами, использование такого кодирования делает передачу данных практически полностью безопасной. [8]

В настоящее время, в сфере волоконно-оптических линий связи, кроме рассмотренных шифрования, широкое применение нашла квантовая криптография. Это обусловлено тем, что с их помощью возможна передача фотонов света на большие расстояния и с мизерными искажениями. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике, рассматривая случаи, когда информация переносится с помощью объектов квантовой механики. [9]

Заключение

Квантовая криптография уже заняла достойное место среди систем обеспечивающих конфиденциальную передачу информации. От обсуждения достоинств и недостатков различных протоколов распределения ключей научный мир перешел к поиску наиболее удачных структурных и схемотехнических решений, обеспечивающих увеличение дальности связи, повышение скорости формирования ключей и снижение влияния дестабилизирующих факторов. Одной из тенденций развития является совершенствование элементной базы систем квантовой криптографии, предусматривающее преодоление технологических сложностей изготовления компонентов. [10]

В литературе отсутствует описание влияния параметров функциональных узлов на характеристики эффективности систем квантовой криптографии. Тесным образом с этой проблемой связано отсутствие общепризнанных методик исследования (измерения)

параметров систем квантового распределения ключей в целом, а так же всех функциональных узлов, входящих в состав систем. Для реализации систем, работающих на спутанных состояниях, необходимо создание источников оптического излучения нового класса, позволяющих формировать спутанные фотонные пары.

Основными потребителями систем квантовой криптографии в первую очередь выступают министерства обороны, министерства иностранных и внутренних дел, а так же крупные коммерческие объединения. На настоящий момент высокая стоимость квантовых систем распределения ключей ограничивает их массовое применение для организации конфиденциальной связи между небольшими и средними фирмами и частными лицами.

Несмотря на современные способы защиты от несанкционированного доступа к информации через оптоволоконный канал связи, вероятность этого доступа все еще не нулевая, и нельзя говорить о стопроцентной защищенности сети. На данном этапе развития кабелей и сетей в целом, ОВ являются самыми надежными, а методы внедрения устройств, мешающие их нормальной работе, дорогостоящими, поэтому это хороший выбор для организаций и компаний, как крупных, так и не очень. [11]

Примечания:

1. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. СПб.: ООО «Издательство Полигон», 2000. 856 с.
2. Хорев А.А. Технические каналы утечки акустической (речевой) информации // Специальная техника. 2004. № 3, 4, 5.
3. Боос А.В., Шухардин О.Н., Анализ проблем обеспечения безопасности информации, передаваемой по оптическим каналам связи, и пути их решения. // Информационное противодействие угрозам терроризма, 2007. №5, С. 162-168.
4. Килин С.Я. Квантовая информация // Успехи Физических Наук. 1999. Т. 169. С. 507—527.
5. Холево А.С. Квантовые системы, каналы, информация. М.: МЦНМО, 2010.
6. M.ZIQBAL, Optical Fiber Tapping: Methods and Precautions. High Capacity Optical Networks and Enabling Technologies HFATHALLAH, NBELHADJ. 2011.
7. Смарт Н. Криптография. М.: Техносфера, 2006. 468 с.
8. Голубчиков Д.М., Румянцев К.Е. Квантовая криптография: принципы, протоколы, системы. Таганрог: Таганрогский технологический институт Южного федерального университета, 2008. 37 с.
9. Курс «Безопасность сетей Windows для профессионалов» от Академии специальных курсов по компьютерным технологиям.
10. Статья «Перехват данных на оптоволоконной линии и преимущества шифрования» – Режим доступа: http://nag.ru
11. Каторин Ю.Ф., Ныркov А.П., Соколов С.С., Ежгуров В.Н. Основные принципы построения защищенных информационных систем автоматизированного управления транспортно-логическим комплексом. СПб.: // Проблемы информационной безопасности. Компьютерные системы. 2013. № 2. С. 54-58.

References:

1. Katorin YU.F., Kurenkov E.V., Lysov A.V., Ostapenko A.N. Large encyclopedia of industrial espionage. St. Petersburg: OOO “publishing house is range”, 2000. 856 s.
2. Khorev A.A. Technical channels of the leakage of acoustic (vocal) information // Special technology. 2004. № 3, 4, 5.
3. Boos A.V., Shukhardin O.N., the case study of providing safety of information, transferred by the optical communication channels, and the method of their solution. /Information opposition to the threats of terrorism, №5, 2007. With 162-168.
4. Kilin S.YA. Quantum information/the successes of physical sciences. 1999. T. 169. C. 507—527.
5. Ischolic A.S. Quantum systems, channels, information. M.: MTSNMO, 2010.
6. M.ZIQBAL, Optical Fiber Tapping: Methods and Precautions. High Capacity Optical Networks and Enabling Technologies HFATHALLAH, NBELHADJ. 2011.
7. Smart n. Cryptography. M.: Technosphere, 2006. 468 s.

8. Dear fellows D.M., Rumyantsev K.E. Quantum cryptography: principles, protocols, system. Taganrog: Taganrog technological institute of southern federal university, 2008. 37 s.
9. Course “safety of networks Windows for the professionals” from the academy of special courses on the computer technologies.
10. The article “Interception of data on the optovolokonnoy line and of the advantage of coding” - the regime of the access: http://nag.ru
11. Katorin YU.F., Nurkov A.P., Sokolov S.S., Ezhgurov V.N. Basic principles of the construction of the protected information systems of automated management by transport-logical complex. St. Petersburg: / The problems of information safety. Computer systems. 2013. № 2. S. 54-58.

УДК 004.056.53

Криптографические и другие методы защиты ВОЛС

[1] Артем Александрович Гончар
[2] Ксения Александровна Кудрявцева

[1] Санкт-Петербургский Университет МВД России, Российская Федерация
198206, Санкт-Петербург, ул. Летчика Пилютова, 1
Кандидат военных наук, майор полиции, старший преподаватель
E-mail: gonchar.tema@yandex.ru
[2] Университет ИТМО, Российская Федерация
197101, Санкт-Петербург, Кронверский проспект, 49
E-mail: kudriavtseva.ksyu@yandex.ru

Аннотация. В данной статье рассмотрены способы, с помощью которых может быть обеспечена целостность информации передаваемой по оптоволоконным каналам: начиная от мониторинга кабеля и заканчивая преимуществами одномодового волокна, а так же разобраны способы шифрования информации при передачи в ВОЛС и новейшие разработки в этой области.

Ключевые слова: информационная безопасность, оптический сигнал, оптоволоконная линия связи, криптография, защищенность от угроз.