Copyright © 2015 by Academic Publishing House *Researcher*

Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 6, Is. 4, pp. 133-139, 2015

DOI: 10.13187/vesp.2015.6.133
www.ejournal21.com

Technical Means

UDC 004.056.53

The Analysis of Access Points to FOL

[1] Xenia A. Kudryavtseva
[2] Natalia M. Zaitseva

[1] ITMO University, Russian Federation
197101, Saint-Petersburg, Kronverkskiyprospekt, 49
E-mail: kudriavtseva.ksyu@yandex.ru
[2] ITMO University, Russian Federation
197101, Saint-Petersburg, Kronverkskiyprospekt, 49
E-mail: Zaytsevanm@yandex.ru

Abstract

This article describes the ways in which can be intercepted information transmitted over fiber optic channels, considered two types of offender and analyze potential actions that both types can be applied to modify the data to be protected and abductions. There are described and analyzed the basic methods of the output of information from the optic lines. Based on this analysis there are determined the most vulnerable points of the optic line, which is easier to intercept the information, and which first of all need protection.

Keywords: information security, optical signal, fiber optic communications, information threats, types attacker to intercept traffic.

Введение

Переход от электронных технологий к фотонным, перевод значительной доли информационного трафика на оптический кабель несет не только существенные преимущества, но и новые проблемы для информационной безопасности человека, общества и государства. Здесь необходимо оценить возможные угрозы. [1]

Главными целями деятельности по обеспечению информационной безопасности являются ликвидация угроз и минимизация возможного ущерба, который может быть нанесен вследствие реализации данных угроз.

Угроза — одно из ключевых понятий в сфере обеспечения информационной безопасности.

Угроза объекту информатизации есть совокупность факторов и условий, возникающих в процессе взаимодействия различных объектов (их элементов) и способных оказывать негативное воздействие на конкретный объект информационной безопасности.

Негативные воздействия различаются по характеру наносимого вреда, а именно: по степени изменения свойств объекта безопасности и возможности ликвидации последствий проявления угрозы.

Анализ угроз информационной безопасности позволяет выделить их составляющие источники, способы и последствия реализации. Анализ исключительно важен для получения всей необходимой информации об информационных угрозах, определения потенциальной величины ущерба, как материальной, так и нематериальной, и выработки адекватных мер противодействия.

В данной статье, на основании анализа известных методов перехвата информации в ВОЛС, обозначены их наиболее уязвимые места, которые в первую очередь нуждаются в защите.

Материалы и методы

Основным источником для написания данной статьи стали официальные документы, регламентирующие информационную безопасность каналов связи, а также результаты последних исследований по способам перехвата информации в ВОЛС.

Методологическую основу данного исследования составили такие общенаучные подходы, как диалектический, системно-структурный и функциональный. Наряду с эти используются логические приемы, определения, описания, анализа и синтеза, которые позволяют на основе обобщения сформулировать понятия, дефиниции, определения. Также использован общенаучный метод анализа.

Обсуждение

Современное правовое, нормативное и методическое обеспечение безопасности информации в волоконно-оптических коммуникациях явно недостаточно, оно охватывает только государственные и военные объекты, оставляя личность и предпринимательство без должного внимания.

Под объектом информатизации понимается совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров. [2]

Оптическая кабельная инфраструктура объекта информатизации может включать не только локальную сеть, но и сети телефонной связи, кабельного телевидения, систем видеонаблюдения, различных измерительных систем и другие кабельные системы. Передаваемый по оптическим кабелям трафик носит конфиденциальный характер и имеет важное значение для функционирования объекта независимо от вида сети. Трафик может подвергаться различным опасностям, таким как нарушение конфиденциальности, целостности и доступности.

ВОЛС может располагаться как в периметре предприятия, так и за его границами. Нужно понимать, как и где злоумышленник может подобраться к объекту информатизации. Для этого введем понятие контролируемой зоны.

Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств. [3]

Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения. [4]

Любое современное предприятие не может обойтись без использования глобальной сети Internet, для связи как между сотрудниками внутри организации, так и для взаимодействия с различными органами исполнительной власти. Информацию, которую передают или получают сотрудники, можно объединить в понятие «интернет-трафик».

Как раз эта информация может быть перехвачена, модифицирована или удалена при подключении к ВОЛС, что принесет предприятию убытки в денежном эквиваленте, часто не малые.

Результаты

Угрозы реализуются различными способами, но одним из основных способов является перехват информации посредством несанкционированного доступа (НСД) или несанкционированного съема информации (НСИ). Обычно злоумышленник обладает техническими средствами съема информации на самом современном уровне развития этого вида техники и способен реализовать любой сценарий по получению доступа к конфиденциальной информации, не противоречащий законам физики.

Перехват трафика — это получение доступа к информационным потокам, передаваемые через компьютерную, телефонную сеть, сеть кабельного телевидения, сети систем безопасности, измерительные и другие сети объекта информатизации, которые построены на основе внутренней оптической кабельной инфраструктуры объекта и с выходом за пределы объекта информатизации и контролируемой зоны.

Для того чтобы понять, как происходит подключение к волоконно-оптическому кабелю, необходимо знать, кто может осуществить данное подключение. Перехват трафика злоумышленником может быть осуществлен на основе двух подходов – внешнего и внутреннего нарушителя.

Внешний нарушитель — злоумышленник, использующий технические средства разведки для подключения к оптической структурированной кабельной системы, располагаемой за пределами объекта информатизации и вне контролируемой зоны.

Модель перехвата трафика внешним нарушителем показана на рисунке 1.1, где X — злоумышленник, B — контролируемая зона, A — ВОЛС, / — объект, подверженный атаке.

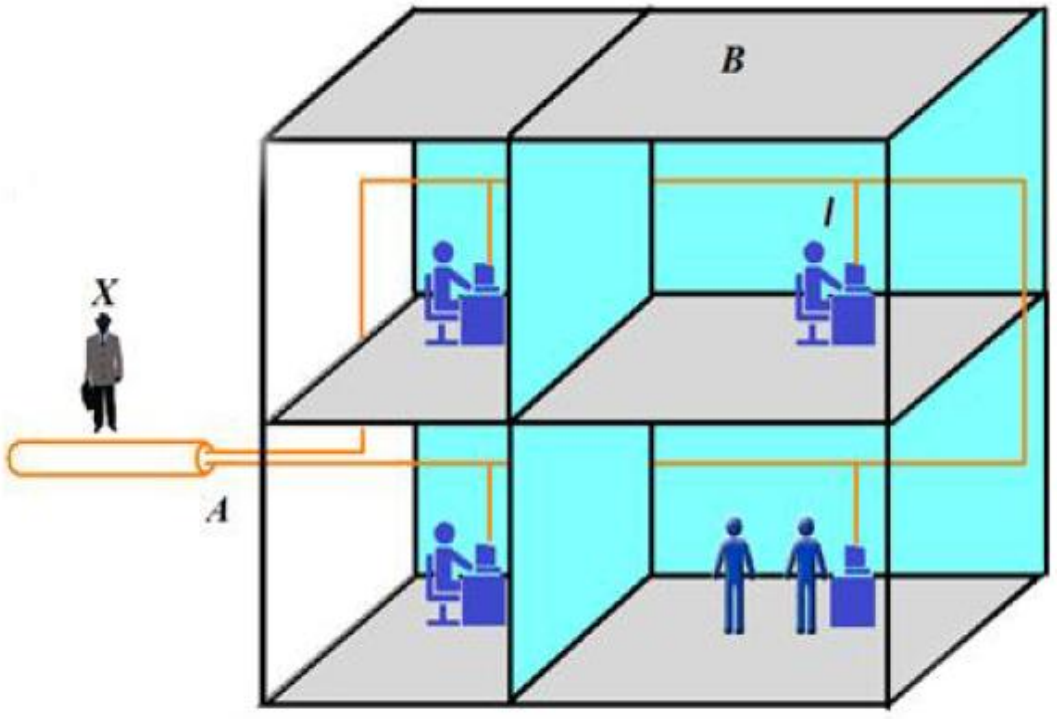

Рис. 1.1. Модель внешнего нарушителя

Внутренний нарушитель — злоумышленник, использующий возможности физического доступа и особенности оптической кабельной системы внутри объекта информатизации и внутри контролируемой зоны. [5]

Модель перехвата трафика внутренним нарушителем показана на рисунке 1.2, где X — злоумышленник, B — контролируемая зона, A — ВОЛС, / — объект, подверженный атаке.

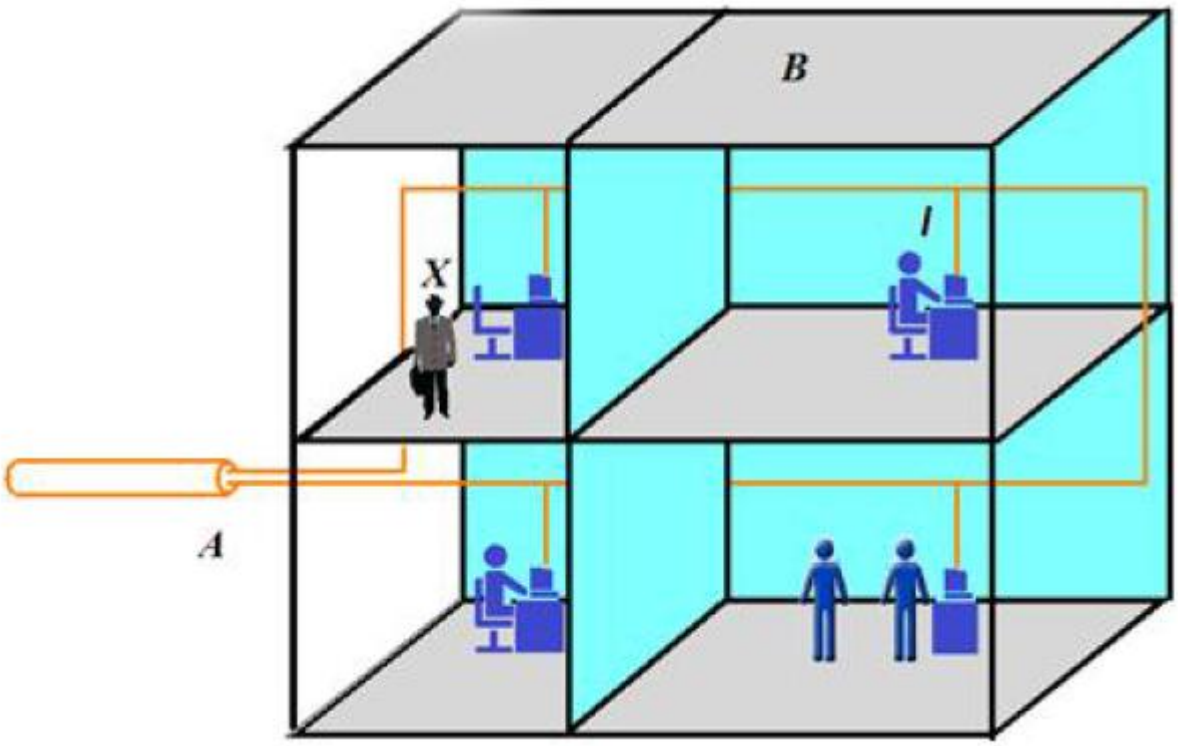

Рис. 1.2. Модель внутреннего нарушителя

Для внешнего и внутреннего нарушителя существует некоторый перечень действий, без которых перехват информации невозможен:

1. выявить топологию кабельной инфраструктуры:
1.1. точка – точка
1.2. звезда
1.3. кольцо
1.4. смешанная
2. определить расположение коммутационных элементов;
3. определить типы оптического кабеля, волокна и выявить характерные неоднородности кабельной системы (места сварки и разъемных соединений);
4. подбор специальных технических средств, подключение к оптическому каналу и реализация съема информации;
5. регистрация сигнала утечки информации и перехват трафика.[6]

Рассмотрим сценарии перехвата трафика из волоконно-оптических линий связи нарушителем. Существует два метода подключения: подсоединение к сети передачи данных, т. е. контактный метод, и подсоединение с удалённой обработкой — дистанционный.

Контактные методы включают в себя:

А — контактный перехват с разрывом оптоволокна и вставкой;

В — контактный перехват с прямым доступом к волокну.

Наиболее опасные для перехвата по типу А и В участки кабельной системы — это защитные оптические муфты для сварных соединений, а также коммутационно-распределительные устройства (оптические кросс-панели, стойки).

Контактный метод с разрывом волоконно-оптического кабеля происходит путем замыкания оптического канала через оптоволоконную вставку соединением волокон.

Время необходимое злоумышленнику на подсоединение к ВОЛС контактным методом с разрывом волоконно-оптического кабеля можно увидеть в таблице 1. В данной таблице указано время операции без учета времени подготовки волокон. [7]

Таблица 1

Время подсоединения к ВОЛС для метода А

Технологии соединения волокон	Время операции
Сварное соединение	около 100 сек
Клеевое соединение	около 30 сек
Механическое соединение	около 30 сек

Для осуществления контактного метода перехвата информации без разрыва оптоволокна, можно воспользоваться ответвителем-прищепкой или способом оптического туннелирования.

Оптическое туннелирование представляет собой захват части излучения, выходящего за пределы сердцевины основного световода, вспомогательным световодом с более высоким показателем преломления.

Формирование сигнала утечки путем оптического туннелирования излучения из волокна в специальное волокно механически сцепленные боковыми поверхностями.

Дистанционные методы включают в себя:

C — дистанционный перехват на основе параметрических методов;

D — дистанционный перехват с регистрацией побочных излучений.

Этот способ основан на характерных неоднородностях оптической структурированной кабельной системы.

Наиболее опасные для перехвата по типу C и D участки кабельной системы — это места соединения и коммутации (оптические кроссы и муфты), а также места соединения с активным оборудованием, скрутка кабеля.

Более опасны дистанционные методы подключения к ВОЛС, ибо при их использовании существует два важных плюса:

- при подключении к дальним высокоскоростным (несколько Гбит/сек) каналам связи, роль хранилища становится крайне важной. Захваченные пакеты заполняют диск крайне быстро.
- привлечение сетевых экспертов для работы в полевых условиях может оказаться весьма затратным. Более удобно организовать им работу в удаленном центре обработки, где присутствует любое необходимое оборудование, сложно выносимое в поле. [8]

Заключение

Таким образом, наиболее уязвимы с точки зрения перехвата сигнала участки ВОЛС, включающие свободный оптический кабель, разъемное оптическое соединение, а также кабель, имеющий виброакустический контакт с конструкциями здания. Неправильная сварка концов волокон так же образует весьма опасный канал утечки информации. [9]

С учетом того, что оборудование для перехвата трафика не является специальным и регламентированным для продажи, и злоумышленник может использовать общедоступные стандартные приборы, как техническое средство разведки, эти точки в первую очередь должны быть обеспечены надежной защитой от несанкционированного доступа. [10]

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. ФЗ 149 «Об информации, информационных технологиях и о защите информации» - 2006, ст. 2

3. РД 45.236-2002 «Средства измерений электросвязи рефлектометры оптические технические требования» - 2003 г.

4. Обеспечение информационной безопасности в организации// ГОСТ Р 53114-2008, Москва. 2009, с. 6.

5. Гришачев В.В. Информационная безопасность волоконно-оптических технологий//учебно-методический курс – 2 раздел, Угрозы информации в ВОТ
6. Шапкин А.В. К вопросу о способах защиты информации при её передаче в волоконно-оптических линиях связи//Информационные технологии, связь и защита информации МВД России. 2011. С. 52-53
7. Гришачев В.В. Информационная безопасность волоконно-оптических технологий//учебно-методический курс – 2 раздел, ТСР в ВОТ
8. Хорев А.А. Технические каналы утечки акустической (речевой) информации // Специальная техника. 2004. № 3, 4, 5
9. Вихров Н.М., Каторин Ю.Ф., Нырков А.П., Соколов С.С. О безопасности инфраструктуры водного транспорта. // Морской вестник. 2014. №4 (58). С. 99–102.
10. 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. 162-168.

References:

1. Katorin YF, Kurenkov YV Vlasov, A., A. Ostapenko Great Encyclopedia of industrial espionage. SPb .: OOO "Publishing Polygon", 2000. 856 p.
2. Federal Law 149 "On information, information technologies and information protection" - 2006, art. 2
3. RD 45.236-2002 "Means of measuring optical telecommunication OTDRs technical requirements" – 2003.
4. Ensuring information security in an organization // GOST R 53114-2008, Moscow - 2009, p.6
5. Grishachev VV, Information security fiber-optic technology // Training Resource Course - 2 section Threats to information HERE
6. Shapkin AV, the question of how to protect information during its transfer to the fiber-optic communication lines // Information Technology, Communications and Information Protection Ministry of Internal Affairs of Russia - 2011, p. 52-53
7. Grishachev VV, Information security fiber-optic technology // Training Resource Course - 2 section in the TCP HERE
8. Horev. AA Technical acoustic leakage channels (voice) information // Special equipment. 2004. № 3, 4, 5
9. Vikhrov N.M., Katorin YU.F., pochards A.P., Sokolov number systems. On the safety of the infrastructure of water transport. // Marine herald. 2014. №4 (58). s. 99–102.
10. A. Boos, Shukhardin ON, analysis of the security problems of information transmitted via optical communication channels and ways of solving them. // Information counter the threats of terrorism, №5, 2007. Pp. 162-168.

УДК 004.056.53

Анализ точек доступа к ВОЛС

[1] Ксения Александровна Кудрявцева
[2] Наталья Михайловна Зайцева

[1] Университет ИТМО, Российская Федерация
197101, Санкт-Петербург, Кронверский проспект, 49
E-mail: kudriavtseva.ksyu@yandex.ru
[2] Университет ИТМО, Российская Федерация
197101, Санкт-Петербург, Кронверский проспект, 49
E-mail: Zaytsevanm@yandex.ru

Аннотация. В данной статье рассмотрены способы, с помощью которых может быть перехвачена информация, передаваемая по оптоволоконным каналам, рассмотрены два вида нарушителя и проанализированы потенциальные действия, которые оба вида могут применить для модификации и похищения защищаемых данных. Описаны и проанализированы основные способы съема информации из оптоволоконных линий. На основании этого анализа определены наиболее уязвимые точки оптоволоконной линии, на который легче всего осуществить перехват информации, и которые в первую очередь нуждаются в защите.

Ключевые слова: информационная безопасность, оптический сигнал, оптоволоконная линия связи, угрозы информации, виды злоумышленника, перехват трафика.