Инженерный вестник Дона, №5 (2023)
ivdon.ru/ru/magazine/archive/n5y2023/8380

Особенности построения системы специальной связи на базе волоконно-оптических линий

А.С. Коновалов

ООО «Четвертое измерение», Санкт-Петербург

Аннотация: В статье рассматриваются особенности построения специальной связи на основе волоконно-оптических линий связи. Произведен анализ надежности использования волоконно-оптических линий связи с точки зрения возможности несанкционированного съема передаваемой информации. Представлены преимущества практического использования систем связи на базе волоконно-оптических линий. Рассмотрены способы защиты волоконно-оптических линий связи от несанкционированного доступа, где приоритетным способом защиты информации является ее шифрование различными методами. В заключение подчеркиваются мероприятия, необходимые для построения надежной системы связи на базе волоконно-оптических линий.
Ключевые слова: информация, специальная связь, сегменты связи, связи общего пользования, оптическое волокно, волоконно-оптические линии, несанкционированный доступ, шифрование, построение системы связи, криптографические протоколы.

В соответствии с [1,2], под системой специальной связи подразумевается система связи, предназначенная для нужд органов государственной власти, нужд обороны страны, безопасности государства. В результате анализа информации, изложенной в [3] в настоящее время в составе системы специальной связи включены многочисленные сегменты систем связи общего пользования, коммерческих телекоммуникационных ресурсов, а также коммерческие протоколы и технологии.

Развитие технологий, в том числе, средств специальной связи, находится в процессе постоянного развития. Изобретение новых технологий и методов открывает не только ранее недоступные перспективы развития систем специальной связи, но и ставит ранее неизвестные задачи, а вызовы современности требуют все новых подходов, видений и взглядов на решение таковых проблем.

В настоящее время для построения наземной системы специальной связи широко используются волоконно-оптические линии связи (ВОЛС). Система специальной связи на базе ВОЛС является высокоскоростной и

надежной технологией передачи данных, которая использует световые волны для передачи информации вместо электрических сигналов. Данные каналы передачи информации отличаются крайне высокой информационной мощностью и надежностью работы. Это объясняется тем, что они значительно превосходят проводные по следующим показателям [4]:

пропускная способность ВОЛС может достигать нескольких терабит в секунду;

передача данных на большие расстояния без значительных потерь качества сигнала;

сигналы не подвержены перехвату или помехам, которые могут возникнуть при использовании проводных линий;

устойчивость к внешним воздействиям, таким как электромагнитные поля, радиочастотные помехи и другие внешние факторы;

ВОЛС могут легко масштабироваться для увеличения пропускной способности и расширения диапазона передачи данных.

Считается, что ВОЛС, в силу особенностей распространения электромагнитной энергии в оптическом волокне, обладают повышенной скрытностью. Это объясняется тем, что оптическое излучение, являющееся носителем информации, распространяется в оптическом волокне согласно закону полного внутреннего отражения. Участки, где возможна утечка электромагнитного излучения и несанкционированный съем информации «классическими» радиотехническими методами, относительно малочисленны. Приемо-передающая аппаратура, регенерационные пункты изучены и локализованы [5], по этой причине эти участки сравнительно легко могут быть поставлены под контроль.

Несмотря на высокий уровень защищенности, ВОЛС не являются абсолютно защищенными от несанкционированного доступа. Способы съема, которые могут быть использованы для перехвата информации с ВОЛС

изложены в [6]. Один из наиболее распространенных методов несанкционированного снятия информации — это перехват сигнала, передаваемого через волоконно-оптический кабель при помощи перехватывающего устройства; физический доступ к кабелю; взлом системы управления; атака на криптографические протоколы; использование беспроводных технологий.

Интересным является протяженный безразрывный съем информации, который можно осуществить или на пологом изгибе волокна, или на прямом волокне под воздействием низких температур. Дело в том, что при низких температурах происходит изменение коэффициентов преломления стекла, в результате чего в сердцевине может повыситься уровень рассеяния [7].

Для защиты ВОЛС от несанкционированного доступа рекомендуется использовать следующие методы:

1. Шифрование является одним из наиболее эффективных методов защиты. Одним из основных принципов шифрования сигналов на ВОЛС является использование криптографических алгоритмов [8]. Для этого используются специальные криптографические устройства, которые устанавливаются как на конечных устройствах (например, на компьютерах) так и на промежуточных узлах ВОЛС. В зависимости от требований к защите информации, используются различные криптографические алгоритмы. Наиболее популярными из них являются алгоритмы шифрования AES (Advanced Encryption Standard) и RSA (Rivest–Shamir–Adleman).

Шифрование является эффективным методом защиты конфиденциальной информации на ВОЛС, однако его использование может повышать нагрузку на сеть и увеличивать задержки при передаче данных. Поэтому выбор метода шифрования и протокола защиты данных на ВОЛС должен осуществляться с учетом требований к скорости передачи и степени защиты информации.

2. Установка системы контроля доступа, позволяющая определить, имеет ли пользователь право на доступ к ВОЛС [9]. Для этого вводятся различные виды авторизации. Для реализации системы контроля доступа ВОЛС используются различные технологии, такие как VPN (Virtual Private Network), firewalls, IDS/IPS (Intrusion Detection/Prevention System).

Например, VPN позволяет создать защищенное соединение между двумя узлами ВОЛС через общедоступную сеть, такую, как Интернет. В этом случае, передаваемые данные шифруются и аутентифицируются, чтобы обеспечить конфиденциальность и целостность информации.

Firewall представляет собой систему защиты, которая фильтрует трафик, проходящий через ВОЛС, и блокирует попытки несанкционированного доступа.

IDS/IPS - системы обнаружения и предотвращения вторжений позволяют обнаруживать и блокировать попытки несанкционированного доступа к ВОЛС и защищать ее от различных типов кибератак.

3. Использование защитных устройств для ВОЛС применяется от различных видов внешних воздействий, такие как оптические сплиттеры, репитеры, подземные защитные контуры и фильтры.

4. Использование криптографических протоколов. Рассмотрим наиболее распространённые:

SSL / TLS (Secure Sockets Layer / Transport Layer Security) - протоколы, которые используются для защиты информации, передаваемой по сети Интернет. Они используют алгоритмы шифрования для защиты данных, передаваемых между клиентом и сервером [10].

IPsec (Internet Protocol Security) - протокол, который обеспечивает безопасную передачу данных по IP-сетям, включая ВОЛС [11]. IPsec использует различные методы шифрования для защиты данных, передаваемых между двумя узлами сети.

Kerberos - протокол аутентификации и авторизации, который используется для защиты информации, передаваемой по сети [12]. Он позволяет пользователям проверять свою личность и получать доступ к ресурсам сети.

SSH (Secure Shell) - протокол, который используется для удаленного управления компьютерами и сетями. Он обеспечивает защиту данных, передаваемых между клиентом и сервером, используя различные методы шифрования [13].

В заключение необходимо отметить, что при построении системы специальной связи на базе ВОЛС учитывается ряд особенностей. ВОЛС чувствительны к механическим повреждениям и перегибам, поэтому требуют особой осторожности при монтаже и эксплуатации. Также для эффективной работы системы ВОЛС необходимо обеспечить высокую качество соединений и оптических разъемов. Для защиты системы ВОЛС от несанкционированного доступа могут использоваться различные методы, включая системы контроля доступа, защитные устройства и криптографические протоколы. Кроме того, для обеспечения надежности и устойчивости к внешним воздействиям, система ВОЛС может иметь резервирование линий и блокирование неисправных участков линий.

Таким образом, система специальной связи на базе ВОЛС обладает рядом преимуществ перед другими средствами передачи данных, но при ее построении необходимо учитывать особенности и требования к качеству соединений, безопасности и устойчивости к внешним воздействиям.

Литература

1. Осипов В. А., Безуглый А. В. Волоконно-оптическая линия связи как линия с распределенными параметрами // Инженерный вестник Дона, 2017, – №. 4. URL: ivdon.ru/ru/magazine/archive/n4y2017/4609

2. Корольков А. В., Кращенко И. А., Матюхин В. Г. Синев С. Г. "Проблемы защиты информации, передаваемой по волоконно- оптическим линиям связи, от несанкционированного доступа" // Информационное Общество, 1997, № 1. URL: emag.iis.ru/arc/infosoc/emag.nsf/0/c0a700122533e000c32575be003cb751?OpenDocument&Click=

3. Бабин В. С. Современные тенденции развития систем специальной связи и показателей эффективности процесса их функционирования // Сборник статей Международной научно-практической конференции, «Молодёжная наука», Пенза МЦНС «Наука и Просвещение» 2020 30.10.2020 г. Пенза. – 2020. – С. 37-40.

4. Сиднев С. А., Зубилевич А. Л. Применение экономического критерия при выборе одномодовых оптических волокон для ВОЛС //Век качества. – 2011. – №. 1. – С. 60-61.

5. Свинцов А. Г. Оптимизация параметров оптического рефлектометра для обнаружения неоднородности при попытке несанкционированного доступа в ВОСП //Фотон-экспресс. – 2006. – №. 6. – С. 56-71.

6. Горлов Н. И., Шайгараева Т. Н. Способы несанкционированных подключений к ВОЛС //Инновационные, информационные и коммуникационные технологии. – 2017. – №. 1. – С. 192-195.

7. Богачков И. В., Майстренко В. А., Трухина А. И. Изучение способов формирования каналов утечки информации в оптических волокнах // Методические вопросы преподавания инфокоммуникаций в высшей школе. – 2016. – Т. 5. – №. 2. – С. 11-13.

8. Кольцов А. С., Филатова Н. В., Пальчиков А. В. Исследование методов защиты информации, передаваемой по волоконно-оптическим линиям связи //Актуальные проблемы деятельности подразделений УИС. – 2018. – С. 43-46.

9. Безуглый А. В., Черных В. Н. Повышение надежности систем автоматического управления передачей данных путем оптимизации волоконно-оптических линий связи // Инженерный вестник Дона, 2019, № 8. URL: ivdon.ru/ru/magazine/archive/N8y2019/6250

10. Мартыненков И. В. Основные этапы развития криптографических протоколов SSL/TLS и IPsec //Прикладная дискретная математика. – 2021. – №. 51. – С. 31-67.

11. Alshamrani H. Internet Protocol Security (IPSec) Mechanisms //International Journal of Scientific & Engineering Research. – 2014. – Т. 5. – №. 5. – pp. 2229-5518.

12. Hu D., Du Z. An improved Kerberos protocol based on fast RSA algorithm //2010 IEEE International Conference on Information Theory and Information Security. – IEEE, 2010. – pp. 274-278.

13. Bergsma F. et al. Multi-ciphersuite security of the Secure Shell (SSH) protocol //Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. – 2014. – pp. 369-381.

References

1. Osipov V. A., Bezuglyj A. V. Inzhenernyj vestnik Dona. 2017. №. 4. URL: ivdon.ru/ru/magazine/archive/n4y2017/4609

2. Korolkov A. V. Informatsionnoe Obshchestvo. 1997, № 1. URL: emag.iis.ru/arc/infosoc/emag.nsf/0/c0a700122533e000c32575be003cb751?OpenDocument&Click=

3. Babin V.S. Cbornik statej Mezhdunarodnoj nauchno-prakticheskoj konferencii, «Molodyozhnaya nauka», Penza MCNS «Nauka i Prosveshchenie» 2020 30.10.2020 g. Penza. 2020. pp. 37-40.

4. Sidnev, S. A., & Zubilevich, A. L. Vek kachestva, (1), pp. 60-61.

5. Svinsov, A. G. (2006). Photon-Express. (6), pp. 56-71.

6. Gorlov N. I., SHajgaraeva T. N. Innovacionnye, informacionnye i kommunikacionnye tekhnologii. 2017. №. 1. pp. 192-195.

7. Bogachkov, I.V., Maistrenko, V.A., & Trukhina, A.I. Methodological Questions of Teaching Infocommunications in Higher Education. 5(2), pp. 11-13.

8. Kol'tsov, A. S., Filatova, N. V., & Pal'chikov, A. V. Actual Problems of Activities of UIS Divisions. pp. 43-46.

9. Bezuglyj A. V., CHernyh V. N. Inzhenernyj vestnik Dona. 2019. №. 8. URL: ivdon.ru/ru/magazine/archive/N8y2019/6250

10. Martynenkov I. V. IPsec Prikladnaya diskretnaya matematika. 2021. №. 51. pp. 31-67.

11. Alshamrani H. International Journal of Scientific & Engineering Research. 2014. T. 5. №. 5. pp. 2229-5518.

12. Hu D., Du Z. IEEE International Conference on Information Theory and Information Security. IEEE, 2010. pp. 274-278.

13. Bergsma F. et al. ACM SIGSAC Conference on Computer and Communications Security. 2014. pp. 369-381.