Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 621.391

Веремейчик
Илья Геннадьевич

Асинхронный волоконно-оптический канал связи для передачи конфиденциальных данных

Автореферат
диссертации на соискание ученой степени магистра технических наук
по специальности 1-98 80 01 – Методы и системы защиты информации, информационная безопасность

Научный руководитель
кандидат технических наук,
доцент Тимофеев А.М.

Минск, 2020

КРАТКОЕ ВВЕДЕНИЕ

В настоящее время для передачи конфиденциальных данных широкое применение находят оптические волокна (ОВ). Для обеспечения конфиденциальности и подлинности источника широко используются криптографические преобразования информации, механизмы взаимной идентификации и аутентификации пользователей и данных. Однако в силу открытости большинства алгоритмов, их криптостойкость зависит от вычислительных возможностей злоумышленника, что является угрозой для большинства криптосистем.

Поэтому возникает необходимость в канале связи с защитой от несанкционированного доступа. ОВ имеет ряд преимуществ. Среди них высокие пропускная способность, длина участка регенерации и помехозащищенность; малые габаритные размеры и масса оптических кабелей; относительно низкая стоимость.

В силу особенностей распространения электромагнитной энергии в оптическом волокне, обладают повышенной скрытностью. Однако, всегда существует принципиальная возможность съема информации с оптического кабеля. Существуют способы съема оптических излучений, которые могут быть использованы для перехвата информации с боковой поверхности ОВ. Условно, их можно разделить на 3 группы.

1 Способы, основанные на регистрации излучения с боковой поверхности ОВ (пассивные).

2 Способы, основанные на регистрации излучения, выводимого через боковую поверхность ОВ с помощью специальных средств (активные).

3 Способы, основанные на регистрации излучения, выводимого через боковую поверхность ОВ с помощью специальных средств, с последующим формированием и вводом в ОВ излучения, компенсирующего потери мощности при выводе излучения (компенсационные) [3].

Благодаря использованию защитных оболочек, боковое излучение кабеля ослабляется до величин, меньших квантового предела обнаружения оптического излучения, поэтому перехват может осуществляться только при нарушении внешней защитной оболочки кабеля и доступом непосредственно к ОВ.

В связи с вышесказанным представляет интерес разработка такого канала связи, который позволил бы обнаруживать несанкционированный съем передаваемой информации. Для передачи и считывания данных с этого канала связи необходимо устройство, которое для передачи каждого бита информации использует маломощные оптические сигналы, содержащие от одного до десяти фотонов излучения.

Также необходимо установить пропускную способность защищенного от несанкционированного доступа асинхронного волоконно-оптического канала связи с установлением степени влияния мертвого времени на эту способность.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Целью настоящей диссертационной работы является разработка асинхронный волоконно-оптический канал связи, с защитой от перехвата данных. Необходимо разработать устройство передачи данных, построить математическую модель канала связи.

Для достижения поставленной цели потребовалось решение следующих взаимосвязанных задач:

1. Исследовать существующие каналы передачи данных, выявить их преимущества и недостатки.
2. Проанализировать асинхронный волоконно-оптический канал связи.
3. Разработать устройство передачи данных.
4. Построить математическую модель канала связи.
5. Провести экспериментальные испытания.

Объекта исследования являлся разработанный асинхронный волоконно-оптический канал связи для передачи конфиденциальных данных.

Предметом исследований являлось установить пропускную способность канала связи, разработать устройство передачи данных.

Личный вклад соискателя

Содержание диссертации отражает личный вклад соискателя. В работах, выполненных в соавторстве, автор принимал участие в определении целей, задач исследований, а также в проведении самих исследований и обработке полученных результатов.

Апробация и опубликованность результатов

Основные полученные результаты диссертационной работы докладывались и обсуждались на XVII Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, Республика Беларусь, 2019 г.) и XXIII Международной научно-

технической конференции «Современные средства связи» (Минск, Республика Беларусь, 2018 г.). Опубликовано три тезиса докладов.

Структура и объем диссертации

Диссертационная работа состоит из перечня используемых сокращений, введения, общей характеристики работы, четырех глав, заключения и библиографического списка. Полный объем диссертации составляет
56 страниц машинописного текста. Диссертация включает в себя 4 главы, общим объемом 61 страница, в том числе 12 рисунков и 9 формул. Библиографический список занимает 6 страниц и состоит из 70 наименований использованных источников и списка собственных публикаций соискателя из трех наименований на одной странице.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** определены основные направления исследований, обоснована актуальность темы диссертации, показана необходимость канала передачи защищенной от несанкционированного доступа информации.

В **первой главе** были рассмотрены основные каналы утечки информации, а также описаны их основные характеристики. Каналы утечки информации различаются между собой по области распространения, по характеристике передаваемых данных, а также по сложности их эксплуатации. Было определено, что волоконно-оптический канал связи лишен большинства из недостатков: он не создает электромагнитных излучений и индукционных токов, что делает невозможным перехват информации без повреждения защитной оболочки

Во **второй главе** рассмотрены основные методы защиты информации от утечки по техническим каналам. В общем случае защита информации от утечки представляет собой комплекс мероприятий, направленный на обеспечение невозможности распознавания передаваемой информации. Было описано, что волоконно-оптический кабель будет оснащен защитной оболочкой для предотвращения бокового излучения, что делает невозможным регистрацию излучения с боковой поверхности ОВ, а также для передачи информации будут использоваться маломощные оптические сигналы, содержащие от одного до десяти фотонов излучения, что делает невозможным активные и компенсационные способы перехвата информации. Устройство передачи данных будет регистрировать аномальные потери фотонов при передаче данных, или наоборот аномально большое количество фотонов (в случае ретрансляции оптического сигнала) и прерывать обмен информацией, что делает невозможным перехват информации злоумышленником.

В **третьей главе** были описаны основные виды использующихся сегодня криптосистем. Для шифрования передаваемой информации был выбран алгоритм AES-128. Алгоритм является симметричным, что означается высокую скорость шифрования и расшифрования передаваемой информации.

В четвертой главе была построена математическая модель разрабатываемого асинхронного оптического канала связи с приемником на основе счетчика фотонов. Было получено выражение для пропускной способности этого канала, учитывающее статистические распределения

числа импульсов на выходе счетчика фотонов при передаче символа «0» и символа «1», а также пороговые уровни регистрации импульсов при передаче этих символов. Получено, что при длительности передачи одного бита информации, равной 20 мкс, и длительности Δtc, равной длительности защитного интервала, для всех исследуемых типов лавинных фотоприемников пропускная способность принимает максимальное значение. Увеличить пропускную способность можно путем применения схемы активного гашения лавины ЛФП, что, в сравнении со схемой пассивного гашения, повысит пропускную способность канала связи до 100 кбит/с за счет уменьшения мертвого времени счетчика фотонов.

ЗАКЛЮЧЕНИЕ

В диссертации были проведены исследования различных каналов передачи данных, а также проведена разработка асинхронного волоконно-оптического канала связи для передачи конфиденциальных данных.

Было проведено исследование различных технических каналов утечки информации и выявлены их основные характеристики и уязвимости. Было выяснено, что волоконно-оптический канал связи не обладает уязвимостями, которые характерны для других существующих каналов связи. Разрабатываемый канал связи устойчив к пассивным, активным и компенсационным методам перехвата информации.

Были проанализированы основные виды защиты информации от утечки по техническим каналам связи, выявлены основные достоинства и недостатки этих методов. Разрабатываемый канал связи будет обладать комплексом мер для защиты передаваемой информации. Волоконно-оптический кабель будет оснащен защитной оболочкой для предотвращения бокового излучения, что делает невозможным регистрацию излучения с боковой поверхности ОВ. Также, для передачи информации будут использоваться маломощные оптические сигналы, содержащие от одного до десяти фотонов излучения, что делает невозможным активные и компенсационные способы перехвата информации.

Был проведен анализ защиты информации в каналах передачи информации. Выяснилось, что для защиты информации при передаче используется шифрования. После анализа современных алгоритмов шифрования было решено, что для повышения уровня защиты передаваемой информации будет использоваться симметричный алгоритм шифрования AES-128.

В ходе работы была построена математическая модель асинхронного волоконно-оптического канала связи. Были разработаны экспериментальная установка и методика эксперимента. В результате было выяснено, что разработанный канал связи обладает максимальной пропускной способностью при длительности передачи одного бита информации, равной 20 мкс. Скорость передачи данных при этом составит 100 кбит/с.

Также было разработано устройство передачи данных, реализующее асинхронный волоконно-оптический канал связи. Принцип работы устройства описан в главе 5. Данное устройство не нуждается в дополнительной линии связи для передачи импульсов синхронизации. Устройство посылает оптические импульсы слабой мощности, что позволит выявить потенциальные утечки информации и прекращать

ередачу в этом случае, что позволит предотвращать компрометацию конфиденциальных данных.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1] Веремейчик, И.Г. Асинхронный волоконно-оптический канал связи для передачи конфиденциальных данных / И.Г. Веремейчик // Современные средства связи: тезисы докладов XXIII Международной научно-технической конференции – Минск, 2018 – С.191.

[2] Тимофеев, А.М. Исследование вероятности ошибочной регистрации символов «0» в квантово-криптографическом канале связи с приемным модулем на основе счетчика фотонов / А. М. Тимофеев, И.Г. Веремейчик, В.А. Касько, И.А. Ковалев // Технические средства защиты информации : тезисы докладов XVII Белорусско-российской научно – технической конференции – Минск, 2019 – С.68-69.

[3] Тимофеев, А.М. Оценка потерь информации однофотонного канала связи с приемным модулем на основе счетчика фотонов / А. М. Тимофеев, И.Г. Веремейчик, В.А. Касько, И.А. Ковалев // Технические средства защиты информации : тезисы докладов XVII Белорусско-российской научно – технической конференции – Минск, 2019 – С.69.