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

УДК 621.391; 621.383.92

Касько
Виктор Анатольевич

Устройство конфиденциальной передачи данных с автоматическим контролем несанкционированного пользователя

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1 –98 80 01,«Методы и системы защиты информации. Информационная безопасность»

Научный руководитель

Тимофеев А. М.,
кандидат технических наук,
доцент

Минск 2020

КРАТКОЕ ВВЕДЕНИЕ

Жизнь в современных реалиях немыслима без широко разветвленных и устойчиво функционирующих систем передачи и обработки информации, важнейшей частью которой является система связи. Под системой связи в самом общем виде понимают алгоритм установления связи и передачи сообщений от отправителя к получателю. Одной из важнейших задач, решаемых при разработке современных систем связи, является обеспечение конфиденциальности передаваемых данных, а также установление личности участников таких систем.

Для решения данной задачи разрабатываются криптографически защищенные системы связи, позволяющие передавать конфиденциальную информацию по незащищенным каналам связи благодаря криптоподобным преобразованиям информации. Так как любая из криптосистем при определённых условиях становится уязвимой и может быть подвергнута атакам со стороны несанкционированного пользователя, поэтому требуется разработка комбинированных систем связи, которые бы исключали возможность реализации угроз на криптосистему. Существуют способы защиты информации при передаче в оптоволоконных системах, но они не позволяют исключить несанкционированный доступ в полном объеме. Причиной тому являются методы вывода информации посредством микро- и макроизгибов оптоволоконного кабеля. При определенной величине макроизгиба ОВ на границе раздела сердцевина-оболочка угол падения оптической волны становится меньше предельного угла, и в месте макроизгиба создается побочное излучение, в результате чего может осуществляться несанкционированный съем передаваемой информации. В настоящее время разработан ряд способов и устройств для обнаружения таких каналов утечки информации, однако они малоэффективны, когда осуществляется несанкционированный забор не более десяти фотонов оптического излучения из каждого бита передаваемой информации. В этих случаях для передачи конфиденциальной информации следует использовать оптические импульсы малой мощности, для формирования и регистрации которых применяют одноквантовые системы передачи и приема как наиболее чувствительные

В связи с этим целью данной работы являлась разработка устройства передачи данных по волоконно-оптической линии связи с возможностью обнаружения несанкционированного доступа.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Цель диссертационной работы заключается в разработке устройства конфиденциальной передачи информации с контролем несанкционированного доступа к волоконно-оптической линии связи.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1 изучить основные характеристики волоконно-оптических линий связи;

2 рассмотреть и проанализировать влияние показателя профиля преломления оптического волокна на распространение в нем световых лучей;

3 определить основные методы компенсации дисперсии, а также рассмотреть имеющиеся в оптическом волокне нелинейные эффекты, классификацию и характеристики промышленных оптических волокон;

4 изучить и определить принцип работы системы связи с идентификацией взаимодействующих сторон на основе методов криптоподобных преобразований информации;

5 рассмотреть вопрос потерь оптического сигнала на макроизгибе оптического волокна;

6 предложить устройство передачи информации с контролем несанкционированного доступа к волоконно-оптической линии связи; рассмотреть принцип его работы;

7 исследовать и проанализировать зависимости потерь оптического сигнала от диаметра макроизгиба волокна, по результатам анализа определить оптимальные для использования в устройстве длины волн.

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 четыре тезиса докладов.

Структура и объем диссертации

Диссертационная работа состоит из перечня используемых сокращений, введения, общей характеристики работы, трех глав, заключения и библиографического списка. Полный объем диссертации составляет 51 страница машинописного текста. Диссертация содержит 23 рисунка на 20 страницах. Библиографический список занимает 6 страниц и состоит из 70 наименований использованных источников и списка собственных публикаций соискателя из четырех наименований на одной странице.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

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

В **первой главе** приведены результаты анализа литературы, где рассмотрены характеристики волоконно-оптических линий связи. Определено, что при распространении луча света по оптическому волокну возможно искажение луча света в процессе движения по волокну (дисперсия), что повышает вероятность ошибочной регистрации данных. Для уменьшения дисперсии в многомодовом ОВ необходимо использовать волокна с плавным профилем показателя преломления, а для одномодовых ОВ – волокна со смещенной дисперсией либо волокна с компенсацией дисперсии.

Во **второй главе** дано описание предложенной системы связи, принципов ее функционирования. Описана процедура идентификации в системе связи. Предложенная система позволяет обеспечить криптозащищенную связь, безопасность которой основана на сложности факторизации большого числа. Установлены виды изгибов оптического волокна, определена зависимость вероятности потерь оптического сигнала от диаметра макроизгиба ОВ; длина волны оптического излучения. В сравнении с другими, наиболее эффективным способом несанкционированного снятия информации является способ создания локальной неоднородности в оптическом волокне за счет его макроизгиба.

В **третьей главе** дано описание принципов передачи защищенной от несанкционированного доступа информации для разработанного устройства. Предложенное устройство позволяет шифровать передаваемые данные, идентифицировать участинков системы связи, обнаруживать несанкционированный доступ, осуществляемый компенсационным методом. На основе разработанного приемного модуля оптического излучения предложена система передачи и приема конфиденциальных данных по волоконно-оптической линии связи, и, применительно к этой системе, экспериментально обоснован выбор длин волн излучения для передачи информации и для синхронизации времени передачи и приема информации и обнаружения несанкционированного доступа к информации, создаваемого посредством макроизгибов оптического волокна.

ЗАКЛЮЧЕНИЕ

На основании выполненного аналитического обзора литературных источников установлены основные особенности передачи информации по волоконно-оптическим линиям связи. Определено, что при распространении луча света по оптическому волокну со стандартным (ступенчатым) профилем показателя преломления в многомодовом оптическом волокне наблюдаются значительные показатели межмодовой дисперсии. Для уменьшения межмодовой дисперсии в многомодовом оптическом волокне следует использовать волокно с плавным (градиентным) показателем преломления.

Установлено, для предотвращения хроматической дисперсии одномодового волокна при работе на высоких скоростях передачи данных следует использовать волокна с компенсацией дисперсии, включающие в себя участки волокна с отрицательной дисперсией. В противном случае импульс будет подвергаться хроматической дисперсии при его распространении по оптическому волокну, увеличивая вероятность ошибочной регистрации данных.

Предложена система передачи и приема конфиденциальных данных по волоконно-оптической линии с идентификацией взаимодействующих сторон на основе методов криптоподобных преобразований информации, обеспечивающей криптографическую безопасность с помощью асимметричного криптографического алгоритма RSA с возможностью идентификации взаимодействующих сторон с помощью протокола идентификации с нулевой передачей знаний Фейге-Фиата-Шамира. Проведен анализ потерь сигнала на изгибах оптического волокна, из чего установлено, что вероятность потери оптического сигнала в оптическом волокне тем меньше, чем больше диаметр макроизгиба.

На основе предложенной системы связи разработано устройство конфидециальной передачи данных по волоконно-оптической линии связи, позволяющее автоматически обнаруживать несанкционированный доступ, осуществляемый путем формирования макроизгибов оптического волокна,. Экспериментально обоснован выбор двух длин волн излучения для работы устройства, одна из которых используется для передачи информации, а вторая – для синхронизации времени передачи и приема информации и обнаружения несанкционированного доступа к информации, создаваемого посредством макроизгибов оптического волокна.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1 Касько, В.А. Характеристики волоконно-оптических линий связи для передачи конфиденциальной информации / В.А. Касько, И.А. Ковалёв // Современные средства связи : материалы XXIII Междунар. науч.-техн. конф., 18-19 окт. 2018 года, Минск, Респ. Беларусь ; редкол. : А. О. Зеневич [и др.]. – Минск : Белорусская государственная академия связи , 2018. – с. 208-209.

2 Ковалёв, И.А. Двухключевая криптографическая система связи с возможностью обнаружения несанкционированного пользователя / И.А. Ковалёв, В.А. Касько // Современные средства связи : материалы XXIII Междунар. науч.-техн. конф., 18-19 окт. 2018 года, Минск, Респ. Беларусь ; редкол. : А. О. Зеневич [и др.]. – Минск : Белорусская государственная академия связи , 2018. – с. 209.

3 Исследование вероятности ошибочной регистрации символов «0» в квантово-криптографическом канале связи с приемным модулем на основе счетчика фотонов / А. М. Тимофеев [и др.] // Технические средства защиты информации : тезисы докладов XVII Белорусско-российской научно – технической конференции, Минск, 11 июня 2019 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол. : Т. В. Борботько [и др.]. – Минск, 2019. – С. 68 – 69.

4 Оценка потерь информации однофотонного канала связи с приемным модулем на основе счетчика фотонов / А. М. Тимофеев [и др.] // Технические средства защиты информации : тезисы докладов XVII Белорусско-российской научно – технической конференции, Минск, 11 июня 2019 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол. : Т. В. Борботько [и др.]. – Минск, 2019. – С. 69.