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

УДК 621.391; 621.383.92

Ковалёв
Илья Андреевич

Устройство обнаружения несанкционированного доступа к волоконно-оптической линии связи

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

Научный руководитель
Тимофеев Александр Михайлович
кандидат технических наук, доцент

Минск 2020

КРАТКОЕ ВВЕДЕНИЕ

В современном мире информация играет ключевую роль. В условиях всеобщей информатизации, вопросы информационной безопасности и защиты информации становятся наиболее актуальными. Проблемы конфиденциальности, целостности и подлинности циркулирующей в системах связи информации решает криптография. Появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем, еще недавно считавшихся практически нераскрываемыми. Все это постоянно подталкивает исследователей на создание новых криптосистем и тщательный анализ уже существующих.

В настоящее время для передачи данных широко используются волоконно-оптические линии связи, которые обладает массой преимуществ перед классическими проводными и беспроводными системами передачи информации. ВОЛС обладают высокой пропускной способностью и малыми оптическими потерями. Одной из важнейших задач, решаемых при разработке системы волоконно-оптической связи, является обеспечение конфиденциальности передаваемых данных. Сегодня это позволяют сделать квантовые оптические системы. Использование в квантовых системах маломощных оптических сигналов позволяет обнаружить любую попытку перехвата данных из канала связи. В таком случае необходимо применять приемные модули, которые способны регистрировать импульсы, содержащие от одного до десятка фотонов. Высокочувствительные приемные модули позволяют выполнить диагностику волоконно-оптических кабелей, обнаруживать потери оптического излучения, вызванные злоумышленником при внедрении в канал связи. Одним из наиболее чувствительных методов регистрации оптических сигналов является метод счета фотонов, а его реализация на базе кремниевых лавинных фотодиодов не требует применения схем охлаждения, в отличие от других типов фотоприемников. Однако, одним из основных недостатков существующих квантовых оптических систем является низкая пропускная способность, что ограничивает функциональные возможности таких систем. Причиной этого является наличие эффекта мертвого времени приемного модуля в квантовых системах, которое проявляется как интервал времени после регистрации фотона детектором, в течение которого он не может зарегистрировать следующий фотон.

Актуальность темы магистерской диссертации обусловлена быстрым развитием компьютеров с большими вычислительными мощностями и как следствие необходимостью разработки квантовых криптографических систем связи, которые бы обеспечивали не только шифрование и расшифрование конфиденциальной информации, но и предотвращали утечку зашифрованных

данных из канала связи и последующий их криптоанализ. Поэтому требуется разработка устройства обнаружения несанкционированного доступа к ВОЛС, которое сочетает преимущества двухключевых криптографических систем и квантовых оптических систем связи. Для повышения пропускной способности квантовой системы, содержащей в качестве приемного ЛФД, необходимо провести исследования влияния мертвого времени приемного модуля на пропускную способность квантового оптического канала связи.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Целью настоящей диссертационной работы является разработка устройства обнаружения несанкционированного доступа к волоконно-оптической линии связи и определение оптимального мертвого времени приемного модуля, при котором достигается максимальная пропускная способность канала связи.

Для достижения поставленной цели потребовалось решение следующих взаимосвязанных задач:

1 Исследовать основные элементы системы волоконно-оптической линии связи и определить наиболее подходящие для разрабатываемого устройства;

2 Рассмотреть особенности наиболее распространенных протоколов квантово-криптографической связи, выявить их достоинства и недостатки;

3 Обосновать выбор компонентов квантовой криптографической системы связи с возможностью обнаружения несанкционированного доступа;

4 Предложить структурную схему устройства обнаружения несанкционированного доступа к волоконно-оптической линии связи;

5 Установить зависимости быстродействия счетчика фотонов, пропускной способности квантовой оптической системы от напряжения питания ЛФД и интенсивности оптического излучения, используемого для передачи информации;

6 Определить формулу расчета пропускной способности квантового оптического канала связи;

7 Выполнить исследования влияния мертвого времени приемного модуля на пропускную способность канала связи разработанного устройства.

Исследуемым объектом является устройство обнаружения несанкционированного доступа к ВОЛС, содержащее в качестве приёмного модуля лавинный фотодиод, работающий в режиме счета фотонов. Предметом исследования являются разработка устройства обнаружения несанкционированного доступа и оптимизация схемы разрабатываемого устройства, направленные как на обеспечение безопасности передаваемой информации, так и на повышение пропускной способности канала связи.

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 XXIII Международной научно-технической конференции «Современные средства связи» (Минск, Республика Беларусь, 2018 г.) и XVII Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, Республика Беларусь, 2019 г.). Опубликовано четыре 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 74 страниц машинописного текста. Диссертация содержит 15 рисунков на 6 страницах, 5 таблиц на 1 странице. Библиографический список занимает 7 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 обнаружения несанкционированного доступа к ВОЛС и проведения исследований влияния мертвого времени приемного модуля квантовой системы на пропускную способность канала связи.

В **первой главе** приведены результаты анализа литературы, где рассматрены основные элементы системы волоконно-оптической линии связи. Такие системы обеспечивают высокую пропускную способность канала связи. Передача информации однофотонными импульсами позволяет обеспечить её защиту от несанкционированного доступа. Поэтому проводился сопоставительный анализ рассматриваемых элементов ВОЛС, на основании которого выявлено, что в качестве источника одиночных фотонов наиболее часто применяются псевдооднофотонные источники фотонов, основанные на ослаблении лазерных импульсов, одномодовые волокна хорошо подходят для передачи как многофотонного излучения, так и одиночных фотонов, а для их детектирования наиболее широко используются лавинные фотодиоды.

Во **второй главе** дано описание наиболее распространенных протоколов квантово-криптографической связи. Установлены два направления развития протоколов, которые базируются на кодировании квантового состояния одиночной частицы и на эффекте квантового перепутывания фотонов. Наиболее распространенные протоколы первого направления: BB84, B92, BB84 (4+2), с шестью состояниями, Гольденберга-Вайдмана, Коаши-Имото. Сравнительный анализ протоколов первого направления показал, что наиболее эффективным является протокол BB84, более поздние его модификации направлены на уменьшение процента ошибок и количества полезной информации, которую теоретически может получить злоумышленник. Обнаружено, что базовым протоколом квантового распределения ключа на основе эффекта квантового запутывания является протокол E91, в котором предлагается использовать пары фотонов, рождающихся в антисимметричных поляризационных состояниях. Перехват одного из фотонов пары не приносит злоумышленнику никакой информации, но является сигналом о несанкционированном доступе к системе.

В **третьей главе** диссертации в качестве устройства обнаружения несанкционированного доступа к волоконно-оптической линии связи предлагается двухключевая криптографическая система связи на базе алгоритма Рабина с возможностью обнаружения несанкционированного пользователя за счет применения кодирующего-декодирующего устройства с передачей криптограммы по ВОЛС. Дается оценка информационной безопасности и

надежности криптосистемы Рабина. Приводится описание работы схемы устройства обнаружения несанкционированного доступа к ВОЛС с примером временной диаграммой работы устройства. Работа предлагаемого кодирующего устройства заключается в том, что по оптической линии связи на одной длине волны транслируются синхроимпульсы и сигнальные импульсы. Функциональные возможности кодека позволяют вести контроль вероятности ошибки регистрации символов и автоматически отслеживать несанкционированный доступ к каналу связи. Преимущество устройства заключается в том, что информация может быть восстановлена полностью из зашифрованного текста только при условии, что дешифровщик способен к эффективной факторизации открытого ключа N. Но даже если несанкционированный пользователь и обладает такими вычислительными возможностями, то предлагаемая квантовая система позволит вовремя обнаружить его вмешательство в линию связи и остановить передачу, что делает построенную схему устройства обнаружения несанкционированного доступа к ВОЛС неуязвимой.

В **четвертой главе** дается описание результатов экспериментальных исследований влияния мертвого времени приемного модуля квантовой системы на пропускную способность канала связи разработанного устройства передачи данных по ВОЛС с возможностью обнаружения несанкционированного доступа. Выполнены исследования зависимостей быстродействия счетчиков фотонов, пропускной способности канала связи от напряжения питания ЛФД и интенсивности оптического излучения ИОФ. В ходе исследований определено, что величина напряжения питания ЛФД и интенсивность оптического изучения влияют на значения длительности мертвого времени ЛФД и квантовой эффективности регистрации счетчика фотонов. Так максимальное значение пропускной способности получено при наименьшей длительности мертвого времени и наибольшей квантовой эффективности регистрации. Для достижения максимальной пропускной способности канала связи, выполнялся подбор напряжения питания ЛФД и интенсивности оптического изучения. На основании результатов исследований проведен сопоставительный анализ лавинных фотодиодов ФД-115Л, ЛФД со структурами p^+n-ν-n^+ и n^+p-π-p^+. Исследования показали, что ЛФД с меньшими диаметрами фоточувствительной поверхности обладают меньшим значением длительности мертвого времени. В результате максимальная пропускная способность получена в случае с использованием ФД-115Л и ЛФД со структурой n^+p-π-p^+, и составила приблизительно 81 кбит/с при $\tau_м \approx 1$. Выбор компонентов квантовой оптической системы устройства осуществляется на основании описанных результатов экспериментальных исследований.

ЗАКЛЮЧЕНИЕ

В качестве устройства обнаружения несанкционированного доступа к волоконно-оптической линии связи предлагается двухключевая криптографическая система связи на базе алгоритма Рабина с возможностью обнаружения несанкционированного пользователя за счет применения кодирующего-декодирующего устройства с передачей криптограммы по ВОЛС.

Установлены основные элементы системы волоконно-оптической линии связи. Такие системы обеспечивают высокую пропускную способность канала связи. Передача информации однофотонными импульсами позволяет обеспечить её защиту от несанкционированного доступа. Выявлено, что в качестве источника одиночных фотонов наиболее часто применяются псевдооднофотонные источники фотонов, основанные на ослаблении лазерных импульсов, одномодовые волокна хорошо подходят для передачи как многофотонного излучения, так и одиночных фотонов, а для их детектирования наиболее широко используются лавинные фотодиоды.

Определены наиболее распространенные протоколы квантово-криптографической системы связи. Установлены два направления развития протоколов, которые базируются на кодировании квантового состояния одиночной частицы и на эффекте квантового перепутывания фотонов. Наиболее распространенные протоколы первого направления: BB84, B92, BB84 (4+2), с шестью состояниями, Гольденберга-Вайдмана, Коаши-Имото. Базовым протоколом на основе эффекта квантового запутывания является E91.

Сущность предлагаемого кодирующего устройства заключается в том, что по оптической линии связи на одной длине волны транслируются синхроимпульсы и импульсы, при помощи которых передаются зашифрованные данные. Функциональные возможности кодека позволяют вести контроль вероятности ошибки регистрации символов и автоматически отслеживать несанкционированный доступ к передаваемой информации.

Преимущество устройства заключается в том, что информация может быть восстановлена полностью из криптограммы только при условии, что дешифровщик способен к эффективной факторизации открытого ключа N. Но предлагаемая квантовая система позволяет вовремя обнаружить вмешательство в линию связи и остановить передачу, что делает построенную схему устройства обнаружения несанкционированного доступа к ВОЛС неуязвимой.

Выполнены экспериментальные исследования влияния мертвого времени приемного модуля квантовой системы на пропускную способность канала связи разработанного устройства передачи данных по ВОЛС с возможностью обнаружения несанкционированного доступа.

Выявлено, что величина напряжения питания ЛФД и интенсивность оптического изучения влияют на значения длительности мертвого времени и квантовой эффективности регистрации счетчика фотонов. Так максимальное значение пропускной способности получено при наименьшей длительности мертвого времени и наибольшей квантовой эффективности регистрации. Для достижения максимальной пропускной способности канала связи, выполнен подбор напряжения питания ЛФД и интенсивности оптического изучения.

На основании результатов исследований проведен сопоставительный анализ лавинных фотодиодов ФД-115Л, ЛФД со структурами p^+n-ν-n^+ и n^+p-π-p^+. Обнаружено, что ЛФД с меньшими диаметрами фоточувствительной поверхности показали меньшее значение длительности мертвого времени. В итоге максимальная пропускная способность получена в квантовых оптических системах, в которых использовались ФД-115Л и ЛФД со структурой n^+p-π-p^+, и составила приблизительно 81 кбит/с при $\tau_м \approx 1$.

Разработанное устройство, реализующее двухключевую криптографическую систему с использованием квантовой оптической системы, может найти применение в качестве системы волоконно-оптической связи, в которой осуществляется как шифрование передаваемой конфиденциальной информации, так и обнаружение несанкционированного доступа к каналу связи.

Предлагаемая схема соответствуют современным требованиям и может применяться в системах связи, в которых безопасность передаваемой конфиденциальной информации должна быть на высоком уровне, а также возможно ее использование в будущем для проведения других исследований в сфере защиты информации.

Выбор компонентов квантовой оптической системы устройства обнаружения несанкционированного доступа к ВОЛС осуществляется на основании описанных результатов экспериментальных исследований, что позволит обеспечить наибольшую скорость передачи информации и при этом её защиту от несанкционированного доступа.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1 – А.] 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.

[2 – А.] 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.

[3 – А.] 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 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 – А.] Тимофеев, А.М. 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.