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

УДК 004.056.5:621.39

ЗЛОБИНА
Юлия Валерьевна

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ ЗАЩИЩЁННОЙ СВЯЗИ

Автореферат
на соискание степени магистра
по специальности 1–98 80 01 Информационная безопасность

_____

Научный руководитель
Доцент кафедры защиты информации,
кандидат технических наук, доцент
ТИМОФЕЕВ Александр Михайлович

_____

_____

Минск 2023

ВВЕДЕНИЕ

В настоящее время для защиты информации при передаче применяют криптографические и криптоподобные преобразования данных, обеспечивающие конфиденциальность, целостность и доступность информации [1, 2, 3, 4, 5]. Для этого целесообразно использовать квантово-криптографические каналы связи, характеризующиеся абсолютной скрытностью и конфиденциальностью передаваемой информации [6, 7, 8].

Это становится возможным благодаря использованию в таких каналах связи квантового ресурса, например, поляризации, частоты, длины волны, отдельных фотонов оптического излучения [9, 10].

Одной из наиболее важных задач, решаемых при построении квантово-криптографических систем связи, является построение математических моделей каналов связи, позволяющих оценить пропускную способность каналов связи и учитывающих такие важные характеристики, как квантовая эффективность регистрации, вероятность появления темновых импульсов легитимного приёмника и др. [9, 10, 11].

Поскольку до настоящего времени такие математические модели отсутствуют, это являлось целю данной работы.

Для достижения поставленной цели потребовалось решение следующих взаимосвязанных задач:

1. Рассмотреть математические модели каналов связи и выбрать для рассмотрения подходящую модель, применимую к оптическо-волоконным системам передачи данных.
2. Провести аналитических обзор существующих систем связи с возможностью обеспечения конфиденциальности передаваемой информации и алгоритмов шифрования.
3. На основе выполненного обзора выбрать наиболее подходящую систему криптографической связи для проведения оценки её пропускной способности.
4. Разработать математическую модель волоконно-оптического канала связи при передаче данных сигналами малой мощности, учитывающую вероятность образования темновых импульсов и квантовую эффективность регистрации приемного модуля канала связи.
5. Экспериментально исследовать влияние таких факторов, как вероятность потерь, время и скорость передачи информации, энтропии на пропускную способность канала передачи информации.

В качестве объекта исследования использовался волоконно-оптический канал связи, в котором приемным модулем служит счетчик фотонов на базе лавинного фотодиода ФД-115Л, лавинных приёмниках со структурой металл – резистивный слой – полупроводник, серийно выпускаемое одномодовое оптическое волокно G.652 длиной 398 м.

Предметом исследований являлось установить, какое влияние оказывают макроизгибы оптического волокна на пропускную способность канала связи.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Целью данной диссертационной работы является разработка математической модели системы защищённой связи, позволяющей обнаружить нелегитимного пользователя путём анализа пропускной способности системы передачи информации.

Для достижения поставленной цели потребовалось решение следующих взаимосвязанных задач:

1. Рассмотреть математические модели каналов связи и выбрать для рассмотрения подходящую модель, применимую к оптическо-волоконным системам передачи данных.
2. Провести аналитических обзор существующих систем связи с возможностью обеспечения конфиденциальности передаваемой информации и алгоритмов шифрования.
3. На основе выполненного обзора выбрать наиболее подходящую систему криптографической связи для проведения оценки её пропускной способности.
4. Разработать математическую модель волоконно-оптического канала связи при передаче данных сигналами малой мощности, учитывающую вероятность образования темновых импульсов и квантовую эффективность регистрации приемного модуля канала связи.
5. Экспериментально исследовать влияние таких факторов, как вероятность потерь, время и скорость передачи информации, энтропии на пропускную способность канала передачи информации.

В качестве объекта исследования использовался волоконно-оптический канал связи, в котором приемным модулем служит счетчик фотонов на базе лавинного фотодиода ФД-115Л, лавинных приёмниках со структурой металл – резистивный слой – полупроводник, серийно выпускаемое одномодовое оптическое волокно G.652 длиной 398 м.

Предметом исследований являлось установить, какое влияние оказывают макроизгибы оптического волокна на пропускную способность 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.

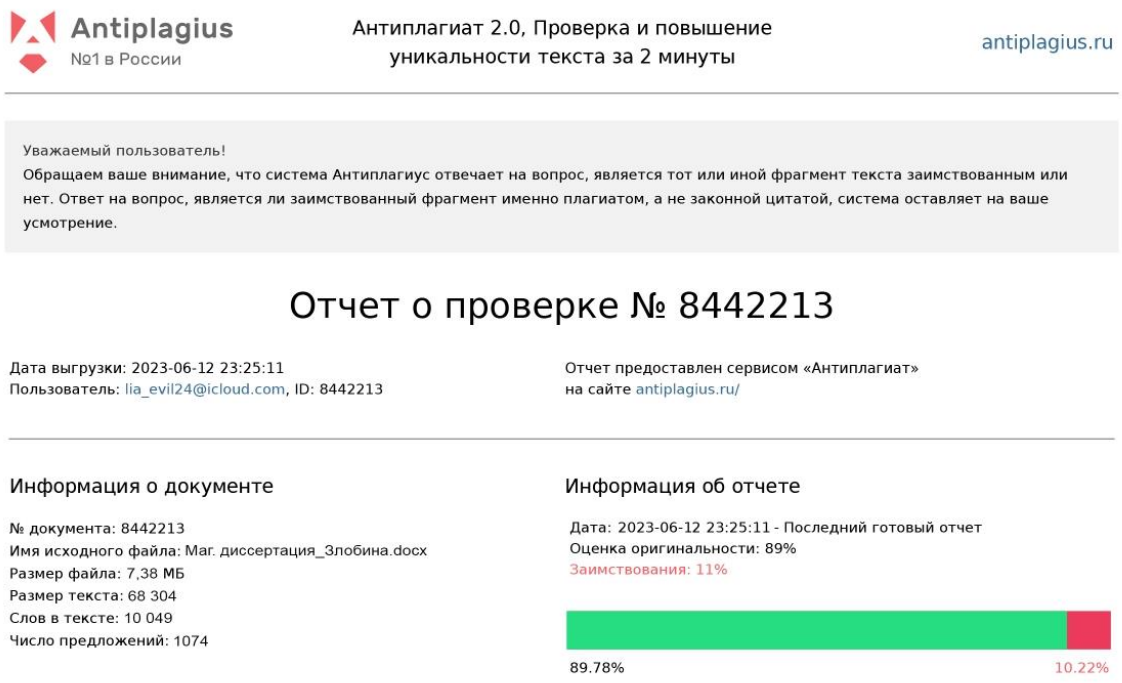
Апробация и опубликованность результатов

Основные полученные результаты диссертационной работы докладывались на 14-й Международной научно-технической конференции «Приборостроение – 2021», XX Белорусско-российской научно-технической конференции и XI Белорусско-Российской научно-технической конференции «Технические средства защиты информации». Опубликованы тезисы доклада, научные статьи «Потери информации в квантово-криптографическом канале связи» и «Математическая модель квантово-криптографического канала связи с приемным модулем на основе счетчика фотонов».

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, трех глав, заключения и библиографического списка. Полный объем диссертации составляет 50 страниц машинописного текста. Диссертация содержит 9 рисунков на 3 страницах, 2 таблицы на 2 страницах. Библиографический список занимает 4 страницы и состоит из 50 наименований использованных источников и списка собственных публикаций соискателя из трёх наименований на одной странице.

Проверка на уникальность



Antiplagius
№1 в России

Антиплагиат 2.0, Проверка и повышение уникальности текста за 2 минуты

antiplagius.ru

Уважаемый пользователь!
Обращаем ваше внимание, что система Антиплагиус отвечает на вопрос, является тот или иной фрагмент текста заимствованным или нет. Ответ на вопрос, является ли заимствованный фрагмент именно плагиатом, а не законной цитатой, система оставляет на ваше усмотрение.

Отчет о проверке № 8442213

Дата выгрузки: 2023-06-12 23:25:11
Пользователь: lia_evil24@icloud.com, ID: 8442213

Отчет предоставлен сервисом «Антиплагиат»
на сайте antiplagius.ru/

Информация о документе

№ документа: 8442213
Имя исходного файла: Маг. диссертация_Злобина.docx
Размер файла: 7,38 МБ
Размер текста: 68 304
Слов в тексте: 10 049
Число предложений: 1074

Информация об отчете

Дата: 2023-06-12 23:25:11 - Последний готовый отчет
Оценка оригинальности: 89%
Заимствования: 11%

89.78%

10.22%

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении к магистерской диссертации рассмотрена проблема защиты информации при передаче. Отмечается важность разработки математических моделей каналов связи, учитывающих квантовую эффективность регистрации, вероятность появления темновых импульсов, вероятность потерь и другие важные характеристики. Поставлены цели и сформулированы задачи для их достижения.

Во общей характеристике работы представлено обоснование актуальности исследования, а также обозначен личный вклад соискателя в данную работу.

В первой главе представлен обзор математических моделей каналов связи. Рассмотрены модели непрерывных каналов связи без шума, с аддитивным гауссовым шумом и с неопределенной фазой сигнала. Описана математическая модель дискретного канала связи и модель дискретно-непрерывного канала связи. В результате сравнения математических моделей каналов связи было установлено, что модель непрерывного канала связи без шума, модель с аддитивным гауссовским шумом и модель с неопределённой фазой сигнала применяются для исследования электрических каналов связи. Каждая модель имеет свои преимущества и применима в определенных ситуациях, включая проводные и радиосвязные каналы. Волоконно-оптические каналы связи широко распространены, и для их описания подходит математическая модель дискретного канала связи в то время, как предыдущие модели оказываются непригодными.

В второй главе рассматриваются системы связи с возможностью обеспечения конфиденциальности передаваемой информации. Описываются одноключевые и двухключевые системы криптографической связи, а также системы на основе гибридного метода шифрования данных. Приводятся выводы по данной главе.

В третьей главе представлена разработка математической модели системы передачи конфиденциальных данных. Проведён анализ систем передачи информации с использованием количественных мер, таких как пропускная способность канала связи, энтропия и скорость передачи данных. Рассмотрена проблема утечки информации в квантовом канале связи через макроизгиб оптического волокна. Разработана математическая модель канала связи

ЗАКЛЮЧЕНИЕ

В данной магистерской диссертации были рассмотрены вопросы, связанные с волоконно-оптическими каналами связи и квантовыми каналами связи. Исследования показали, что для описания волоконно-оптических каналов связи целесообразно использовать математическую модель дискретного канала связи, учитывающую особенности таких каналов.

В работе была предложена и построена математическая модель квантового канала связи, содержащего в качестве приемного модуля счетчик фотонов. Для этого канала связи были получены соответствующие выражения, позволяющие определять его пропускную способность как на участке между легитимными пользователями, так и на участке между легитимной передающей стороной и нелегитимным пользователем.

Оценка пропускной способности на участке между легитимными пользователями учитывает различные параметры, такие как вероятность несанкционированного вывода мощности излучения из оптического волокна ($P_{пот}$), вероятность появления темновых импульсов (P_t) и квантовую эффективность регистрации (η_p). Данные выражения позволяют оценить эффективность передачи данных в квантовом канале связи и провести анализ безопасности системы передачи информации.

Результаты исследования указывают на преимущества двухключевых систем криптографической связи по сравнению с одноключевыми системами, включая более безопасный обмен ключами и более высокий уровень безопасности. Кроме того, длина ключа существенно влияет на уровень безопасности в двухключевых системах.

Магистерская диссертация обобщает существующие знания о волоконно-оптических и квантовых каналах связи, а также представляет новые математические модели и выражения, которые могут быть использованы для оценки пропускной способности и безопасности систем передачи информации. Результаты исследования могут быть полезны для разработки и оптимизации квантовых систем связи и обеспечения безопасной передачи данных. Дополнительные исследования могут быть проведены для более детального изучения влияния других параметров, таких как тип волокна, радиус изгиба и другие, на пропускную способность канала утечки информации. Это поможет более полно понять и оптимизировать системы передачи данных, основанные на макроизгибе оптического волокна.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1–А Тимофеев, А. М. Потери информации в квантово-криптографическом канале связи / А. М. Тимофеев, Ю. В. Злобина, А. Л. Чупина // Приборостроение – 2021: материалы докладов XIV Международной научно-технической конференции, Минск, 17-19 ноября 2021 г. / Белорусский национальный технический университет ; редкол.: О. К. Гусев [и др.]. – Минск, 2021. – С. 131–132.

2–А Тимофеев, А. М. Математическая модель квантово-криптографического канала связи с приемным модулем на основе счетчика фотонов / Тимофеев А. М., Злобина Ю. В. // Технические средства защиты информации : тезисы докладов XX Белорусско-российской научно-технической конференции, Минск, 7 июня 2022 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Т. В. Борботько [и др.]. – Минск, 2022. – С. 101 – 102.