Министерство образования Республики Беларусь

Учреждение образования

Белорусский государственный университет

информатики и радиоэлектроники

УДК 621.383

Корбут

Матвей Валентинович

СИСТЕМА ВЫСОКОСКОРОСТНОГО РАСПРЕДЕЛЕНИЯ СЕКРЕТНЫХ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ ПО ВОЛОКОННО-ОПТИЧЕСКИМ КАНАЛАМ СВЯЗИ

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-98 80 01 Информационная безопасность

Научный руководитель

Тимофеев А.М.

Кандидат технических наук, доцент

Минск 2021

ВВЕДЕНИЕ

В настоящее время информационная безопасность – одно из приоритетных направлений развития современных средств связи, в которых данные передаются по волоконно-оптическим линиям связи. Обеспечить защиту информации от несанкционированного доступа можно с помощью систем связи, использующих для защиты информации криптографические и криптоподобные преобразования данных. При этом работа указанных систем возможна только при условии наличия у санкционированных сторон секретных ключей. Передача этих ключей выполняется по защищенным каналам связи.

Следует отметить, что при организации криптографических каналов связи необходимо учитывать, что в случае получения злоумышленником шифротекстов информационная безопасность таких каналов может быть уменьшена в случае, если злоумышленник обладает неограниченными вычислительными ресурсами. Так, например, при известном алгоритме щифрования и расшифрования существует возможность перебора всех возможных значений секретного ключа с использованием соответствующих вычислительных ресурсов.

Абсолютной скрытностью и конфиденциальностью передаваемой информации характеризуются квантовые системы связи. Данные системы основаны на использовании квантово-механического ресурса для кодирования передаваемой информации (поляризации передаваемых фотонов, частоты, фазы и других параметров).

Однако, известные устройства используемые для организации такой защищенной связи, характеризуются достаточно низкой скоростью передачи информации. Это обусловлено тем, что существующие системы квантово-криптографической связи требуют несколько циклов передачи и приема информации от отправителя к получателю.

В связи с этим целью данной работы являлась разработка системы волоконно-оптической связи, позволяющей повысить скорость распределения секретных криптографических ключей.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью данной работы являлась разработка системы волоконно-оптической связи, позволяющей повысить скорость распределения секретных криптографических ключей.

Для достижения поставленной цели потребовалось решение следующих взаимосвязанных задач:

1 Рассмотреть основные криптографические системы и методы защиты информации, существующую элементную базу.

2 Изучить методы несанкционированного съема информации из канала связи на физическом уровне и уровне приложений

3 Предложить способ передачи ключа по волоконно-оптической линии связи

Тема диссертации соответствует приоритетным направлениям научных исследований в Республике Беларусь на 2021–2025 годы, установленным Указом Президента Республики Беларусь от 7 мая 2020 г. № 156 «О приоритетных направлениях научной, научно-технической и инновационной деятельности на 2021–2025 годы» п. 6.3 «Средства технической и криптографической защиты информации, криптология и кибербезопасность».

Личный вклад соискателя

Результаты исследований получены автором самостоятельно. Научный руководитель принимал участие в определении целей и задач исследования, интерпретации промежуточных результатов.

Апробация результатов диссертации

По теме диссертации опубликовано 3 тезиса доклада в сборниках материалов конференции.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе рассмотрены наиболее распространенные алгоритмы и стандарты криптографической защиты информации (DES, 3DES, IDEA, ГОСТ 28147-89, RSA, Эль Гамаля, Полига-Хеллмана), установлены их основные преимущества и недостатки.

Приведены основные криптографические протоколы для передачи конфиденциальных данных:

- SSL;
- TLS;
- SSH;
- Kerberos;
- IPSec.

Также рассмотрены квантово-криптографические системы связи, основанные на поляризационном кодировании передаваемых данных, фазовом кодировании и временном кодировании.

Во второй главе приведены основные методы несанкционированного доступа к информации на физическом уровне и уровне приложений. Определены наиболее распространенные программные и физические средства защиты информации.

В третьей главе рассмотрена пропускная способность волоконно-оптического канала связи. Приведен способ оценки максимальной скорости передачи информации.

Предложено устройство высокоскоростной передачи и приема криптографического ключа, позволяющее уменьшить ошибку передачи данных, связанную с деполяризацией оптического излучения, упростить процедуру согласования базисов, в которых переданы и приняты символы при формировании ключа, и повысить за счет этого скорость передачи ключа.

Приведена структурная схема разработанного устройства, а также пример случайной селекции оптического излучения по длине волны и углу линейной поляризации.

Проведено исследование пропускной способности квантового канала связи, получены зависимости пропускной способности квантово-криптографического канала связи от длины оптического волокна без учета вероятности деполяризации передаваемых фотонов, с учетом вероятности деполяризации и вероятность поглощения передаваемых фотонов.

ЗАКЛЮЧЕНИЕ

На основании выполненного аналитического обзора литературных источников определены наиболее распространенные алгоритмы и стандарты криптографической защиты информации. Установлено, что существующие алгоритмы и стандарты характеризуются недостатком, вызванным необходимостью передачи и приема ключевой информации по незащищенным каналам связи (симметричные криптосистемы), а также весьма сложными вычислениями, требующими возведения в степень больших чисел в большую степень (разрядностью от 1500 десятичных разрядов до 3000 - несимметричные криптосистемы).

Определены наиболее распространенные программные и физические средства защиты информации, установлены преимущества и недостатки программных средств.

Рассмотрены квантово-криптографические системы связи, основанные на поляризационном кодировании передаваемых данных, фазовом кодировании и временном кодировании. Определено, что общим недостатком таких систем является необходимость передачи и приема «сырого» ключа от получателя к отправителю данных на втором этапе обмена ключевой информации. В результате этого скорость передачи информации по каналу связи снижается.

Разработана система передачи и приема ключевой информации, сущность функционирования которой основана на выполнении калибровочного цикла и цикла передачи и приема данных. В течение калибровочного цикла определяют квантовую эффективность регистрации, а также длины волн оптического излучения для передачи данных. В течении цикла передачи и приема данных в начале передают.

Предложенная система отличается от существующих большей скоростью обмена ключевой информацией за счет того, что в ней отсутствует необходимость передачи от получателя к отправителю информации о

выбранном угле линейной поляризации, что выполняется в существующих системах. За счет этого скорость передачи ключевой информации повышается, что позволяет увеличить пропускную способность каналов связи.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1 Тимофеев, А.М. Потери информации при ее измерении в асинхронном квантово-криптографическом канале связи / А.М. Тимофеев, А.С. Колядич, М.В. Корбут // Приборостроение – 2019: материалы докладов XXII Междунар. науч.-техн. конф., Минск, 13-15 нояб. 2019 г. / Белорус. нац. техн. ун-т; редкол.: О.К. Гусев [и др.]. – Минск, 2019. – С. 75–77.

2 Тимофеев, А.М. Достижение наименьших потерь информации в однофотонном канале конфиденциальной связи / А.М. Тимофеев, А.С. Колядич, М.В. Корбут // Технические средства защиты информации: материалы докладов XVIII Междунар. Белорусско-российской науч.-техн. конф., Минск, 9 июня 2020 г. / Белорус. гос. ун-т информатики и радиоэлектроники; редкол.: Т.В. Борботько [и др.]. – Минск: БГУИР, 2020. – С. 76.

Корбут, М.В. Система высокоскоростного распределения ключевой информации / Корбут, М.В. // XVII Международная научно-практическая конференция «Управление информационными ресурсами» Академия управления при Президенте Республики Беларусь, РИВШ. Минск, 12 марта 2021 г. – Минск, 2021. – С. 214–215