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

УДК_____

Буренков
Андрей Радикович

# Разработка программного обеспечения для шифрования высокоскоростного трафика

**АВТОРЕФЕРАТ**
на соискание степени магистра технических наук
*(указать отрасль наук)*
по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность
*(шифр и название специальности согласно учебному плану)*

_____
*(подпись магистранта)*

Научный руководитель
Першин Виктор Тихонович
*(фамилия, имя, отчество)*
Кандидат физ.-мат. наук, доцент
*(ученая степень, ученое звание)*

_____
*(подпись научного руководителя)*

Минск 2016

Библиотека БГУИР

# ВВЕДЕНИЕ

Вопрос безопасности связи всегда был одним из самых важных в сетях телекоммуникаций. В настоящее время в связи с бурным развитием глобальных компьютерных сетей, и в том числе сети интернет, обеспечение безопасности передачи информации становится еще более актуальным, поскольку темпы развития технологий взлома не отстают от темпов развития сетей передачи данных. Таким образом, обеспечение безопасности передачи информации по сетям общего пользования является предметом настоящей работы.

Целью работы является разработка программного обеспечения, обеспечивающего конфиденциальность и целостность данных, передаваемых по сетям общего пользования с высокой скоростью. Для достижения цели, ставятся следующие задачи: анализ проблемы и обзор существующих решений, обоснование предлагаемого решения, реализация предложенного решения в виде программного средства.

Под сетями общего пользования в данной работе понимаются локальные сети и глобальная сеть интернет. Самым распространенным протоколом обмена данными в таких сетях является межсетевой протокол IP, это маршрутизируемый протокол сетевого уровня стека TCP/IP, именно протокол IP объединил в одну глобальную сеть все сегменты локальных сетей. При помощи сетей построенных на этом протоколе можно обмениваться любым типом трафика. Обмен происходит за счет заключения информации в пакет разделенный на служебную и информативную части.

Основной проблемой безопасности в данном случае является нахождение на пути прохождения трафика множества различных устройств, к которым не применимы административные меры обеспечения безопасности.

Для обеспечения целостности и конфиденциальности передуваемой информации применяется комплекс мер состоящий из шифрования передаваемых данных и контроля целостности зашифрованных данных. При применении подобных мер пакеты интернет трафика проходящие по сети распространяются в понятном виде для маршрутизации, но содержат зашифрованные информационные сообщения, что и обеспечивает конфиденциальность передаваемых данных, не внося помех в маршруты их распространения.

Разработанное программное средство должно обеспечивать защиту на сетевом уровне, выполнять криптографические манипуляции с передаваемыми данными согласно стандартам примиряемым в Республике Беларусь, обладать достаточным уровнем защищенности, не вносить помехи для работы различного программного обеспечения установленного на устройствах конечных потребителей сети, обеспечивать шифрование данным на скорости до

Библиотека БГУИР

1Гбит в секунду. Так же программное средство должно обладать гибкостью в настройке и возможностью установки на аппаратные комплексы различной вычислительной мощности будь то высокопроизводительные серверные решение или же низкопроизводительные небольшие устройства для защиты каналов сети.

Новизна разработанного устройства заключается в наличии реализации сертифицированных в Республике Беларусь криптографических алгоритмов, гибкости применения и высокой масштабируемости решения.

В данной диссертационной работе представлено исследование и разработка программного обеспечения для шифрования высокоскоростного трафика.

Библиотека БГУИР

# ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Связь работы с приоритетными направлениями научных исследований**

Тема диссертационной работы соответствует пункту 13 «Безопасность человека, общества и государства» приоритетных направлений научных исследований Республики Беларусь на 2016 – 2020 годы., утверждённых Постановлением Совета Министров Республики Беларусь от 12 марта 2015 года № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

**Цель и задачи исследования**

Цель диссертационной работы разработка и внедрение в эксплуатацию программного обеспечения для шифрования высокоскоростного трафика.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать современные стандарты и методики в области защиты конфиденциальности данных передуваемых по сетям общего пользования.
2. Определить способы и средства для выполнения поставленной задачи.
3. Спроектировать и разработать программный продукт.
4. Провести апробацию полученного решения.

**Личный вклад соискателя**

Все основные результаты, выводы получены соискателем самостоятельно. Разработка программного обеспечения для шифрования высокоскоростного трафика так же выполнена самостоятельно

**Апробация результатов диссертации**

Результатом диссертационной работу является готовое программное решение прошедшее государственные испытания в оперативно-аналитическом центре при президенте республики Беларусь, внедренное в производство и проходящее сертификацию на соответствие стандартам республики Беларусь о применение криптографических методов защиты информации.

**Опубликованность результатов диссертации**

По результатам исследований, представленных в диссертации, публикаций нет, но опубликована 1 работа, не относящаяся к теме диссертации в том числе 1 статьи в сборниках материалов конференций.

Библиотека БГУИР

# КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

**Первая глава** «Анализ существующих методов защиты данных передаваемых по сетям общего пользования» состоит из двух основных частей, а так же описывает основные угрозы для информации передуваемой по сетям общего трафика.

Первая часть «Основные протоколы защиты информации в сетях общего пользования» содержит описание и сравнение основных протоколов защиты информации передаваемой по сетям общего доступа. Так же первая часть разделена на пять разделов. В первом разделе «Набор протоколов защиты информации IPSec» приведено общее описание методов защиты IP трафика с помощью набора протоколов IPSec. Второй раздел «Структура IPSec» посвящен описанию структуры и основных частей набора протоколов криптографической защиты IPSec. Третий раздел «Протокол обмена ключами IKE» описывает алгоритмы и методы протокола выработки и согласования ключей применяемых для симметричного шифрования. В четвертом разделе «Принцип работы IPSec» кратко описан общий принцип работы выбранных протоколов безопасности. Пятый раздел «Пример реализации VPN сети с помощью IPSec» содержит описание защищенной виртуальной частной сети, и способ её реализации с помощью набора протоколов IPSec.

Вторая часть «Программное средство с открытыми кодами Strongswan» описывает программное средство, выбранное как основа будущего программного обеспечения, и разделена на четыре раздела. В первом разделе «Структура Strongswan» приведен перечень компонентов программного средства, и описаны методы и способы их взаимодействия. Второй раздел «Установка и настройка Strongswan» содержит описание способа установки и сборки программного средства поставляемого в виде архива с исходными текстами, а так же описан способ его настройки. Третий раздел «Сценарии использования Strongswan» описывает три наиболее распространенные сценария организации защищенной сети с использованием программного обеспечения Strongswan. В четвертом разделе «Общий анализ Strongswan» приведен краткий анализ и сделаны выводы о пригодности к использованию программного обеспечения Strongswan, для создания на его основе комплекса крипто-графической защиты высокоскоростного трафика. В конце главы приведены краткие выводы относительно информации рассмотренной в первой главе

**Вторая глава** «Выбор среды разработки и методов криптографической защиты» разделена на три части.

Первая часть «Выбор среды разработки» разделена на четыре раздела. В первом разделе «Выбор операционной системы для разработки программы»

Библиотека БГУИР

выбрана операционная система для которой будет проектироваться программное обеспечение. Второй раздел «Выбор языка программирования» посвящен описанию выбранных языков программирования, их плюсах и минусах. Третий раздел «Выбор инструментальной среды» описывает инструменты примененные для написания исходного кода программы. Четвертый раздел «Выбор средств сборки и установки» описывает примененные методы компиляции программного средств, а так же метод установки программного обеспечения на компьютеры потребителей.

Вторая часть «Выбор криптографических алгоритмов» описывает криптографические алгоритмы используемые для шифрования, хэширования и контроля целостности в разработанном программном обеспечении.

Третья часть «Выбор алгоритмов преобразования ключей» посвящена описанию криптографических алгоритмов применяемых для выработки сеансовых ключей на основе эллиптических кривых, обработки сертификатов открытых ключей и генерации секретных личных ключей.

В завершение главы приведены краткие выводы.

**Третья глава** «Разработка программного обеспечения для шифрования высокоскоростного трафика» разделена на шесть частей.

Первая часть «Разработка криптографической библиотеки» посвящена процессу переработки библиотеки ContactCrypto32LE для обеспечения взаимодействия с разрабатываемым программным средством.

Вторая часть «Разработка модулей ядра операционной системы», описывает специфические особенности ядра Линукс, в отличии от программ исполняемых в пользовательском пространстве, приведена характеристика разработанного модуля ядра реализующего функции шифрования, хеширования и генерации случайной последовательности.

В третьей части «Разработка плагинов и модернизация исходных кодов программы Strongswan» описываются программные модули добавленные в основное программное средство, и процесс его модернизации для выполнения требуемых криптографических функций. Так же описан расширяемый протокол аутентификации.

Четвертая часть «Разработка приложений тестирования и контроля целостности» описывает реализованный способ тестирования программного средства для определения правильности работы, и соответствия стандартам регламентирующим применение криптографических алгоритмов. Так же описана система контроля целостности программного обеспечения

Пятая часть «Тестирование программного комплекса на соответствие требованиям» приведены данные измерения скорости шифрования и пропускной способности программного комплекса.

Библиотека БГУИР

В шестой части «Анализ полученного программного обеспечения» проведен краткий анализ разработанного средства, оценены его новизна и конкурентоспособность, приведено сравнение с возможными конкурентными решениями. Сделаны выводы об эффективности готового программного решения.

В конце главы сделаны краткие выводы о разработке программного средства и его технико экономическом анализе.

Библиотека БГУИР

# ЗАКЛЮЧЕНИЕ

В ходе выполнения работы были проанализированы современные стандарты и методики в области анализа систем защиты информации передаваемой по сетям общего пользования, и разработано программное средство обеспечивающее криптографическую защиту информации на сетевом уровне.

Разработанный модуль криптографической защиты высокоскоростного трафика выполняет криптографические операции шифрования, контроля целостности, управления криптографическими ключами в соответствии со стандартами Республики Беларусь, с целью обеспечения конфиденциальности, подлинности и целостности информации ограниченного распространения. Также данное программное обеспечение предназначено для:

- создания защищенных локальных сетей передачи данных,
- обеспечения безопасного удаленного доступа к защищенным сетям,
- взаимодействия с защищенными хранилищами критичных данных (личных криптографических ключей, прочих персональных данных, требующих защиту от несанкционированного доступа);
- генерации криптографических ключей;
- генератора случайных чисел.

Разработанное программное средство обеспечивает конкурентоспособность в отношении аналогичных устройств Республики Беларусь, Украины, Казахстана, Узбекистана и Российской Федерации.

Также реализованное программное средство может применяться на различных типах устройств и различных операционных системах, программное средство не вносит помех в маршрутизацию сообщений и не ограничивает возможности использования различного программного обеспечения на клиентском оборудовании.

Из всего написанного ранее можно сделать вывод, что программное обеспечение для шифрования высокоскоростного трафика — очень полезное нововведение в информационных системах Республики Беларусь, в которых необходимо использование криптографической защиты информации ограниченного распространения, передающейся по сетям общего пользования.

Библиотека БГУИР

**Список публикаций соискателя**

1-А. Буренков А.Р. Модуляция положением импульса в радио идентификаторах / А.Р. Буренков В.Т. Першин // Технические средства защиты информации: тезисы докладов XIII Белорусско-Российской науч.–техн. конф., Минск 4 - 5 июня 2015 г. / БГУИР, редкол.: Л.М. Лыньков [и др.]. - Минск, 2015. - С.38

Библиотека БГУИР