МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра     Систем сбора и обработки данных

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА**

***Ермошенко Павла Андреевича***

(фамилия, имя, отчество автора)

***Создание протокола защищенного обмена данными. Разработка серверного приложения.***

|  |  |
| --- | --- |
| Направление подготовки | ***230200 Информационные системы*** |

|  |  |
| --- | --- |
| **Руководитель**  ***Воронов В.В.***  (фамилия, И.О.)  ***Старший преподаватель кафедры ССОД***  (уч. степень, уч. звание)  (подпись, дата) | **Автор**  ***Ермошенко П.А.***  (фамилия, И.О.)  ***АВТ,*** ***АТ-03***  (факультет, группа)  (подпись, дата) |

Новосибирск, 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра    Систем сбора и обработки данных

|  |  |
| --- | --- |
|  | Утверждаю  Зав. кафедрой  (подпись)  Белик Д.В.  (фамилия, инициалы)  « »   г. |

**ЗАДАНИЕ  
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ БАКАЛАВРА**

студенту ***Ермошенко Павлу Андреевичу***

(фамилия, имя, отчество студента)

|  |  |
| --- | --- |
| Направление подготовки | ***230200 Информационные системы*** |

***Факультет автоматики и вычислительной техники***

Тема  ***Создание протокола защищенного обмена данными. Разработка серверного приложения.***

Исходные данные (или цель работы):

*Создание защищенного протокола, позволяющего производить обмен любыми данными через незащищенный канал. Протокол должен обеспечивать как конфиденциальность, так и невозможность подмены данных.*

Структурные части работы:

1. Изучение предметной области:
   1. Существующие алгоритмы шифрования. Преимущества/недостатки.
   2. Известные атаки на алгоритмы. Способы защиты от известных атак.
2. Выбор параметров будущей системы. Определение основных принципов.
3. Подбор спецификаций демонстрационной системы (серверного приложения).
4. Создание протокола с учетом существующих методов шифрования и атак на них.
5. Создание серверного приложения. Тестирование приложения на полное соответствие с заявленным протоколом.
6. Описание полученной технологии. Создание ВКР.

**План-график выполнения работы**

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование этапа | Планируемые сроки выполнения |
| 1 | Анализ существующих алгоритмов шифрования, их преимуществ/недостатков а также известных атак. Анализ способов защиты от известных атак. | 12.02.2014 – 01.04.2014 |
| 2 | Выбор параметров будущей системы. Определение основных принципов. | 05.04.2014 – 15.05.2014 |
| 3 | Подбор спецификаций демонстрационной системы (серверного приложения). | 15.05.2014 – 20.05.2014 |
| 4 | Создание протокола с учетом существующих методов шифрования и атак на них. | 20.05.2014 – 26.05.2014 |
| 5 | Создание серверного приложения. Тестирование приложения на полное соответствие с заявленным протоколом. | 26.05.2014 – 07.06.2014 |
| 6 | Описание полученной технологии. Создание ВКР. | 07.06.2014 – 20.06.2014 |

Задание согласовано и принято к исполнению.

|  |  |
| --- | --- |
| **Руководитель**  ***Воронов В.В.***  (фамилия, И.О.)  ***кафедры ССОД***  (уч. степень, уч. звание)    ***(***подпись, дата) | **Автор**  ***Ермошенко П.А.***  (фамилия, И.О.)  ***АВТ, АТ-03***  (факультет, группа)    ***(***подпись, дата) |

Тема утверждена приказом по НГТУ №***6550/2***  от « ***4*** »***декабря***  ***2013*** г.

(подпись секретаря экзаменационной комиссии по защите ВКР, дата)

(фамилия, инициалы секретаря экзаменационной комиссии по защите ВКР)

# Реферат

Данная выпускная квалификационная работа содержит quint8 n; страниц, quint8 m иллюстраций и quint8 o; таблиц. В процессе создания этой работы были использованы следующие источники:

* Раздел Information Security на Stack Exchange: <http://security.stackexchange.com/>
* Стандарт RFC5114 описывающий выбор параметров открытых ключей для алгоритма Диффи-Хеллмана: <http://www.ietf.org/rfc/rfc5114.txt>
* Спецификация Rijndael (победителя конкурса на Advanced Encryption Standard – AES):  
  <http://en.wikipedia.org/wiki/Advanced_Encryption_Standard>
* Спецификация PKI – Public Key Infrastructure:  
  <http://en.wikipedia.org/wiki/Public_key_infrastructure>
* Описание схемы шифрования RSA:  
  <http://en.wikipedia.org/wiki/RSA_(cryptosystem)>
* Описание схемы обмена ключами Диффи-Хеллмана:  
  <http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange>

Целью этой работы является создание защищенного протокола на основе SSL/TLS. В отличие от TLS (который применяется в основном при передаче данных в Internet – веб страниц), данный протокол предназначен для применения в более узких областях. Небольшая распространенность является его преимуществом по отношению к TLS – не требуется продолжительная поддержка более старых версий (которая обычно влечет к дополнительным уязвимостям).

Объектом исследования являются криптографические алгоритмы и их реализации. Анализ существующих атак и методов защиты от них позволяет повысить устойчивость полученного протокола.

В ходе выполнения этой работы был разработан протокол защищенного обмена данных по незащищенному каналу. Протокол берет свой дизайн из широко известного и популярного протокола TLS (бывший SSL). В его основе лежат такие криптографические алгоритмы, как RSA, Rijndael (AES) и технология обмена ключами Диффи-Хеллмана. После разработки протокола он был реализован в серверном приложении написанном на C++/QT(возможно развертывание на всех трех основных операционных системах: Windows NT, Linux, OSX). Также в совместном проекте существует совместимое клиентское приложение. Протокол не ограничен “банковской” сферой применения и созданные приложения являются лишь примерами его применения.

Криптографическая защита данных является очень популярной областью исследования (множество людей задействовано по всему миру ввиду ценности информации в современном мире) и любые полученные результаты требуют постоянного обновления, чтобы оставаться достоверными. *Потому* ***блять*** *написание бумажек в 40 листов is a waste of time.*

Созданный протокол не привязан к типу передачи данных и требует лишь наличие механизма, отвечающего за доставку данных через сеть (или другую используемую среду), такого как TCP (Transmission Control Protocol – один из двух основных протоколов транспортного уровня используемых в Internet).

В данную работу не входит создание физического устройства, в связи с чем ее объем несколько ниже среднего.

Ключевые слова: **RSA**, **DH**, **AES**, **TLS**, **криптография**, **шифрование**.

Содержание

[Реферат 5](#_Toc390083737)

[Введение 8](#_Toc390083738)

# Введение