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 по протоколу HTTP через 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(что позволяет использовать полученное приложение 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 наше время) и любые полученные результаты требуют постоянного обновления, чтобы оставаться достоверными.

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, вторым является UDP).

Система, полученная в процессе выполнения данной работы, была создана с учетом существующих атак и методов взлома. Однако, перед использованием этой системы в корпоративных целях стоит провести полный аудит безопасности с целью повторной проверки принципов алгоритмов, ответственных за защиту конфиденциальных данных.

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

**Содержание**

[Реферат 5](#_Toc390176213)

[Введение 9](#_Toc390176214)

[Глава 1: Описание предметной области 12](#_Toc390176215)

[1.1. Анализ состояния разрабатываемого вопроса 12](#_Toc390176216)

[1.2. Исследование существующих методов шифрования, их достоинств и недостатков 12](#_Toc390176217)

[1.3. Выводы по результатам проработки предметной области 12](#_Toc390176218)

[Глава 2: Описание нового протокола 13](#_Toc390176219)

[2.1. Описание новых методов шифрования и защиты данных 13](#_Toc390176220)

[2.2. Создание нового протокола 13](#_Toc390176221)

[2.3. Анализ нового протокола с учетом известных атак на существующие системы 13](#_Toc390176222)

[Глава 3: Разработка серверного приложения 14](#_Toc390176223)

[3.1. Описание будущего проекта 14](#_Toc390176224)

[3.2. Создание серверного приложения, описание дизайна 14](#_Toc390176225)

[3.3. Оценка получившегося решения 14](#_Toc390176226)

[Заключение 15](#_Toc390176227)

[1. Общая оценка работы 15](#_Toc390176228)

[2. Полнота решения поставленных задач 3. Экономическая и научная значимость работы 15](#_Toc390176229)

[Список использованных источников 16](#_Toc390176230)

[Приложения 17](#_Toc390176231)

# Введение

Информация обладает огромной ценностью в современном мире. С продолжающимся переносом всей информации в электронный вид, все большую значимость обретают методы защиты информации. Однако, настоящая сложность в защите информации возникает именно во время ее передачи, а не во время хранения. Сложность конфиденциальной передачи информации обусловлена высоким уровнем развития информационных технологий – практически все, что попадает в “сеть” становится общедоступным вне зависимости от того Internet это или локальная сеть. Более того, одной конфиденциальностью ограничиться нельзя. Аутентичность (уверенность в том, что полученная информация не была кем-либо изменена во время передачи) играет не менее важную роль в таких типах информации, как, например, банковские транзакции. Так, например, общедоступность информации о конкретной банковской транзакции может не представлять прямую угрозу банковскому счету (или счетам) который в них замешан, но она вредит анонимности (всем заинтересованным становится известно какие операции и в каком объеме были проведены). С другой стороны, подмена информации о транзакции грозит внезапным опустошением счета. Передача паролей (будь то от банковского аккаунта или любого другого вида сетевой идентификации) в незашифрованном виде – напротив, грозит потерей этого аккаунта и попаданием его в руки злоумышленника.

Целью этой работы является применение уже известных технологий шифрования и аутентификации для создания защищенного протокола обмена любыми данными через незащищенный канал. Самым простым примером незащищенного канала является всемирная сеть Internet: пока сигнал (или “пакет”) путешествует от компьютера источника к компьютеру получателя он проходит десятки а иногда и сотни других узлов. Столь обширная сеть не позволяет соединить каждый ее узел напрямую с каждым другим (даже если бы это было возможно, не было бы гарантий отсутствия подслушивающих или изменяющих данные устройств на самих соединяющих магистралях), поэтому защиту приходится обеспечивать другими (не физическими) средствами. То, что среда является незащищенной (или даже “общедоступной”), принято как данность. Таким образом, единственным способом защиты является шифрование (обеспечивающее конфиденциальность) и использование цифровых подписей (обеспечивающих неизменность) перед передачей. Такой подход не лишен своих трудностей. Например, совсем не очевидной является задача отправки первоочередного ключа по незащищенному каналу (шифрование безопасно лишь на столько, на сколько сложно узнать используемый ключ). Незащищенная передача первоочередного ключа является самой критичной и сложной задачей во всей схеме шифрования. Однако, и эта задача была в конце концов решена несколькими способами, что и привело к появлению таких систем безопасности как GNUPG и TLS. В данной работе использованы уже зарекомендовавшие себя алгоритмы – протокол построен из уже проверенных “блоков”. Также, с учетом постоянного увеличения вычислительных мощностей, новый протокол должен быть достаточно расширяемым, чтобы не терять актуальность. Другим немаловажным фактором является невозможность использования “закрытых” решений (с закрытым исходным кодом). При использовании такого решения невозможно получить гарантии отсутствия нежелательных механизмов (шифрование является бессмысленным, если программа, защищающая данные, перед этим отправляет их данные кому-то другому).

# Глава 1: Описание предметной области

## 1.1. Анализ состояния разрабатываемого вопроса

Вопрос защиты информации в общем и шифрования в частности является очень популярным в наше время из-за высокой ценности информации в современном мире. Огромное количество людей вовлечено в разработку новых решений и улучшение уже имеющихся. Это обусловлено тем, что вопрос защиты информации одинаково важен как для больших компаний, которым требуется защита важной информации, так и для отдельных людей, беспокоящихся за конфиденциальность своих личных данных. Существует огромное множество различных алгоритмов и групп алгоритмов нацеленных на самые разные задачи. Используемые в данный момент алгоритмы (считающиеся достаточно защищенными) являются результатом многолетнего опыта (в основном опыта полученного путем проб и ошибок). Нужно помнить, что есть большая разница между алгоритмами, защищенными теоретически и безопасными на практике. Так, алгоритм, называемый One Time Pad считается единственным ***абсолютно защищенным*** (его взлом не просто является вычислительно маловероятным, а невозможным в принципе) в теории, но его применение на практике ограничено. One Time Pad имеет 3 основных принципа:

* Ключ имеет ту же длину, что и исходный текст.
* Ключ (и его части) никогда не используется повторно.
* Ключ является “абсолютно случайным” (энтропия из которой он получен является настолько же длинной как и сам ключ).

В качестве шифрования может применяться простая операция XOR (исключающее логическое ИЛИ). Принимая во внимание вышеперечисленные принципы можно заметить, что у атакующего нет способов проверить правильно ли расшифрован фрагмент текста (так как ключ никогда не используется повторно), что и делает алгоритм полностью защищенным. Однако, применение (полностью верная реализация) этого алгоритма на практике практически невозможна по следующим причинам:

* Настоящие случайные числа (в отличие от псевдослучайных, которые можно получить легко и в больших количествах) очень сложно создать. Учитывая, что нам нужно создать ключ длиной исходного текста, задача становится трудновыполнимой уже на этом этапе.
* Алгоритм не описывает процесс передачи самого ключа с одного конца передачи данных на другой. Если существует безопасный механизм передачи ключа (длиной исходного текста) на другую сторону, то с таким же успехом можно было передать и сам текст. Шифрование в таком случае теряет смысл.
* Отказ от одного из свойств (отсутствия повторного использования ключа или использования настоящих случайных чисел) с целью облегчения реализации резко ухудшает качество шифрования, что, в добавление к полному отсутствию аутентификации, делает применение One Time Pad на практике очень сложным если не невозможным.

Пример с One Time Pad показывает, что при выборе алгоритмов нужно принимать во внимание не только их теоретические характеристики, но и реальную возможность их реализации.

Далее мы рассмотрим алгоритмы, которые получили успешное применение на практике: **RSA**, **Rijndael** (далее AES), **Diffie-Hellman** (далее DH).

## 1.2. Исследование существующих методов шифрования, их достоинств и недостатков

## 1.3. Выводы по результатам проработки предметной области

Мы рассмотрели все основные успешные на данный момент алгоритмы шифрования, обмена ключами и цифровых подписей. Рассмотренные алгоритмы решают все основные проблемы реализации шифрования (передача ключа по незащищенному каналу, обеспечение аутентичности, повышение скорости после установления первоочередного “рукопожатия”). В выборе из двух алгоритмов обмена ключами (RSA против DH) более логичным выбором будет DH из-за более высокой скорости генерации ключей (при условии повторного использования некоторых параметров). Это помогает достичь *совершенной прямой секретности* (свойство алгоритма обмена ключами, которое гарантирует, что сессионные ключи, полученные при помощи набора ключей долговременного пользования, не будут скомпрометированы при компрометации одного из долговременных ключей) с использованием меньшей вычислительной мощности. Выбор AES для симметричного шифрования обусловлен достаточно высокой скоростью шифрования в сочетании с очень хорошей устойчивостью к взлому. Также, для алгоритма симметричной цифровой подписи был выбран SHA256, так как этот алгоритм хеширования является одобренным для применения в криптографических целях (для однонаправленной хеш-функции это значит, что не существует метода нахождения двух входных сообщений с одинаковой хеш-суммой более быстрого, чем перебор всех возможных входных сообщений).

Причины, описанные выше, являются лишь поверхностными описаниями. Более подробная информация доступна в следующей главе.

# Глава 2: Описание нового протокола

## 2.1. Описание новых методов шифрования и защиты данных

## 2.2. Создание нового протокола

## 2.3. Анализ нового протокола с учетом известных атак на существующие системы

# Глава 3: Разработка серверного приложения

## 3.1. Описание будущего проекта

## 3.2. Создание серверного приложения, описание дизайна

## 3.3. Оценка получившегося решения

# Заключение

## 1. Общая оценка работы

## 2. Полнота решения поставленных задач 3. Экономическая и научная значимость работы

# Список использованных источников

# Приложения