ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВО УрГУПС)

Отдел докторантуры и аспирантуры
Кафедра «Информационные технологии и защита информации»
Направление подготовки 10.04.01 «Информационная безопасность»
Направленность: «Информационная безопасность»

Допускается к защите
И.о. зав. кафедрой Зырянова Т.Ю.
канд. техн. наук
_____
«21» июня 2017г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
в виде магистерской диссертации
Тема: «Моделирование симметричного алгоритма передачи сообщений»

10.04.01.05.ВКР.ИБм-215.ПЗ
(обозначение документа)

Разработал студент ИБм-215 20.06.17 Марченко А.В.
(студент-дипломник) (группа) (подпись) (дата) (ф.,и.,о.)
Руководитель доцент, к.т.н. 20.06.17 Волынская А.В.
(должность, звание) (подпись) (дата) (ф.,и.,о.)
Нормоконтролер: к.т.н. 21.06.17 Зырянова Т.Ю.
(должность, звание) (подпись) (дата) (ф.,и.,о.)

Рецензент: начальник секретного отделения военного комиссариата Октябрьского и Ленинского районов города Екатеринбург Свердловской области 19.06.17 Лямина А.М.
(должность, звание) (подпись) (дата) (ф.,и.,о.)

Екатеринбург
2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВО УрГУПС)

Отдел докторантуры и аспирантуры
Кафедра «Информационные технологии и защита информации»
Направление подготовки «Информационная безопасность»

УТВЕРЖДАЮ:
и. о. заведующего кафедрой
Зырянова Татьяна Юрьевна
«14» июня 2017г.

Задание

на выпускную квалификационную работу обучающемуся

Марченко Александру Владимировичу
(Фамилия Имя Отчество)

1. Тема ВКР Моделирование симметричного алгоритма передачи сообщений
утверждена приказом по университету от «14» июня 2017г. № 1303-со
2. Срок сдачи обучающимся законченного ВКР 21.06.2017
3. Исходные данные к ВКР материалы, справочная, научная, методическая литература, справочные материалы и книги по программированию
4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов)
Исследование методов работы симметричных алгоритмов шифрования, моделирование с помощью языков программирования, анализ нормативно-правовых и нормативно-методических документов в области организационного регулирования применения криптографических средств защиты информации
5. Перечень демонстрационно–графического материала (с точным указанием обязательных чертежей и другого наглядного материала)
шифр Вернама, сравнение используемых сред программирования, процесс моделирования на выбранных языках программирования, анализ преимуществ и недостатков, используемых методов моделирования

КАЛЕНДАРНЫЙ ПЛАН-ГРАФИК

№ п/п	Наименование этапов ВКР	Срок выполнения этапов ВКР	Примечание
1.	Изучение существующих методов симметричного шифрования со-общений и принципа их работы.	29 - 31. 05. 2017	
2.	Проведение сравнительного анализа существующих методов симметричного шифрования сообщений и их возможностей.	01 - 04. 06. 2017	
3.	Изучение методов моделирования симметричного алгоритма пере-дачи сообщений с помощью современных объектно-ориентированных языков программирования.	05-08. 06. 2017	
4.	Разработка программного обеспечения с пользовательским интерфейсом на объектно-ориентированных языках программирования, для наглядного моделирования работы симметричного алгоритма шифрования сообщения.	09-15. 06. 2017	
5.	Выбор более удобного и практичного метода моделирования с помощью объектно-ориентированных языков программирования. Описание процесса моделирования и функционала программного обеспечения.	16 - 18. 06. 2017	
7.	Оформление пояснительной записки и графических материалов	19 20. 06. 2017	

Дата выдачи задания, руководитель

20.06.17 Волченская А.В.

(дата, подпись ФИО)

Задание принял к исполнению обучающийся

20. 06. 17 Морозов Д.В.

(дата, подпись ФИО)

СОДЕРЖАНИЕ

РЕФЕРАТ

Магистерская диссертация: 69 с., 21 рис., 2 табл., 12 источников, 3 приложения.

МОДЕЛИРОВАНИЕ, СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, КРИПТОГРАФИЯ, ПЕРЕДАЧА ЗАШИФРОВАННОГО СООБЩЕНИЯ.

Объектом исследования являются симметричные алгоритмы передачи информации.

Цель работы – моделирование работы симметричного алгоритма передачи сообщений, с помощью разработанного программного обеспечения.

В процессе работы были исследованы существующие симметричные алгоритмы передачи сообщений и различные методы моделирования с применением современных языков программирования.

В результате исследования, промоделирован один из симметричных алгоритмов передачи сообщений. Разработано программное обеспечение с помощью двух современных объектно-ориентированных языков программирования. Описан процесс моделирования, с использованием пользовательского интерфейса разработанного программного обеспечения.

ESSAY

Master's thesis: 69 with., 21 fig., 2 table, 12 sources, 3 applications. SIMULATION, SYMMETRIC ALGORITHMS OF ENCRYPTION, SOFTWARE, CRYPTOGRAPHY, TRANSMISSION OF THE ENCRYPTED MESSAGE.

The object of research are symmetrical algorithms of information transmission. The aim of the work is to simulate the operation of a symmetric message transfer algorithm, using the developed software.

In the process of work, existing symmetric algorithms of message transmission and various modeling methods using modern programming languages were investigated.

As a result of the study, one of the symmetric algorithms of message transmission is modeled. The software is developed using two modern object-oriented programming languages. The modeling process is described using the user interface of the developed software.

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВО УрГУПС)

ОТЗЫВ

о выпускной квалификационной работе студента факультета *Докторантуры и аспирантуры*

(Наименование)

Направление подготовки (специальности) *10.04.01 «Информационная безопасность»*

(Код, наименование)

Марченко А.В.

(Фамилия, имя, отчество)

Руководитель *к.т.н., доцент кафедры «ИТ и ЗИ» Волынская А.В.*

(Ученая степень, ученое звание, должность, Фамилия, имя, отчество)

Тема работы «Моделирование симметричного алгоритма передачи сообщений».

В ходе работы исследованы существующие симметричные алгоритмы передачи сообщений и различные методы моделирования с применением современных языков программирования. В результате исследования смоделирован один из симметричных алгоритмов передачи сообщений. Разработано программное обеспечение с помощью двух современных объектно-ориентированных языков программирования. Описан процесс моделирования с использованием пользовательского интерфейса разработанного программного обеспечения.

Цель и задачи ВКР четко сформулированы, представленная в ВКР информация систематизирована и структурирована. В изложении содержания ВКР присутствует логика. Приведен подробный анализ альтернативных вариантов решения исследовательских задач.

Список использованных источников достаточно объемен, систематизирован, отражает тематику всех разделов ВКР. Расстановка ссылок на использованные источники в тексте ВКР соответствует содержанию. Знания и умения, полученные из использованных источников, отражены в тексте ВКР.

Представлено авторское решение задачи, продемонстрирован творческий подход. В ВКР обоснованно и правильно применяются математические методы исследования защищенности объектов. Автор демонстрирует глубокое понимание физических эффектов и явлений, используемых для обеспечения информационной безопасности, применяет профессиональные программные средства для обработки результатов эксперимента. Результаты экспериментов, проведенных в ходе работы над ВКР, обработаны с применением профессиональных программных средств.

В ВКР приведен раздел, содержащий разработку учебно-методических рекомендаций по тематике исследования (разработаны тестовые материалы).

Результаты, полученные в ходе работы над ВКР, обоснованы, тема раскрыта полностью. Студент показал высокий уровень владения теоретическим

материалом, необходимыми для магистра по защите информации умениями и навыками.

В процессе работы студент проявил себя способным самостоятельно решать поставленные задачи, грамотно планировать ход выполняемых работ, работать с литературой и нормативно-техническими документами.

Оформление работы соответствует требованиям «Положения об итоговой государственной аттестации» и Стандарта «Дипломное проектирование» системы менеджмента качества УрГУПС.

Считаю, что выпускная квалификационная работа Марченко А.В. может быть представлена к защите. Рекомендуемая оценка – «отлично».

22.06.17

А.В. Волынская

РЕЦЕНЗИЯ

На выпускную квалификационную работу (ВКР)

по теме Моделирование симметричного алгоритма передачи сообщений
обучающегося Марченко Александра Владимировича, гр. ИБм-215
(Ф.И.О., группа)

ВКР объемом 69 страниц, содержит таблиц 2 иллюстраций 21, источников 12 приложений 3.

ВКР посвящена моделированию и наглядному отображению работы
(актуальность и социальная значимость темы)
симметричного алгоритма передачи сообщений с помощью современных языков программирования

Основные результаты исследованы наиболее защищенные симметричные алгоритмы передачи сообщений, разработано программное обеспечение, позволяющее промоделировать работу симметричного шифра

Новизна и оригинальность идей, положенных в основу ВКР, а также методы его выполнения программное обеспечение, способное промоделировать работу симметричного шифра, разработано с помощью современных языков программирования

Практическая значимость ВКР разработанное программное обеспечение можно применять для наглядного отображения работы симметричных алгоритмов передачи сообщений
(возможность внедрения результатов проекта (работы) в практику, ожидаемый эффект)

Анализ обоснованности выводов и предложений выводы аргументированы и обоснованы актуальностью и новизной разработанного программного обеспечения

Качество оформления работы соответствует требованиям к оформлению дипломных работ

Недостатки ВКР особо значимых недостатков в работе не обнаружено

Изложенное позволяет считать, что рецензируемая ВКР отвечает установленным требованиям, предъявляемым к дипломным работам и заслуживает оценки «хорошо»

Дата 19.06.17 Рецензент Лямина А.М. Подпись
(Фамилия И.О.)

МИНИСТЕРСТВО ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
ВОЕННЫЙ КОМИССАРИАТ СВЕРДЛОВСКОЙ ОБЛАСТИ
29