ТИТУЛЬНЫЙ ЛИСТ

## РЕФЕРАТ

Выпускная квалификационная работа бакалавра состоит из 00 страниц, 00 рисунков, 00 таблиц, 00 использованных источников, 00 приложений.

РАСПРЕДЕЛЕННАЯ СИСТЕМА КРИПТОГРАЧИСЕКОЙ ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Целью данной работы является исследование применения криптографических алгоритмов шифрования на основе эллиптических кривых для защиты данных и реализация распределенной системы криптографической защиты данных с использованием разработанных инструментов для работы с эллиптическим кривыми. Были использованы материалы о существующих алгоритмах шифрования и о применении этих алгоритмов в существующих системах, использующих эти криптографические алгоритмы для шифрования и дальнейшего хранения данных. Для реализации был использован язык программирования C#, фреймворки ASP.NET и WPF. В результате было разработана библиотека исходного кода для работы с эллиптическими кривыми и клиент-серверное приложение мессенджера, состоящее из распределенной системы, использующей алгоритм шифрования на основе эллиптических кривых для защиты данных пользователей, и приложения для персональных компьютеров для взаимодействия с распределенной системой. Разработанное приложение может использоваться для обеспечения безопасности общения и хранения данных компаний.

**СОДЕРЖАНИЕ**

[ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 4](#_Toc127449243)

[ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ 5](#_Toc127449244)

[ВВЕДЕНИЕ 6](#_Toc127449245)

[1 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ 7](#_Toc127449246)

[1.1 Алгоритмы шифрования 7](#_Toc127449247)

[1.2 Название подраздела 7](#_Toc127449248)

[1.3 Название подраздела 7](#_Toc127449249)

[2 НАЗВАНИЕ РАЗДЕЛА 8](#_Toc127449250)

[2.1 Название подраздела 8](#_Toc127449251)

[2.2 Название подраздела 8](#_Toc127449252)

[2.3 Название подраздела 8](#_Toc127449253)

[ЗАКЛЮЧЕНИЕ 9](#_Toc127449254)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 10](#_Toc127449255)

[ПРИЛОЖЕНИЕ А Наименование приложения 11](#_Toc127449256)

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящей выпускной квалификационной работе бакалавра применяют следующие термины с соответствующими определениями:

|  |  |
| --- | --- |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |
| Термин | - определение |

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В настоящей выпускной квалификационной работе бакалавра применяют следующие сокращения и обозначения:

|  |  |
| --- | --- |
| Обозначение | - детальная расшифровка |
| Обозначение | - детальная расшифровка |
| Обозначение | - детальная расшифровка |
| Обозначение | - детальная расшифровка |
| Обозначение | - детальная расшифровка |
| Обозначение | - детальная расшифровка |
| Обозначение | - детальная расшифровка |
| Обозначение | - детальная расшифровка |
| Обозначение | - детальная расшифровка |
| Обозначение | - детальная расшифровка |
| Обозначение | - детальная расшифровка |
| Обозначение | - детальная расшифровка |

## ВВЕДЕНИЕ

В современном мире, охватывающем все больше сфер деятельности, данные играют все более важную роль. Времена, когда данные были лишь вспомогательным инструментом для принятия решений, давно прошли. Сегодня они стали неотъемлемой частью многих сфер деятельности, таких как экономика, медицина, наука, технологии и многие другие. Важность данных заключается не только в их количестве, но и в качестве, в их интерпретации и использовании. Данные имеют огромное значение, потому что они могут дать нам важную информацию о нашем мире, помочь нам принимать решения, оптимизировать процессы и увеличивать эффективность наших действий.

Данные используются в различных сферах деятельности, таких как экономика, медицина, наука, технологии, государственное управление, и многие другие. В современном мире существует огромное количество данных, их обработка и интерпретация требуют высококвалифицированных специалистов и современных технологий. Правильно обработанные данные могут помочь нам принимать более обоснованные решения, оптимизировать бизнес-процессы, повышать эффективность производственных и научных процессов, а также создавать новые продукты и услуги.

Несмотря на значимость данных в нашей жизни, существуют также определенные ограничения и проблемы, связанные с их использованием. Одна из главных проблем заключается в защите данных и приватности. С постоянным увеличением объема данных и их значимости, возрастает их уязвимость, и проблема безопасности данных становится все более актуальной.

Данные могут быть украдены, изменены или уничтожены злоумышленниками, что может привести к серьезным последствиям, включая финансовые потери, утечку конфиденциальной информации и нарушение прав человека. Поэтому безопасность данных становится ключевой проблемой, требующей серьезного внимания и многогранного подхода.

Цель данной работы заключается в изучении проблемы безопасности данных в современном мире и анализе методов защиты данных. В работе будут рассмотрены основные угрозы безопасности данных, такие как хакерские атаки, вирусы и вредоносные программы, утечки данных и социальная инженерия. Будут проанализированы методы защиты данных, включая криптографию, биометрические технологии и системы защиты периметра.

Изучение проблемы безопасности данных имеет большое значение, так как поможет повысить эффективность защиты данных и предотвратить возможные угрозы. Результаты данной работы могут быть использованы как в бизнес-сфере, так и в государственном управлении для обеспечения безопасности и конфиденциальности данных.

## 1 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.1 Название подраздела

* 1. Название подраздела
     1. Название пункта
     2. Название пункта
     3. Название пункта

1.3 Название подраздела

## 2 ПРАКТИЧЕСКАЯ ЧАСТЬ

2.1 Алгоритмы шифрования

2.1.1 Виды криптографических алгоритмов шифрования

2.1.1 Название пункта

2.1.2 Название пункта

2.2 Название подраздела

2.3 Название подраздела

2.3.1 Название пункта

2.3.2 Название пункта

## ЗАКЛЮЧЕНИЕ

Заключение должно содержать:

* краткие выводы по результатам выполненной работы или отдельных ее этапов;
* оценку полноты решений поставленных задач;
* разработку рекомендаций и исходных данных по конкретному использованию результатов работы;
* результаты оценки технико-экономической эффективности внедрения;
* результаты оценки научно-технического уровня выполненной работы в сравнении с лучшими достижениями в этой области.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Moos, D., Peska, P. et al. Comprehensive wellbore stability analysis using quantitative risk assessment// Knowledge Organization - 2007 . - Vol. 34, No. 4 . - P. .97–109 .
2. Прогноз научно-технологического развития Российской Федерации на период до 2030 года. - URL: [http://government.ru/media /files/41d4b737638891da2184/pdf](http://government.ru/media%20/files/41d4b737638891da2184/pdf) (дата обращения 15.11.2016).
3. 112. Andy Bradbury, Justin Mclellan, Impact Fluid Solutions Biodegradable shale inhibitor developed for water-based muds, Drilling It Safely, Innovating While Drilling, July/August, Onshore Advances Jul 11. – 2013. - URL: <http://www.nlm.nih.gov/pubs/factsheets/umlsmeta.html>(дата обращения 2013-02-01).
4. Двойников, М.В. Технология бурения нефтяных и газовых скважин модернизированными винтовыми забойными двигателями// Дисс. доктора техн. наук - Тюмень 2011 . – 360 С .
5. Хегай В.К. К вопросу оптимизации режимных параметров бурения с учетом крутильных автоколебаний// Известия Коми НЦ УрО РАН - 2010 . - № 07-08. - С. 6 - 10 .
6. Гуреев В.Н., Мазов Н.А. Использование библиометрии для оценки значимости журналов в научных библиотеках (обзор)// Научно-техническая информация. Сер. 1. - 2015 . - N 2. - С. 8 - 19 .
7. Статистические показатели российского книгоиздания в 2006 г.: цифры и рейтинги [Электронный ресурс]. - URL: <http://bookhamber.ru/stat_2006.htm> (дата обращения 12.03.2009).
8. Web of Science. - URL: [http://apps.webofknowledge.com](http://apps.webofknowledge.com/) (дата обращения 15.11.2016).

## ПРИЛОЖЕНИЕ А

**Наименование приложения**

В приложения рекомендуется включать материалы, дополняющие текст отчета, если они не могут быть включены в основную часть.

Приложения могут включать: графический материал, таблицы, расчеты, описания алгоритмов и программ.

В тексте отчета на все приложения должны быть даны ссылки. Приложения располагают в порядке ссылок на них в тексте отчета.

Каждое приложение следует размещать с новой страницы с указанием в центре верхней части страницы слова ПРИЛОЖЕНИЕ.

Приложение должно иметь заголовок, который записывают с прописной буквы, полужирным шрифтом, отдельной строкой по центру без точки в конце.

Приложения обозначают прописными буквами кириллического алфавита, начиная с А, за исключением букв Ё, З, Й, О, Ч, Ъ, Ы, Ь. После слова ПРИЛОЖЕНИЕ следует буква, обозначающая его последовательность. Допускается обозначение приложений буквами латинского алфавита, за исключением букв I и O.

В случае полного использования букв кириллического или латинского алфавита допускается обозначать приложения арабскими цифрами.

Если в отчете одно приложение, оно обозначается ПРИЛОЖЕНИЕ А".

Приложения должны иметь общую с остальной частью отчета сквозную нумерацию страниц.

Все приложения должны быть перечислены в содержании отчета с указанием их обозначений, статуса и наименования.