Министерство образования и науки Российской Федерации
Федерально государственной бюджетное образовательное учреждение
Высшего профессионального образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Инженерная школа ядерных технологий
Направление подготовки 01.04.02 Прикладная математика и информатика
Отделение экспериментальной физики

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Организация шифрования данных на эллиптических кривых для АО ТОМ-ДОМ ТДСК

УДК 004.67.056.55:514.135

Студент

Группа	ФИО	Подпись	Дата
0ВМ01	Адодин Андрей Николаевич		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Крицкий О.Л.	к. ф.-м. н., доцент		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность, ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Клемашева Е.И.	к.э.н.		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Профессор	Федорчук Ю.М.	д.т.н., профессор		

ДОПУСТИТЬ К ЗАЩИТЕ:

Руководитель ООП	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Семенов М.Е.	к. ф.-м. н., доцент		

Томск – 2022 г.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ООП

Код компетенции	Наименование компетенции
УК(У)-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
УК(У)-2	Способен управлять проектом на всех этапах его жизненного цикла
УК(У)-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
УК(У)-4	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
УК(У)-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
УК(У)-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки
ОПК(У)-1	Способен решать актуальные задачи фундаментальной и прикладной математики
ОПК(У)-2	Способен совершенствовать и реализовывать новые математические методы решения прикладных задач
ОПК(У)-3	Способен разрабатывать математические модели и проводить их анализ при решении задач в области профессиональной деятельности
ОПК(У)-4	Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности
ПК(У)-1	Способен проводить научные исследования и получать новые научные и прикладные результаты самостоятельно и в составе научного коллектива
ПК(У)-2	Способен проводить поиск и анализ научной и научно-технической литературы по тематике проводимых исследований
ПК(У)-3	Способен разрабатывать и анализировать показатели качества информационных систем, используемых в производственной деятельности
ПК(У)-4	Способен планировать научно-исследовательскую деятельность, анализировать риски, управлять проектами, управлять командой проекта
ПК(У)-5	Способен к преподаванию математических дисциплин и информатики в образовательных организациях высшего образования
ПК(У)-6	Способен проектировать и организовывать учебный процесс по образовательным программам с использованием современных образовательных технологий

Министерство образования и науки Российской Федерации
Федерально государственной бюджетное образовательное учреждение
Высшего профессионального образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Инженерная школа ядерных технологий
Направление подготовки 01.04.02 Прикладная математика и информатика
Отделение экспериментальной физики

УТВЕРЖДАЮ:
Руководитель ООП
_____ _____ Семенов М. Е.
(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

Магистерской диссертации

Студенту:

Группа	**ФИО**
0ВМ01	Адодину Андрею Николаевичу

Тема работы:

Организация шифрования данных на эллиптических кривых для АО ТОМ-ДОМ ТДСК	
Утверждена приказом директора (дата, номер)	17.02.2022 №48-21/с

Срок сдачи студентом выполненной работы:	

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе *(наименование объекта исследования или проектирования; производительность или нагрузка; режим работы (непрерывный, периодический, циклический и т.д.); вид сырья или материала изделия; требования к продукту, изделию или процессу; особые требования к особенностям функционирования (эксплуатации) объекта или изделия в плане безопасности эксплуатации, влияния на окружающую среду, энергозатратам; экономический анализ и т.д.)*	Международные стандарты и стандарты РФ для цифровых подписей, а также прочие достоверные источники, содержащие информацию о шифрование данных с помощью метода эллиптических кривых
Перечень подлежащих исследованию, проектированию и разработке вопросов *(с точным указанием обязательных чертежей)*	1. Провести теоретический обзор алгоритма шифрования методом ECC. 2. Сделать выбор программной среды для реализации алгоритма и произвести реализацию (создать программу) алгоритма в выбранной среде. 3. Протестировать запрограммированный алгоритм шифрования. 4. Сравнить скорость шифрования данных методом ECC со скоростью шифрования данных методом RSA.
Перечень графического материала	

(с точным указанием обязательных чертежей)	

Консультанты по разделам выпускной квалификационной работы

(с указанием разделов)

Раздел	Консультант
Финансовый менеджмент, ресурсоэффективность, ресурсосбережение	Клемашева Елена Игоревна
Социальная ответственность	Федорчук Юрий Митрофанович
Раздел на иностранном языке	Кабрышева Оксана Павловна

Названия разделов, которые должны быть написаны на русском и иностранном языках:

Введение
Теоретическая часть
Заключение
Список литературы

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	

Задание выдал руководитель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Крицкий О.Л.	к. ф.-м. н., доцент		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
0ВМ01	Адодин Андрей Николаевич		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
0ВМ01	Адодину Андрею Николаевичу

Школа	**ИЯТШ**	**Отделение школы (НОЦ)**	**ОЭФ**
Уровень образования	Магистратура	**Направление/специальность**	01.04.02 Прикладная математика и информатика

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. *Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих* 2. *Нормы и нормативы расходования ресурсов* 3. *Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования*	Работа с информацией, представленной в российских и иностранных научных публикациях, аналитических материалах, статических бюллетенях и изданиях, нормативно-правовых документах.
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. *Оценка коммерческого и инновационного потенциала НТИ*	Анализ потенциальных потребителей результатов исследования. Анализ конкурентных технических решений. SWOT – анализ. Оценка готовности проекта к коммерциализации. Описание методов коммерциализации результатов научно-технического исследования.
2. *Разработка устава научно-технического проекта*	Определение цели и результатов проекта. Формирование организационной структуры проекта.
3. *Планирование процесса управления НТИ: структура и график проведения, бюджет, риски и организация закупок*	Формирование иерархической структуры работ проекта. Разработка календарного плана проекта. Формирование бюджета научного исследования. Выявление рисков проекта.
4. *Определение ресурсной, финансовой, экономической эффективности*	Определение интегральных показателей эффективности.
Перечень графического материала *(с точным указанием обязательных чертежей):*	
1. *«Портрет» потребителя результатов НТИ* 2. *Сегментирование рынка* 3. *Матрица SWOT* 4. *График проведения НТИ*	

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент ОСГН ШБИП	Клемашева Елена Игоревна	канд.экон.наук		01.02.2022

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
0ВМ01	Адодин Андрей Николаевич		01.02.2022

ЗАДАНИЕ ДЛЯ РАЗДЕЛА «СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
0ВМ01	Адодину Андрею Николаевичу

Школа	ИЯТШ	Отделение (НОЦ)	Экспериментальной физики
Уровень образования	Магистратура	Направление/специальность	01.04.02 Прикладная математика и информатика

Тема дипломной работы: «Формирование оптимального портфеля ценных бумаг с учетом применения метода DEA»

Исходные данные к разделу «Социальная ответственность»:	
1. Характеристика объекта исследования (вещество, материал, прибор, алгоритм, методика, рабочая зона) и области его применения	Шифрование текста методом ECC для передачи и хранения текстовых данных. Работа проводилась в 10 корпусе аудитории 427а.
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Производственная безопасность 1.1. Анализ выявленных вредных факторов: • Природа воздействия • Действие на организм человека • Нормы воздействия и нормативные документы (для вредных факторов) • СИЗ коллективные и индивидуальные 1.2. Анализ выявленных опасных факторов: • Термические источники опасности • Электробезопасность • Пожаробезопасность	1. Вредные факторы: 1.1 Недостаточная освещенность; 1.2 Нарушения микроклимата, оптимальные и допустимые параметры; 1.3 Шум, ПДУ, СКЗ, СИЗ; 1.4 Повышенный уровень электромагнитного излучения, ПДУ, СКЗ, СИЗ; 1.5 УФИ, СКЗ, СИЗ; 1.6. ИК излучение, СКЗ, СИЗ; 1.7. Наличие токсикантов, ПДК, класс опасности, СКЗ, СИЗ; 1.8. Ионизирующее излучение, ПДД, критические оргапны, СКЗ, СИЗ; 2. Опасные факторы: 2.1 Электроопасность; класс электроопасности помещения, безопасные номиналы I, U, $R_{заземления}$, СКЗ, СИЗ; Проведен расчет освещения рабочего места; представлен рисунок размещения светильников на потолке с размерами в системе СИ; 2.2 Пожароопасность, категория пожароопасности помещения, марки огнетушителей, их назначение и ограничение применения; Приведена схема эвакуации. 2.3 Лазерное излучение, класс опасности, СКЗ, СИЗ.

2. Экологическая безопасность: • Выбросы в окружающую среду • Решения по обеспечению экологической безопасности	Наличие промышленных отходов (бумага-черновики, вторцвет и чермет, пластмасса, перегоревшие люминесцентные лампы, оргтехника, обрезки монтажных проводов, бракованная строительная продукция) и способы их утилизации.
3. Безопасность в чрезвычайных ситуациях: • Перечень возможных ЧС при разработке и эксплуатации проектируемого решения; • Разработка превентивных мер по предупреждению ЧС; • Разработка действий в результате возникшей ЧС и мер по ликвидации её последствий.	Рассмотрены 2 ситуации ЧС: 1) природная – сильные морозы зимой, (аварии на электро-, тепло-коммуникациях, водоканале, транспорте); 2) техногенная – несанкционированное проникновение посторонних на рабочее место (возможны проявления вандализма, диверсии, промышленного шпионажа), представлены мероприятия по обеспечению устойчивой работы производства в том и другом случае.
4. Перечень нормативно-технической документации.	– ГОСТы, СанПиНы, СНиПы

Дата выдачи задания для раздела по линейному графику	12.03.2022

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Профессор ТПУ	Федорчук Ю.М.	д.т.н.		12.03.2022

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
0ВМ01	Адодин Андрей Николаевич		

Реферат

Выпускная квалификационная работа содержит 97 страниц, 6 рисунков, 21 таблицу, 22 источника, 5 приложений.

Ключевые слова: шифрование данных, эллиптические кривые, шифрование данных с помощью эллиптических кривых, шифрование данных методом ECC.

Объектом исследования является шифрование с помощью эллиптических кривых.

Цель работы – создать программное обеспечение для шифрования данных с помощью эллиптических кривых.

В процессе работы проводились изучение специальной литературы, выбор языка программирования и библиотек для работы программного обеспечения, написание листинга программ, анализ и интерпретация полученных данных.

В результате работы создано программное обеспечение, позволяющее генерировать ключи шифрования и с их помощью проводить шифрование и расшифрование сообщений.

Степень внедрения: высокая.

Область применения: программное обеспечение может быть использовано для передачи информации, если есть подозрение, что данную информацию могут прочитать посторонние лица, а также можно хранить важную информацию в зашифрованном виде.

Экономическая эффективность/значимость работы: применяя полученное программное обеспечение можно шифровать сообщение (текст) с помощью открытого ключа и передавать эту приватную информацию обладателю закрытого ключа.

Оглавление

Введение

Человечество перешло в эру, когда обмен информацией, представляющей собой ценность для злоумышленников (например, такие как денежные транзакции, приватная переписка или обмен корпоративными документами и т.д.) осуществляется с помощью коммуникаций через сеть Интернет.

В связи с этим актуальной и перспективной темой является работа с информацией, а главным приоритетом становится её защита от прочтения посторонними лицами.

Применение криптографии позволяет эффективно решить проблему обмена информацией через открытые сети. Чаще всего обеспечение безопасности осуществляется посредством шифрования, использованием цифровой подписи или аутентификацию паролем.

Криптография – широкая область знаний о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), шифрования (кодировка данных). Современная криптография начала развиваться с 1970х годов.

Криптоалгоритмы делятся на две большие группы: симметричные (когда обе стороны-участники обмена данными имеют абсолютно одинаковые ключи как для шифрования, так и расшифровки данных) и асимметричные (стороны-участники используют в паре два разных ключа — открытый и секретный, который также называют закрытым).

Широкое распространение получили асимметричные алгоритмы (с открытым ключом), поскольку нет необходимости решения сложнейшей задачи обмена секретными ключами. Одним из известных и распространенным алгоритмов асимметричного шифрования является алгоритм ECC (с помощью эллиптических кривых).

Алгоритм шифрования ECC часто используется для шифрования паролей симметричным алгоритмам. Он очень редко используется для шифрования текстов в связи с тем, что может шифровать только сообщения, которые меньше, чем сам ключ.

Цель данной работы: создание программного обеспечения для шифрования данных с использование алгоритма ECC (эллиптических кривых).

Для достижения поставленной цели необходимо выполнить следующие задачи:

- провести теоретический обзор алгоритма шифрования;
- сделать выбор программной среды для реализации алгоритма;
- произвести реализацию алгоритма в выбранной среде;
- протестировать запрограммированный алгоритм шифрования.
- сравнить данный метод шифрования с более известным RSA.

Обзор литературы

Для выполнения выпускной квалификационной работы была изучена литература, которая включает в себя книги, статьи, а также интернет-ресурсы.

В данной работе в начале рассказывается о криптографии и даются основные термины, изложенные из источников [1] и [2]. Дается понятие о симметричных и асимметричных способах шифрования. Более подробно об асимметричном методе шифрования мы узнаем в источнике [3].

Одним из самых распространенных способов шифрования данных с помощью открытого и закрытого ключа является метод с использование эллиптических кривых, математические формулы которых мы можем посмотреть в сжатой информации из источника [4]. Эллиптическая кривая — это набор точек, описывающихся уравнением Вейерштрассе. Более подробное математическое описание полей эллиптических кривых мы можем посмотреть в источнике [5].

Поскольку шифрование данных предназначено для сокрытия важной информации от посторонних, необходимо также уделять внимание информационной безопасности. Основы которой описаны в источнике [6], а также рассматривается сильные и слабые стороны асимметричного шифрования.

1 Теоретическая часть

1.1 Криптографические системы

Проблемой защиты информации путем ее преобразования занимается криптология. Криптология разделяется на два направления - криптографию и криптоанализ. Криптография занимается поиском и исследованием методов преобразования информации с целью скрытия ее содержания. Сфера интересов криптоанализа – исследование возможности расшифровывания информации без знания ключей.

Основные направления использования криптографических методов: передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации документов, баз данных) на носителях в зашифрованном виде.

Итак, криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

Зашифрование – процесс криптографического преобразования множества открытых сообщений в множество закрытых сообщений.

Расшифрование – процесс криптографического преобразования закрытых сообщений в открытые.

Дешифрование – процесс нахождения открытого сообщения, соответствующего заданному закрытому при неизвестном криптографическом преобразовании.

Шифрование – средство достижения секретности информации, состоящее из двух этапов: зашифрования и расшифрования исходных данных.

Закрытый ключ – это секретная информация, требуемая для расшифровки сообщений.

Открытый ключ – это открытая информация, требуемая для шифрования сообщений, результат шифрования и криптостойкость зависит от длины ключа [1].

Криптографическая система представляет собой семейство $\boldsymbol{T}$ преобразований открытого текста. Члены этого семейства индексируются, или обозначаются символом k; параметр k обычно называется ключом.

Преобразование T_k определяется соответствующим алгоритмом и значением ключа k.

Ключ - информация, необходимая для беспрепятственного шифрования и расшифрования текстов.

Пространство ключей $\boldsymbol{K}$ – это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы подразделяются на симметричные и асимметричные (или с открытым ключом).

В симметричных криптосистемах для шифрования, и для расшифрования используется один и тот же ключ.

В системах с открытым ключом используются два ключа - открытый и закрытый (секретный), которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения [2].

1.2 Асимметричные криптосистемы

Асимметричные системы характеризуются тем, что для шифрования и для расшифрования используются разные ключи, связанные между собой некоторой зависимостью. При этом данная зависимость такова, что установить один ключ, зная другой, с вычислительной точки зрения очень трудно.

Один из ключей (например, ключ шифрования) может быть сделан общедоступным, и в этом случае проблема получения общего секретного ключа

для связи отпадает. Если сделать общедоступным ключ расшифрования, то на базе полученной системы можно построить систему аутентификации передаваемых сообщений. Поскольку в большинстве случаев один ключ из пары делается общедоступным, такие системы получили также название криптосистем с открытым ключом.

Криптосистема с открытым ключом определяется тремя алгоритмами: генерации ключей, шифрования и расшифрования. Алгоритм генерации ключей открыт, всякий может подать ему на вход случайную строку r надлежащей длины и получить пару ключей $(k_1,\ k_2)$. Один из ключей (например, k_1) публикуется, он называется открытым, а второй, называемый секретным, хранится в тайне. Алгоритмы шифрования E_{k_1} и расшифрования D_{k_2} таковы, что для любого открытого текста m $D_{k_2}\ (E_{k_1}\ (m)) = m$. [3]

1.3 Эллиптические кривые

Эллиптическая кривая — это набор точек, описывающихся уравнением Вейерштрассе:

$$y^2 = x^3 + ax + b.$$

Примеры графиков эллиптических кривых:

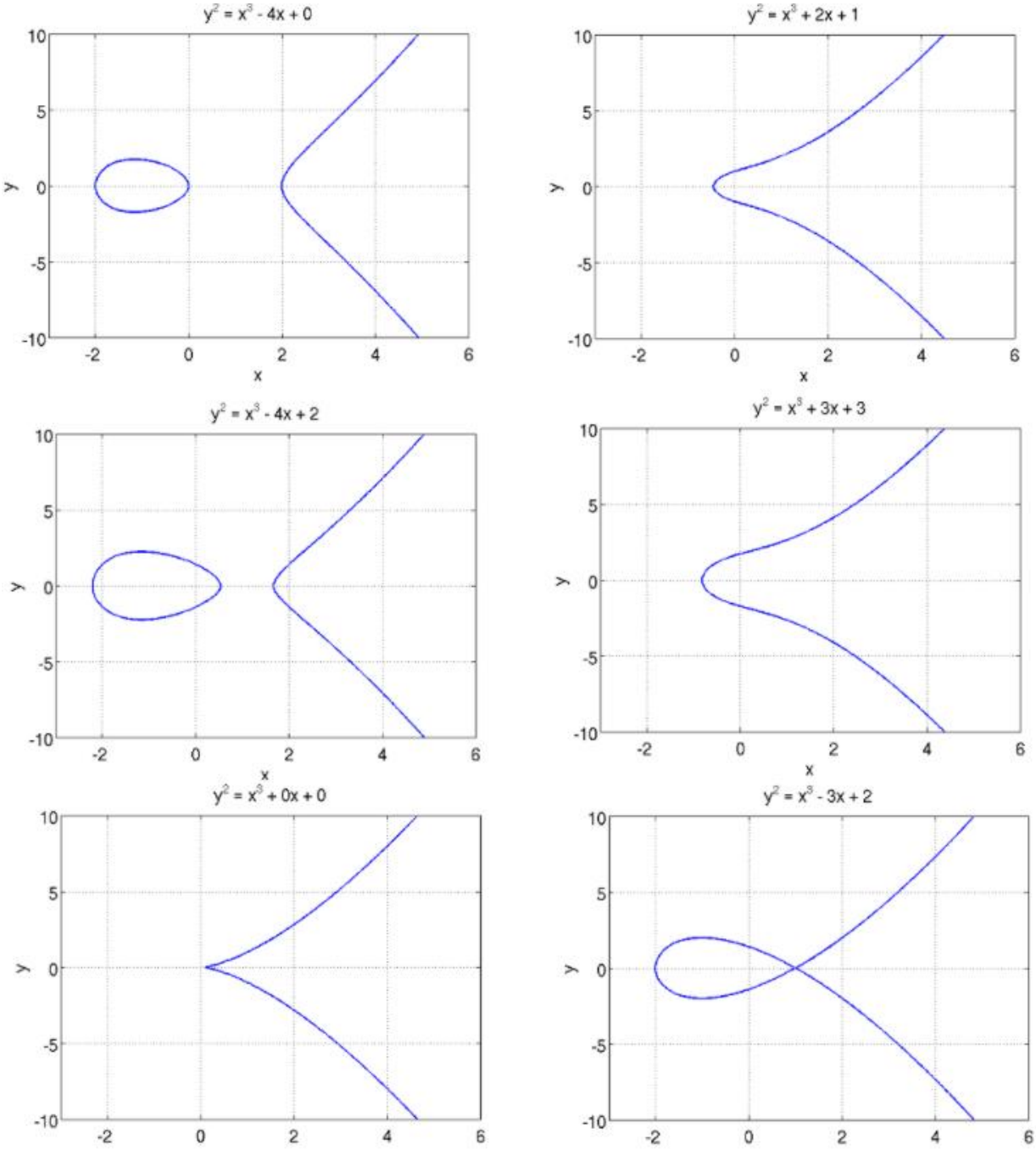

Рисунок 1 – Примеры графиков эллиптических кривых

Эллиптические кривые, представленные на первых четырех графиках, называются гладкими, две нижние кривые относятся к так называемым сингулярным эллиптическим кривым. Для гладких эллиптических кривых выполняется следующее неравенство:

$$4a^3 + 27b^2 \neq 0$$

Тогда как для сингулярных кривых это условие не выполняется.

Нельзя использовать в схемах ЭЦП сингулярные кривые, так как, используя сингулярные кривые, можно значительно снизить стойкость схемы ЭЦП.

Арифметические операции в эллиптической криптографии производятся над точками кривой. Основной операцией является «сложение». Сложение двух точек легко представить графически:

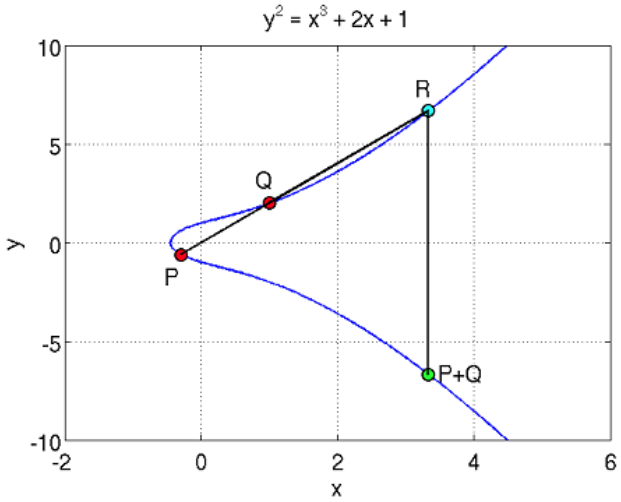

Рисунок 2 – Сложение двух точек в эллиптической криптографии

Как видно из рисунка, для сложения точек P и Q, необходимо провести между ними прямую линию, которая обязательно пересечет кривую в какой-либо третьей точке R. Отразим точку R относительно горизонтальной оси координат и получим искомую точку P+Q.

Алгебраическое представление Сложение задаётся следующим правилом: сумма трёх ненулевых точек P, Q и R, лежащих на одной прямой, будет равна P + Q + R = 0.

Запишем сложение двух точек в виде формулы:

$$P + Q = -R.$$

Пусть координатами точки P будут (X_P, Y_P), а координатами точки Q соответственно (X_Q, Y_Q).

Вычислим

$$\alpha = \frac{Y_Q - Y_P}{X_Q - X_P}$$

и тогда [4] координаты точки P + Q будут равны:

$$X_{P+Q} = \alpha^2 - X_P - X_Q$$

$$Y_{P+Q} = -Y_P + \alpha(X_P - X_R).$$

1.4 Эллиптические кривые в криптографии

Все рассмотренные выше кривые относятся к эллиптическим кривым над вещественными числами. И это приводит к проблеме округления. То есть, используя кривые над вещественными числами, мы не сможем получить биекцию между исходным текстом и зашифрованными данными. Чтобы не округлять, в криптографии используются только кривые над конечными полями. Это означает, что под эллиптической кривой понимается набор точек, чьи координаты принадлежат конечному полю.

В криптографии рассматривается два вида эллиптических кривых: над конечным полем Z_p – кольцо вычетов по модулю простого числа. И над полем $GF(2^m)$ бинарное конечное поле. У эллиптических кривых над полем $GF(2^m)$ есть одно важное преимущество: элементы поля $GF(2^m)$ могут быть легко представлены в виде n-битных кодовых слов, это позволяет увеличить скорость аппаратной реализации эллиптических алгоритмов.

Все математические операции на эллиптических кривых над конечным полем производятся по законам «конечного поля», над которым построена эллиптическая кривая. То есть для вычисления, например, суммы двух точек

кривой E над кольцом вычетов Z_p все операции производятся по модулю числа p.

Однако, если сложить два одинаковых элемента из бинарного конечного поля, то получим в результате 0, т.к. сложение происходит по модулю 2. Это означает что характеристика такого поля равна 2. Но эллиптическая кривая вида

$$y^2 = x^3 + ax + b,$$

описанная над полем характеристики 2 или 3 становится сингулярной, а как уже замечалось выше, использовать сингулярные кривые в криптографии нельзя.

Поэтому над бинарным конечным полем используются кривые вида:

$$y^2 + xy = x^3 + ax^2 + b,\ b \neq 0.$$

Еще одним важным понятием эллиптической криптографии является порядок эллиптической кривой, который показывает количество точек кривой над конечным полем.

Теорема Хассе утверждает, что если N — количество точек кривой, определенной над полем Z_q с q элементами тогда справедливо равенство:

$$|N - (q + 1)| \leq 2\sqrt{q}.$$

Так как бинарное конечное поле $GF(2^n)$ состоит из 2^n элементов мы можем сказать, что порядок кривой $E_{2^n}(a, b)$ равен $2^n + 1 - t$, где $|t| \leq \sqrt{2^n}$.

С числом t связано следующее определение: эллиптическая кривая над бинарным конечным полем называется суперсингулярной, если t делится на характеристику поле (в случае бинарного поля характеристика равна 2) без остатка [5].

1.5 Криптография на эллиптических кривых

Точки эллиптической кривой над конечным полем представляют собой группу. И как уже отмечалось выше, для этой группы определена операция сложения. Соответственно мы можем представить умножение числа k на точку G как G+G+…+G с k слагаемыми.

Предположим, что имеется сообщение M, представленное в виде целого числа. Можно зашифровать его используя выражение C=M*G. Вопрос в том, насколько сложно восстановить M зная параметры кривой E(a,b), шифротекст C и точку G. Данная задача называется дискретным логарифмом на эллиптической кривой и не имеет быстрого решения. Более того, считается, что задача дискретного логарифма на эллиптической кривой является более трудной для решения, чем задача дискретного логарифмирования в конечных полях.

Наиболее быстрые методы, разработанные для конечных полей, оказываются бесполезны в случае эллиптических кривых. Так для решения дискретного логарифма существуют достаточно быстрые алгоритмы, имеющие сложность $O(\exp(c(logP\ log\ log\ P)^d))$, где c и d — некоторые константы, а P – размер поля. Такие алгоритмы называются субэкспоненциальными и позволяют сравнительно легко вскрывать дискретный логарифм в конечном поле, если размер поля не выбран очень большим, порядка 2^{1024}.

В тоже время наиболее быстрые методы решения дискретного логарифма на эллиптической кривой имеют сложность $O(\sqrt{q})$, где q — количество точек эллиптической кривой. Таким образом, для обеспечения уровня стойкости в 2^{80} операций необходимо чтобы $q=2^{160}$. Для того, чтобы получить аналогичный уровень сложности при вычислении дискретного логарифма в конечном поле необходимо поле порядка $q=2^{1024}$.

Следует заметить, что поскольку мощность вычислительной техники постоянно повышается, значение q будет постоянно увеличиваться. Но так как графики функций $O(\sqrt{q})$ и $O(\exp(c(logP\ log\ log\ P)^d))$ резко отличаются друг

от друга, в группе точек эллиптической кривой q будет расти намного медленнее, чем в произвольном конечном поле [4].

На основании всего вышесказанного можно выделить основные достоинства эллиптической криптографии:

1. Гораздо меньшая длина ключа по сравнению с наиболее распространенным методом асимметричного шифрования RSA.
2. Скорость работы эллиптических алгоритмов гораздо выше, чем у классических. Это объясняется как размерами поля, так и применением более близкой для компьютеров структуры бинарного конечного поля.
3. Из-за маленькой длины ключа и высокой скорости работы, алгоритмы асимметричной криптографии на эллиптических кривых могут использоваться в смарт-картах и других устройствах с ограниченными вычислительными ресурсами.

Все плюсы эллиптической криптографии вытекают из одного конкретного факта: для задачи дискретного логарифмирования на эллиптических кривых не существует субэкспоненциальных алгоритмов решения. Это позволяет уменьшить длину ключа и увеличить производительность. Однако, если такие алгоритмы появятся, то это будет означать крах эллиптической криптографии.

Эллиптическая криптография — это очень сложно. Это огромное количество тонкостей, которые необходимо учесть, начиная с выбора эллиптической кривой и заканчивая генерацией ключей. При массовом переходе на эллиптическую криптографию обязательно будет большое количество ошибок и уязвимостей, которые уже отработаны для более привычных методов [6].

uuuuuuuuuuuuuuu2 Практическая часть

Работа будет выполняться на ПК со следующими характеристиками: процессор Intel i5-4670 (6 МБ кэш-памяти, тактовая частота до 3,80 ГГц), остальные характеристики не принципиальны.

Для шифрования длинных текстов будет использовано гибридное шифрование, которое является распространенным способом получить скорость криптосистем с симметричным ключом в сочетании с преимуществами открытого и закрытого ключей ECC.

В своей работе я буду использовать ключи шифрования с различной длиной, а также произведу сравнение с самым распространенным методом шифрования методом RSA.

Гибридная схема работает следующим образом: для симметричного алгоритма (например, AES) генерируется случайный сеансовый ключ, который мы будем использовать в дальнейшем для шифрования и дешифрования текста. Такой ключ как правило имеет размер от 128 до 512 бит (в зависимости от алгоритма). Затем используется данный симметричный алгоритм для шифрования сообщения, что позволит шифровать сообщение с длиной, превышающей длину блока. Что касается самого случайного ключа, он должен быть зашифрован с помощью открытого ключа получателя сообщения, и именно на этом этапе применяется криптосистема с открытым ключом ECC. Поскольку сеансовый ключ короткий, его шифрование занимает немного времени. Однако я в своей работе буду использовать и длинные ключи для сеансовых ключей, чтобы увидеть скорость работы алгоритмов.

Шифрование набора сообщений с помощью асимметричного алгоритма – это задача вычислительно более сложная, поэтому здесь предпочтительнее использовать симметричное шифрование. Затем достаточно отправить сообщение, зашифрованное симметричным алгоритмом, а также соответствующий ключ в зашифрованном виде. Получатель сначала

расшифровывает ключ с помощью своего секретного ключа, а затем с помощью полученного ключа получает и всё сообщение.

Для реализации задачи шифрования и расшифрования текста я буду использовать программу, написанную на языке Python и использующую библиотеки PyCryptodome и tinyec. Также сравним шифрование ECC с шифрованием методом RSA.

Код программ представлен в Приложении Б и В.

Время создания пары ключей ECC, аналогичные по криптозащите RSA, выполняется значительно быстрее, чем методом RSA, что дает нам большую производительность при аналогичной защите.

Таблица 1 – Сравнение времени генерации пары ключей для разных методов шифрования:

RSA, размер ключа	**Время генерации, сек**	**Время генерации, сек**	**ECC, размер ключа**
1024	0.151	0.082	160
2048	1.864	0.085	224
3072	14.256	0.082	256
7680	104.973	0.100	384
15360	859.899	0.102	521

Заметим, что линейной связи между размерами ключей RSA и ECC нет (то есть если мы удваиваем размер ключа RSA, нам не нужно удваивать размер ключа ECC). Из данной таблицы мы видим, что ключи ECC не только используют меньше памяти, но и генерация самих ключей происходит значительно быстрее.

Модуль PyCryptodome не предоставляет возможности шифрования и дешифрования текста методом эллиптических кривых. Поэтому мы будем использовать этот модуль частично для шифрования текста симметричным способом AES, а сам ключ асимметричного шифрования ECC и

шифрование/дешифрование текста будем осуществлять с помощью модуля Tinyec.

Текст программы приложен в Приложении Г.

В качестве шифруемого текста будем использовать текст произведения Л.Н.Толстого «Война и мир» (для большего количества символов), количество символов будет изменяться для определения скорости работы с каждой парой ключей шифрования.

Шифруемый текст:

```
-Eh bien, mon prince. Genes et Lucques ne sont plus que des apanages, des поместья, de la famille Buonaparte. Non, je vous previens, que si vous ne me dites pas, que nous avons la guerre, si vous vous permettez encore de pallier toutes les infamies, toutes les atrocites de cet Antichrist (ma parole, j'y crois) - je ne vous connais plus, vous n'etes plus mon ami, vous n'etes plus мой верный раб, comme vous dites. [  Ну, что, князь, Генуа и Лукка стали не больше, как поместьями фамилии Бонапарте. Нет, я вас предупреждаю, если вы мне не скажете, что у нас война, если вы еще позволите себе защищать все гадости, все ужасы этого Антихриста (право, я верю, что он Антихрист) - я вас больше не знаю, вы уж не друг мой, вы уж не мой верный раб, как вы говорите.]  Ну, здравствуйте, здравствуйте. Je vois que je vous fais peur, [  Я вижу, что я вас пугаю,]  садитесь и рассказывайте. <…>
```

Что получаем в файле, содержащий зашифрованный текст:

```
{'ciphertext':
b'2f045c9a91ae8522ef9c76e009423e26056271ed4faa95bc3d4a4da9825695bee55743e7fccd2fa79f404e7feda
b8336fb2ccb54c6230a38568da2229f17ba402f8101f0694e045dc21a0809eff8623af0da4708669a03d64f873384
74a30983cc5eed9dec954ff3fedfdf7042009ed3bd7cab74c4040f181e2d2b226c92f9b59fcd6f7d84a06b77381fb
b7ae0bd4dea5babca91dd0017187869e5b8d348a6ab660d50a752865d6592cf0e5217aeec329549b6beaf400ebe17
08792f2bbf4760aa7624abae2cf83a7e63133ed09b53f12c2bff370a0285b57524874f387112e1637c51526595bfc
14701be6121864bddcdd369398e83cadd01195e488164d98897c4ae358fc706dd8ffb33cf7f4821389ec17e6e28ca
ae45b26743d52b97ce48edea2af1c8de3772ccc0116663cb78b101b7d0f4f0627530bb652aee78f29fcdb19d01c39
945c8ef7c14a9a8dbb3545b4a5e55c67014b132ab4857dfd7279980f6e60688598fcfa58aeff2408f8231917a4a38
4779b8265d7460305d3cc60049338831224ff063ab3b804e9db537775edac0673d7771d84c2c41deceb8dfcc311aa
1a199974bc405c525893e4be52384645d77a31f9d87af8d36e932ab4e26494a7f9b6eea823a2786f991c25654f320
<…>
```

При выполнении данного кода программы для шифрования текста и расшифрования данного текста имеем следующие показатели выполнения времени, которые занесены в таблицу 2.

В эту же таблицу мы внесем данные по шифрованию и расшифрованию текста с помощью метода RSA, используя сгенерированные ключи, поскольку их генерация занимает значительное время. Текст программы представлен в Приложении Д.

Таблица 2 – Данные по количеству символов шифруемого текста и времени выполнения:

	2^{16} = 65536	2^{18} = 262144	2^{20} = 1048576	2^{22} = 4194304
RSA-1024	0.034	0.035	0.043	0.069
ECC-160	0.038	0.039	0.042	0.058
RSA-2048	**0.073**	**0.075**	**0.083**	**0.108**
ECC-224	0.075	0.075	0.085	0.095
RSA-3072	0.145	0.154	0.157	0.184
ECC-256	**0.098**	**0.100**	**0.107**	**0.118**
RSA-7680	1.113	1.121	1.123	1.153
ECC-384	0.244	0.246	0.246	0.248
RSA-15360	7.108	7.184	7.167	7.153
ECC-512	0.444	0.452	0.456	0.474

Мы видим, что скорость шифрования текста практически не зависит от количества исходных символов, а время выполнения шифрования с помощью гибридного метода (ECC-AES) зависит от скорости создания ключей для асимметричного шифрования. Шифрование небольшого сессионного ключа методом AES и шифрование текста с использованием симметричного ключа занимает небольшое количество времени.

Из-за отсутствия эффективного метода задачи дискретного логарифмирования чисел, сгенерированные единожды ключи длиной 256 бит (которые сейчас имеют наибольшее распространение) можно будет использовать на протяжении нескольких лет, а может и десятилетий. Поскольку на текущий момент удалось решить задачу дискретного логарифмирования эллиптической кривой с интервалом 114 бит на кривой secp256k1, другими словами, на сегодняшний день удалось расшифровать данные, которые были зашифрованы с ключами, основанными на кривых длиной 114 бит.

3 Финансовый менеджмент, ресурсоэффективность и ресурсосбережение

3.1 Предпроектный анализ

3.1.1 Потенциальные потребители результатов исследования

Для анализа потребителей результатов исследования необходимо рассмотреть целевой рынок и провести его сегментирование.

Целевой рынок– сегменты рынка, на котором будет продаваться в будущем разработка. В свою очередь, сегмент рынка– это особым образом выделенная часть рынка, группы потребителей, обладающих определенными общими признаками.

Сегментирование– это разделение покупателей на однородные группы, для каждой из которых может потребоваться определенный товар (услуга). Можно применять географический, демографический, поведенческий и иные критерии сегментирования рынка потребителей, возможно применение их комбинаций с использованием таких характеристик, как возраст, пол, национальность, образование, любимые занятия, стиль жизни, социальная принадлежность, профессия, уровень дохода.

Таблица 3 – Карта сегментирования рынка шифрования данных методом ECC

Размер компании	Вид использования шифрования данных методом ECC		
		Передача информации	Хранение данных
	Крупные		
	Средние		
	Мелкие		

Фирма А Фирма Б

3.1.2 Анализ конкурентных технических решений

Детальный анализ конкурирующих разработок, существующих на рынке, необходимо проводить систематически, поскольку рынки пребывают в постоянном движении. Такой анализ помогает вносить коррективы в научное исследование, чтобы успешнее противостоять своим соперникам. Важно реалистично оценить сильные и слабые стороны разработок конкурентов.

С этой целью может быть использована вся имеющаяся информация о конкурентных разработках:

- технические характеристики разработки;
- конкурентоспособность разработки;
- уровень завершенности научного исследования (наличие макета, прототипа и т.п.);
- бюджет разработки;
- уровень проникновения на рынок;
- финансовое положение конкурентов, тенденции его изменения и т.д.

Анализ конкурентных технических решений с позиции ресурсоэффективности и ресурсосбережения позволяет провести оценку сравнительной эффективности научной разработки и определить направления для ее будущего повышения.

Проведем данный анализ с помощью оценочной карты. В ходе исследования был рассмотрен метод шифрования с помощью метода ECC (эллиптические кривые) (показатель обозначим как ф). Шифрование данных можно провести также с помощью метода RSA (конкурент к1), а также с помощью обмена ключами Диффи–Хелмана (конкурент к2).

Таблица 4 – Оценочная карта для сравнения конкурентных технических решений

Критерии оценки	Вес критерия	Баллы			Конкурентоспособность		
		$Б_ф$	$Б_{к1}$	$Б_{к2}$	$К_ф$	$К_{к1}$	$К_{к2}$
1	2	3	4	5	6	7	8
Технические критерии оценки ресурсоэффективности							
1. Повышение производительности труда пользователя (увеличение скорости расчета, возможность работать с большими объемами данных)	0,09	5	3	3	0,45	0,27	0,27
2. Удобство в эксплуатации (соответствует требованиям потребителей)	0,09	5	5	4	0,45	0,45	0,36
3. Точность вычислений	0,1	5	5	5	0,5	0,5	0,5
4. Сложность вычислений	0,08	5	4	4	0,4	0,32	0,32
5. Доступность и простота (удобный формат, возможность вывода промежуточного результата и пр.) получаемых результатов	0,1	5	5	5	0,5	0,5	0,5
6. Адекватность модели и корректность результатов	0,1	5	5	5	0,5	0,5	0,5
Экономические критерии оценки эффективности							
1. Конкурентоспособность продукта	0,09	4	4	4	0,36	0,36	0,36
2. Уровень проникновения на рынок (степень внедрения данного продукта/услуги)	0,08	5	5	5	0,4	0,4	0,4
3. Стоимость продукта/услуги	0,1	5	4	4	0,5	0,4	0,4
4. Послепродажное обслуживание (техническая поддержка программного продукта/оказание дополнительных консультационных услуг)	0,1	5	5	5	0,5	0,5	0,5
5. Срок выхода на рынок	0,07	4	5	5	0,28	0,35	0,35
Итого	1	53	50	49	4,84	4,55	4,46

Критерии для сравнения и оценки ресурсоэффективности и ресурсосбережения, приведенные в таблице 4, подбираются, исходя из выбранных объектов сравнения с учетом их технических и экономических особенностей разработки, создания и эксплуатации.

Позиция разработки и конкурентов оценивается по каждому показателю экспертным путем по пятибалльной шкале, где 1 – наиболее слабая позиция, а 5

– наиболее сильная. Веса показателей, определяемые экспертным путем, в сумме должны составлять 1.

Анализ конкурентных технических решений определяется по формуле:

$$К = \sum В_i \cdot Б_i,$$

где К - конкурентоспособность научной разработки или конкурента;

$В_i$ - вес показателя (в долях единицы);

$Б_i$ - балл i-го показателя.

Исходя из приведенных расчетов, можно сделать вывод, что шифрование данных методом ECC является более предпочтительным, так как показатель К у первого метода выше, чем у второго. Наиболее низкий показатель у третьего метода. Основываясь на знаниях о конкурентах, можно объяснить, что шифрование данных методом ECC занимает меньше времени, чем двумя другими методами.

3.1.3 SWOT-анализ

Матрица SWOT-анализа представлена в таблице 5.

Таблица 5 – SWOT-анализ

	Сильные стороны: 1. Высокая скорость генерации ключей шифрования 2. Меньший размер ключа шифрования	**Слабые стороны:** 1. Необходимость хранения приватного ключа шифрования в недоступном для других пользователей месте 2. Нельзя допускать утерю ключей шифрования, чтобы не потерять зашифрованные данные
Возможности: 1. Использование данного метода шифрования данных для передачи через незащищенные каналы связи 2. Использование данного метода шифрования данных для хранения критически важной информации	Программа на основе метода ECC быстрее выполняет задачу по шифрованию данных	Необходимо сохранять резервные копии ключей шифрования и важных данных, зашифрованных ими
Угрозы: 1. Потеря ключей шифрования. 2. Вмешательство третьей стороны в канал передачи данных 3. Появление алгоритмов по дешифровке данных 4. Появление новых наиболее эффективных методик шифрования.	При утере ключей шифрования, генерируется новая пара ключей для дальнейшей работы за меньшее количество времени, чем сгенерированные другими методами	Необходимо внимательно изучать внешние угрозы для зашифрованных данных, а при компрометации ключей шифрования немедленно произвести их замену

Таким образом, при помощи построения матрицы SWOT были описаны сильные и слабые стороны проекта, выявлены возможности и угрозы для его реализации, которые могут появиться в его внешней среде.

3.1.4 Оценка готовности проекта к коммерциализации

Оценим степень готовности научной разработки к коммерциализации и выясним уровень собственных знаний для ее проведения. Для этого заполним специальную форму, содержащую показатели о степени проработанности проекта с позиции коммерциализации и компетенциям разработчика научного проекта.

Таблица 6 – Оценка степени готовности научного проекта к коммерциализации

№ п/п	Наименование	Степень проработанности научного проекта	Уровень имеющихся знаний у разработчика
1	Определен имеющийся научно-технический задел	5	4
2	Определены перспективные направления коммерциализации научно-технического задела	3	3
3	Определены отрасли и технологии (товары, услуги) для предложения на рынке	3	3
4	Определена товарная форма научно-технического задела для представления на рынок	3	3
5	Определены авторы и осуществлена охрана их прав	3	3
6	Проведена оценка стоимости интеллектуальной собственности	3	3
7	Проведены маркетинговые исследования рынков сбыта	2	3
8	Разработан бизнес-план коммерциализации научной разработки	3	3
9	Определены пути продвижения научной разработки на рынок	4	3
10	Разработана стратегия (форма) реализации научной разработки	3	2
11	Проработаны вопросы международного сотрудничества и выхода на зарубежный рынок	1	1
12	Проработаны вопросы использования услуг инфраструктуры поддержки, получения льгот	1	1
13	Проработаны вопросы финансирования коммерциализации научной разработки	1	2
14	Имеется команда для коммерциализации научной разработки	1	2
15	Проработан механизм реализации научного проекта	1	3
	ИТОГО БАЛЛОВ	37	39

При проведении анализа по таблице, приведенной выше, по каждому показателю ставится оценка по пятибалльной шкале. При этом система измерения по каждому направлению (степень проработанности научного проекта, уровень имеющихся знаний у разработчика) отличается. Так, при оценке степени проработанности научного проекта 1 балл означает не проработанность проекта, 2 балла – слабую проработанность, 3 балла – выполнено, но в качестве не уверен, 4 балла – выполнено качественно, 5 баллов – имеется положительное заключение независимого эксперта. Для оценки уровня имеющихся знаний у разработчика система баллов принимает следующий вид: 1 означает не знаком или мало знаю, 2 – в объеме теоретических знаний, 3 – знаю теорию и практические примеры применения, 4 – знаю теорию и самостоятельно выполняю, 5 – знаю теорию, выполняю и могу консультировать.

Оценка готовности научного проекта к коммерциализации (или уровень имеющихся знаний у разработчика) определяется по формуле:

$$Б_{сум} = \sum Б_i,$$

где $Б_{сум}$ – суммарное количество баллов по каждому направлению;

$Б_i$ – балл по i-му показателю.

Значение $Б_{сум}$позволяет говорить о мере готовности научной разработки и ее разработчика к коммерциализации. Так, если значение $Б_{сум}$ получилось от 75 до 60, то такая разработка считается перспективной, а знания разработчика достаточными для успешной ее коммерциализации. Если от 59 до 45 – то перспективность выше среднего. Если от 44 до 30 – то перспективность средняя. Если от 29 до 15 – то перспективность ниже среднего. Если 14 и ниже – то перспективность крайне низкая.

Таким образом, можно сделать вывод о том, что перспективность коммерциализации находится на среднем уровне. Этот уровень можно повысить путем более детального исследования коммерческой составляющей проекта, которая включает в себя анализ рынков сбыта, разработку бизнес-плана и т.д.

3.1.5 Методы коммерциализации результатов научно-технического исследования

Время продвижения товара на рынок во многом зависит от правильности выбора метода коммерциализации. Выделяют следующие методы коммерциализации научных разработок.

1. Торговля патентными лицензиями, т.е. передача третьим лицам права использования объектов интеллектуальной собственности на лицензионной основе. При этом в патентном законодательстве выделяют следующие виды лицензий: исключительные (простые), исключительные, полные лицензии, сублицензии, опционы.

2. Передача ноу-хау, т.е. предоставление владельцем ноу-хау возможности его использовать другим лицом, осуществляемое путем раскрытия ноу-хау.

3. Инжиниринг как самостоятельный вид коммерческих операций предполагает предоставление на основе договора инжиниринга одной стороной, именуемой консультантом, другой стороне, именуемой заказчиком, комплекса или отельных видов инженерно-технических услуг, связанных с проектированием, строительством и вводом объекта в эксплуатацию, с разработкой новых технологических процессов на предприятии заказчика, усовершенствованием имеющихся производственных процессов вплоть до внедрения изделия в производство и даже сбыта продукции.

4. Франчайзинг, т.е. передача или переуступка (на коммерческих условиях) разрешения продавать чьи-либо товары или оказывать услуги в некоторых областях.

5. Организация собственного предприятия.

6. Передача интеллектуальной собственности в уставной капитал предприятия.

7. Организация совместного предприятия, т.е. объединение двух и более лиц для организации предприятия.

8. Организация совместных предприятий, работающих по схеме «российское производство – зарубежное распространение».

Для данного научно-технического исследования предпочтительным является метод коммерциализации как передача ноу-хау возможности его использовать другим лицом, так как модель построена на информации, находящейся в открытом доступе.

3.2 Инициация проекта

В рамках данного раздела необходимо определить изначальные цели и содержание, изначальные финансовые ресурсы, внутренние и внешние заинтересованные стороны проекта, которые будут взаимодействовать и влиять на общий результат научного проекта. Данную информацию необходимо закрепить в Уставе проекта.

Устав проекта документирует бизнес-потребности, текущее понимание потребностей заказчика проекта, а также новый продукт, услугу или результат, который планируется создать.

Устав научного проекта магистерской работы должен иметь следующую структуру:

1. Цели и результат проекта. Необходимо привести информацию о заинтересованных сторонах проекта, иерархии целей проекта и критериях достижения целей.

Под заинтересованными сторонами проекта понимаются лица или организации, которые активно участвуют в проекте или интересы которых могут быть затронуты как положительно, так и отрицательно в ходе исполнения или в результате завершения проекта. Это могут быть заказчики, спонсоры, общественность и т.п. Информация по заинтересованным сторонам проекта представлена в таблице 7.

Таблица 7 – Заинтересованные стороны проекта

Заинтересованные стороны проекта	**Ожидания заинтересованных сторон**
НИ ТПУ, ОЭФ	Проведение исследований по данной теме с целью использования настоящей разработки в образовательных целях, а также использование данной разработки в качестве основы под иные проекты, выполняемые на базе ОЭФ.
АО «ТОМ-ДОМ ТДСК»	Использование данной разработки для передачи приватных данных по открытым каналам связи.

В таблице 8 представлена информация о иерархии целей проекта и критерии их достижения. Цели проекта должны включать цели в области ресурсоэффективности и ресурсосбережения.

Таблица 8 – Цели и результат проекта

Цели проекта	Создание механизма для передачи приватных данных по открытым для третьих лиц каналам связи
Ожидаемые результаты проекта	Зашифрованный текст, стойкий ко взлому
Критерии приемки результата проекта	Нет возможности расшифровать перехваченный текст
Требования к результату проекта	Данные после расшифровки полностью совпадают с исходным текстом

2. Организационная структура проекта. Необходимо решить следующие вопросы: кто будет входить в рабочую группу данного проекта, определить роль каждого участника в данном проекте, а также прописать функции, выполняемые каждым из участников и их трудозатраты в проекте. Данная информация представлена в таблице 9.

Таблица 9 – Рабочая группа проекта

№ п/п	ФИО, основное место работы, должность	Роль в проекте	Функции	Трудозатраты, дн.
1	Крицкий Олег Леонидович, доцент Доцент ОЭФ ТПУ	Руководитель проекта	Отвечает за реализацию проекта в пределах заданных ограничений по ресурсам, координирует деятельность исполнителя проекта	13
2	Адодин Андрей Николаевич, студент группы 0ВМ01, ТПУ ИЯТШ	Исполнитель по проекту	Выполняет работы по проекту	118

3. Ограничения и допущения проекта. Ограничения и допущения проекта представлены в таблице 10.

Таблица 10 – Ограничения проекта

Фактор	Ограничения/допущения
Бюджет проекта	229 392
Источник финансирования	НИ ТПУ, ОЭФ
Сроки проекта (дней):	122
Дата утверждения плана управления проектом	31.01.2022
Дата завершения проекта	01.06.2022

1.3 Иерархическая структура работ проекта

Иерархическая структура работ (ИСР) – детализация укрупненной структуры работ. В процессе создания ИСР структурируется и определяется содержание всего проекта. Иерархическая структура работ проекта представлена на рисунке 3.

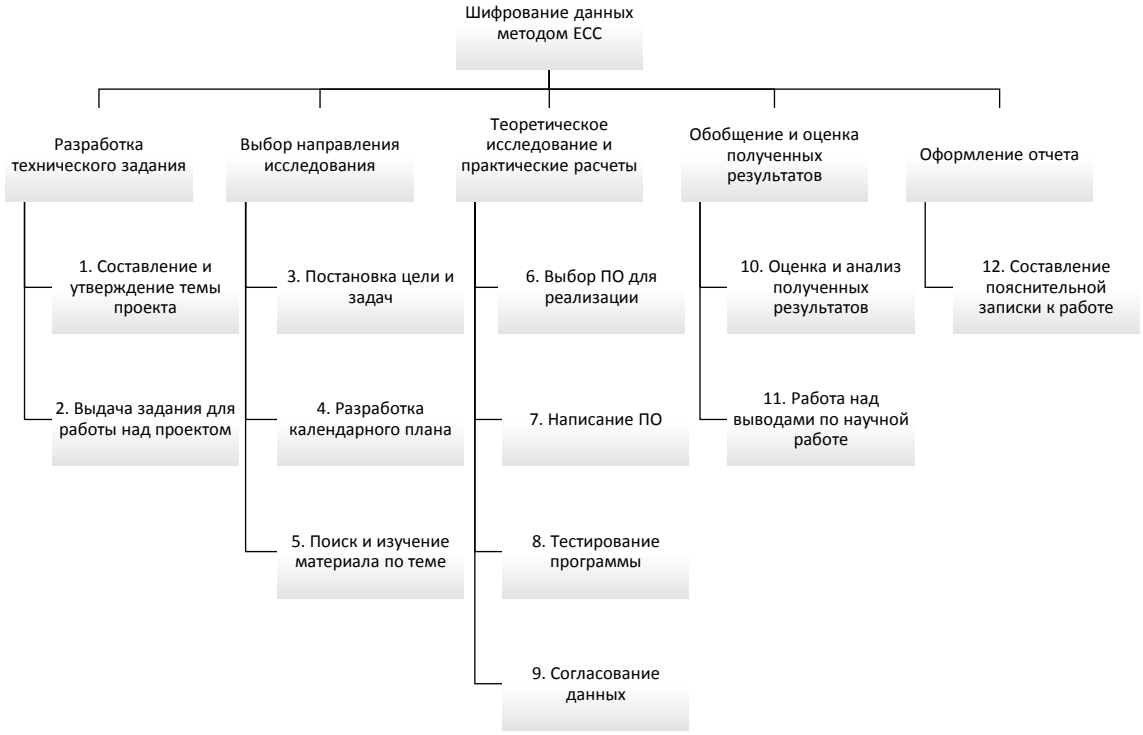

Рисунок 3 – Иерархическая структуры работ по проекту

Таблица 11 – Контрольные события проекта

№ п/п	**Контрольное событие**	**Дата**	**Результат (подтверждающий документ)**
1	Технологическая практика	31.01.2022-12.03.2022	Шифрование данных методом RSA
2	Преддипломная практика	31.03.2022-01.06.2022	Шифрование данных методом ECC

3.4 План проекта

В рамках планирования научного проекта необходимо построить календарный график проекта.

Таблица 12 – Календарный план проекта

Код работы (из ИСР)	Название	Длитель-ность, дни	Дата начала работ	Дата окончания работ	Состав участников (ФИО ответственных исполнителей)
1	Составление и утверждение темы проекта	2	31.01.2022	01.02.2022	Крицкий О.Л.
2	Выдача задания для работы над проектом	2	02.02.2022	03.02.2022	Крицкий О.Л.
3	Постановка цели и задач	3	04.02.2022	07.02.2022	Адодин А.Н.
4	Разработка календарного плана	4	08.02.2022	11.02.2022	Крицкий О.Л. Адодин А.Н.
5	Поиск и изучение материала по теме	8	12.02.2022	21.02.2022	Адодин А.Н.
6	Выбор ПО для реализации	7	22.02.2022	02.03.2022	Адодин А.Н.
7	Написание ПО	40	03.03.2022	21.04.2022	Адодин А.Н.
8	Тестирование программы	5	22.04.2022	27.04.2022	Адодин А.Н.
9	Согласование данных	3	28.04.2022	02.05.2022	Крицкий О.Л. Адодин А.Н.
10	Оценка и анализ полученных результатов	9	03.05.2022	16.05.2022	Адодин А.Н.
11	Работа над выводами по научной работе	5	17.05.2022	22.05.2022	Адодин А.Н.
12	Составление пояснительной записки к работе	9	23.05.2022	01.06.2022	Адодин А.Н.

Итого, общая максимальная длительность работ составила 122 календарных дня. Руководитель Крицкий О.Л. – 11 рабочих дней, исполнитель Адодин А.Н. – 93 рабочих дня, без учета выходных и праздничных дней при 6-дневной рабочей неделе.

Диаграмма Ганта – это тип столбчатых диаграмм (гистограмм), который используется для иллюстрации календарного плана проекта, на котором работы

по теме представляются протяженными во времени отрезками, характеризующимися датами начала и окончания выполнения данных работ.

График представлен на рисунке 4 с разбивкой по месяцам и декадам (10 дней) за период времени выполнения научного проекта. При этом работы на графике следует выделить различной штриховкой в зависимости от исполнителей, ответственных за ту или иную работу.

Код работы (из ИСР)	Название	Исполните-ли	Дата начала работ	Дата окончания работ	Продолжительность выполнения работ, недели
					февраль: 1, 2, 3; март: 1, 2, 3; апрель: 1, 2, 3; май: 1, 2, 3
1	Составление и утверждение темы проекта	Руководитель проекта	31.01.2022	01.02.2022	
2	Выдача задания для работы над проектом	Руководитель проекта	02.02.2022	03.02.2022	
3	Постановка цели и задач	Исполнитель по проекту	04.02.2022	07.02.2022	
4	Разработка календарного плана	Руководитель проекта Исполнитель по проекту	08.02.2022	11.02.2022	
5	Поиск и изучение материала по теме	Исполнитель по проекту	12.02.2022	21.02.2022	
6	Выбор ПО для реализации	Исполнитель по проекту	22.02.2022	02.03.2022	
7	Написание ПО	Исполнитель по проекту	03.03.2022	21.04.2022	
8	Тестирование программы	Исполнитель по проекту	22.04.2022	27.04.2022	
9	Согласование данных	Руководитель проекта Исполнитель по проекту	28.04.2022	02.05.2022	
10	Оценка и анализ полученных результатов	Исполнитель по проекту	03.05.2022	16.05.2022	
11	Работа над выводами по научной работе	Исполнитель по проекту	17.05.2022	22.05.2022	
12	Составление пояснительной записки к работе	Исполнитель по проекту	23.05.2022	01.06.2022	

Рисунок 4 – Календарный план-график проведения НИОКР

- Исполнитель по проекту

- Руководитель проекта

3.4.1 Бюджет научного исследования

При планировании бюджета научного исследования должно быть обеспечено полное и достоверное отражение всех видов планируемых расходов, необходимых для его выполнения.

Сырье, материалы, покупные изделия и полуфабрикаты

В эту статью включаются затраты на приобретение всех видов материалов, комплектующих изделий и полуфабрикатов, необходимых для выполнения работ по данной теме. Количество потребных материальных ценностей определяется по нормам расхода.

Расчет стоимости материальных затрат производится по действующим прейскурантам или договорным ценам. В стоимость материальных затрат включают транспортно-заготовительные расходы (3 – 5 % от цены). В эту же статью включаются затраты на оформление документации (канцелярские принадлежности, тиражирование материалов).

В данной работе не использовались сырье, материалы, комплектующие изделия и полуфабрикаты.

Основная заработная плата

В данную статью включается основная заработная плата исполнителей, непосредственно участвующих в проектировании разработки. Величина расходов по заработной плате определяется исходя из трудоемкости выполняемых работ и действующей системы оплаты труда. В состав основной заработной платы включается премия, выплачиваемая ежемесячно из фонда заработной платы (размер определяется Положением об оплате труда).

Статья включает основную заработную плату работников, непосредственно занятых выполнением проекта, (включая премии, доплаты) и дополнительную заработную плату.

$$С_{зп} = З_{осн} + З_{доп},$$

где $З_{осн}$ – основная заработная плата;

$З_{доп}$ – дополнительная заработная плата.

Основная заработная плата ($З_{осн}$) руководителя рассчитывается по следующей формуле:

$$З_{осн} = З_{дн} \cdot Т_р,$$

где $З_{осн}$ – основная заработная плата;

$З_{дн}$ – среднедневная заработная плата работника, руб.;

$Т_р$ – продолжительность работ, выполняемых научно-техническим работником, раб. дн.

Среднедневная заработная плата рассчитывается по формуле:

$$З_{дн} = \frac{З_м \cdot М}{F_д},$$

где $З_м$ – месячный должностной оклад работника, руб.;

М – количество месяцев работы без отпуска в течение года:

при отпуске в 24 раб. дня М =11,2 месяца, 5-дневная неделя;

при отпуске в 48 раб. дней М=10,4 месяца, 6-дневная неделя;

$F_д$ – действительный годовой фонд рабочего времени научно- технического персонала, раб. дн.

Таблица 13 – Баланс рабочего времени

Показатели рабочего времени	Руководитель	Исполнитель (инженер)
Календарное количество рабочих дней	365	365
Количество рабочих дней Выходные дни/ Праздничные дни	66	66
Потери рабочего времени Отпуск/невыходы по болезни	56	48
Действительный годовой фонд рабочего времени	243	251

Месячный должностной оклад работника:

$$З_м = З_б \cdot (1 + k_{пр} + k_д) \cdot k_р,$$

где $З_б$ – базовый оклад, руб.;

$k_{пр}$ – премиальный коэффициент (определяется Положением об оплате труда);

$k_д$ – коэффициент доплат и надбавок (определяется Положением об оплате труда);

$k_р$ – районный коэффициент, равный 1,3 (для Томска).

Основная заработная плата руководителя (от ТПУ) рассчитывается на основании отраслевой оплаты труда. Отраслевая система оплаты труда в ТПУ предполагает следующий состав заработной платы:

1) оклад – определяется предприятием. В ТПУ оклады распределены в соответствии с занимаемыми должностями, например, ассистент, ст. преподаватель, доцент, профессор. Базовый оклад $З_б$ определяется исходя из размеров окладов, определенных штатным расписанием предприятии.

2) стимулирующие выплаты – устанавливаются руководителем подразделений за эффективный труд, выполнение дополнительных обязанностей и т.д.

3) иные выплаты; районный коэффициент.

Таблица 14 – Расчёт основной заработной платы

Исполнители	$З_б$, руб.	$k_{пр}$	$k_д$	$k_р$	$З_м$	$З_{дн}$	$Т_р$, дн.	$З_{осн}$, руб.
Руководитель	37 000,00	0	0,02	1,3	49 062,00	2 099,77	11,00	23 097,50
Инженер	15 279,00	0	0,00	1,3	19 862,70	823,00	93,00	76 538,66
ИТОГО								**99 636,16**

Дополнительная заработная плата научно-производственного персонала

В данную статью включается сумма выплат, предусмотренных законодательством о труде, например, оплата очередных и дополнительных отпусков; оплата времени, связанного с выполнением государственных и общественных обязанностей; выплата вознаграждения за выслугу лет и т.п. (в среднем – 12 % от суммы основной заработной платы).

Дополнительная заработная плата рассчитывается исходя из 10- 15% от основной заработной платы, работников, непосредственно участвующих в выполнение темы:

$$З_{доп} = З_{осн} \cdot k_{доп},$$

где $З_{доп}$ – дополнительная заработная плата, руб.;

$k_{доп}$ – коэффициент дополнительной зарплаты (на стадии проектирования принимается равным 0,12);

$З_{осн}$ – основная заработная плата, руб.

Таблица 15 – Расчет дополнительной заработной платы

Заработная плата	Основная заработная плата	Дополнительная заработная плата
Руководитель	23 097,50	3 464,63
Исполнитель	76 538,66	11 480,80
ИТОГО		**14 945,42**

Страховые взносы

Статья включает в себя отчисления во внебюджетные фонды.

$$С_{внеб} = (З_{осн} + З_{доп}) \cdot k_{внеб},$$

где $k_{внеб}$ – коэффициент отчислений на уплату во внебюджетные фонды (пенсионный фонд, фонд обязательного медицинского страхования и пр.). Установлен размер страховых взносов равный 30,2%.

Таким образом, затраты на отчисления во внебюджетные фонды составили 34 603,64 руб.

Накладные расходы

В эту статью включаются затраты на управление и хозяйственное обслуживание, которые могут быть отнесены непосредственно на конкретную тему. Кроме того, сюда относятся расходы по содержанию, эксплуатации и ремонту оборудования, производственного инструмента и инвентаря, зданий, сооружений и др. В расчетах эти расходы принимаются в размере 70 - 90 % от суммы основной заработной платы научно-производственного персонала данной научно-технической организации.

Накладные расходы составляют 80-100 % от суммы основной и дополнительной заработной платы, работников, непосредственно участвующих в выполнение темы.

Расчет накладных расходов ведется по следующей формуле:

$$С_{нал} = (З_{осн} + З_{доп}) \cdot k_{накл},$$

где $k_{накл}$ – коэффициент накладных расходов.

Таким образом, размер накладных расходов составил 80 207,11 руб.

На основании полученных данных по отдельным статьям затрат составляется калькуляция плановой себестоимости НТИ.

Таблица 16 – Бюджет затрат НТИ

Статьи	**Сумма, руб.**
Сырье, материалы (за вычетом возвратных отходов), покупные изделия и полуфабрикаты	0,00
Основная заработная плата	99 636,16
Дополнительная заработная плата	14 945,42
Отчисления на социальные нужды	34 603,64
Накладные расходы	80 207,11
Итого плановая себестоимость	**229 392,33**

3.4.2 Реестр рисков проекта

Идентифицированные риски проекта включают в себя возможные неопределенные события, которые могут возникнуть в проекте и вызвать последствия, которые повлекут за собой нежелательные эффекты.

Таблица 17 – Реестр рисков

№	Риск	Потенциальное воздействие	Вероятность наступления (1-5)	Влияние риска (1-5)	Уровень риска	Способы смягчения	Условия наступления
1	Потеря ключей шифрования	Невозможность расшифровать данные	2	5	низкий	Дублирование ключей	Потеря ключа шифрования вследствие утраты или порчи носителя
2	Потеря части зашифрованных данных при передаче	Невозможность расшифровать данные	4	2	высокий	Разбиение данных на несколько блоков. Отправка копии зашифрованных данных	Сбои при передаче данных по каналам связи
3	Потеря части зашифрованных данных при хранении	Невозможность расшифровать данные	2	3	средний	Дублирование зашифрованных данных.	Потеря данных вследствие порчи носителя

3.4.3 Оценка сравнительной эффективности исследования

Определение эффективности происходит на основе расчета интегрального показателя эффективности научного исследования. Его нахождение связано с определением двух средневзвешенных величин: финансовой эффективности и ресурсоэффективности.

Интегральный показатель финансовой эффективности научного исследования получают в ходе оценки бюджета затрат трех (или более) вариантов исполнения научного исследования. Для этого наибольший интегральный

показатель реализации технической задачи принимается за базу расчета (как знаменатель), с которым соотносится финансовые значения по всем вариантам исполнения.

Интегральный финансовый показатель разработки определяется как:

$$I_{\text{ф}}^{p} = \frac{\Phi_{pi}}{\Phi_{max}}$$

где $I_{\text{ф}}^{p}$ - интегральный финансовый показатель разработки;

Φ_{pi} - стоимость i-го варианта исполнения;

Φ_{max} - максимальная стоимость исполнения научно-исследовательского проекта, за максимально возможную стоимость исполнения примем 300 000 руб.

Полученная величина интегрального финансового показателя разработки отражает соответствующее численное увеличение бюджета затрат разработки в разах (значение больше единицы), либо соответствующее численное удешевление стоимости разработки в разах (значение меньше единицы, но больше нуля).

Интегральный показатель ресурсоэффективности вариантов исполнения объекта исследования можно определить следующим образом:

$$I_{\text{ф}}^{p} = \frac{\Phi_{pi}}{\Phi_{max}}$$

где $I_{\text{ф}}^{p}$ - интегральный финансовый показатель разработки; Φ_{pi} - стоимость i-го варианта исполнения; Φ_{max} - максимальная стоимость исполнения научно-исследовательского проекта, за максимально возможную стоимость исполнения примем 250000 руб.

Интегральный показатель ресурсоэффективности определяется по формуле:

$$I_m^a = \sum_{i=1}^{n} a_i b_i^a,$$

$$I_m^p = \sum_{i=1}^{n} a_i b_i^p$$

где I_m – интегральный показатель ресурсоэффективности;

a_i – весовой коэффициент i -го варианта исполнения разработки;

b_i^a, b_i^p – бальная оценка i -го варианта исполнения разработки;

n – число параметров сравнения.

Расчет интегрального показателя ресурсоэффективности проведен в таблице 18.

Таблица 18 – Сравнительная оценка характеристик вариантов исполнения проекта

Критерии	Весовой коэффициент параметра	Текущий проект	Аналог
Способствует росту производительности труда пользователя	0,1	5	4
Удобство в эксплуатации (соответствует требованиям потребителей)	0,15	5	5
Требует наличия исторических данных	0,15	5	5
Простота применения	0,2	4	4
Надежность	0,25	5	5
Конкурентоспособность (с другими моделями)	0,15	5	4
ИТОГО	1	4,8	4,55

$$\text{I}_{\text{тп}} = 5 \cdot 0{,}1 + 5 \cdot 0{,}15 + 5 \cdot 0{,}15 + 4 \cdot 0{,}2 + 5 \cdot 0{,}25 + 5 \cdot 0{,}15 = 4{,}8$$

$$\text{I}_{\text{аналог}} = 4 \cdot 0{,}1 + 5 \cdot 0{,}15 + 5 \cdot 0{,}15 + 4 \cdot 0{,}2 + 5 \cdot 0{,}25 + 4 \cdot 0{,}15 = 4{,}55$$

Интегральный показатель эффективности разработки ($I^{p}_{\text{финр}}$) и аналога ($I^{a}_{\text{финр}}$) определяется на основании интегрального показателя ресурсоэффективности и интегрального финансового показателя по формуле:

$$I^{p}_{\text{финр}} = \frac{I^{p}_{m}}{I^{p}_{\text{ф}}},$$

$$I^{a}_{\text{финр}} = \frac{I^{a}_{m}}{I^{a}_{\text{ф}}},$$

Сравнение интегрального показателя эффективности текущего проекта и аналогов позволит определить сравнительную эффективность проекта. Сравнительная эффективность проекта:

$$\text{Э}_{\text{ср}} = \frac{I^{p}_{\text{финр}}}{I^{a}_{\text{финр}}},$$

где $\text{Э}_{\text{ср}}$ – сравнительная эффективность проекта;

$I^{p}_{\text{финр}}$ – интегральный показатель разработки;

$I^{a}_{\text{финр}}$ – интегральный экономический показатель аналога.

Таблица 19 – Сравнительная эффективность разработки

№ п/п	Показатели	Текущий проект	Аналог
1	Интегральный финансовый показатель разработки	0,76	1,00
2	Интегральный показатель ресурсоэффективности разработки	4,80	4,55
3	Интегральный показатель эффективности	6,28	4,55
4	Сравнительная эффективность вариантов исполнения	1,31	0,95

Таким образом, можно сделать вывод о том, что разрабатываемый проект является более эффективным вариантом решения поставленной задачи по сравнению с предложенным аналогом, основываясь на показателях эффективности.

Сравнение значений интегральных показателей эффективности позволяет понять и выбрать более эффективный вариант решения поставленной в магистерской работе технической задачи с позиции финансовой и ресурсной эффективности.

Выводы

В ходе выполнения части работы по финансовому менеджменту, ресурсоэффективности и ресурсосбережению был проведен анализ разрабатываемого исследования.

Во-первых, оценен коммерческий потенциал и перспективность проведения исследования. Полученные результаты говорят о потенциале и перспективности на уровне выше среднего.

Во-вторых, проведено планирование НИР, а именно: определена структура и календарный план работы, трудоемкость и бюджет НТИ. Результаты соответствуют требованиям к магистерским диссертациям по срокам и иным параметрам.

В-третьих, определена эффективность исследования в разрезах ресурсной, финансовой, бюджетной, социальной и экономической эффективности.

4 Социальная ответственность

Введение

Социальная ответственность - ответственность отдельного ученого и научного сообщества перед обществом. Первостепенное значение при этом имеет безопасность применения технологий, которые создаются на основе достижений науки, предотвращение или минимизация возможных негативных последствий их применения, обеспечение безопасного как для испытуемых, так и для окружающей среды проведения исследований.

В ходе данной работы было написано программное обеспечение, позволяющее генерировать пары ключей шифрования, с помощью одного из которых (открытым) можно шифровать текст сообщения, для дальнейшей передачи его по открытым каналам связи с последующим расшифрованием другим (закрытым) ключом.

Работа выполнялась в аудитории 427а 10-ого корпуса Томского политехнического университета. Раздел также включает в себя оценку условий труда на рабочем месте, анализ вредных и опасных факторов труда, разработку мер защиты от них.

4.1 Производственная безопасность

4.1.1 Отклонение показателей микроклимата в помещении

Проанализируем микроклимат в помещении, где находится рабочее место. Микроклимат производственных помещений определяют следующие параметры: температура, относительная влажность, скорость движения воздуха. Эти факторы влияют на организм человека, определяя его самочувствие.

Оптимальные и допустимые значения параметров микроклимата приведены в таблице 20 и 21.

Таблица 20 – Оптимальные нормы микроклимата

Период года	Температура воздуха, С°	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	19-23	40-60	0.1
Теплый	23-25		0.2

Таблица 21 – Допустимые нормы микроклимата

Период года	Температура воздуха, С°		Относительная влажность воздуха, %	Скорость движения воздуха, м/с
	Нижняя допустимая граница	Верхняя допустимая граница		
Холодный	15	24	20-80	<0.5
Теплый	22	28	20-80	<0.5

Температура в теплый период года 23-25°С, в холодный период года 19-23°С, относительная влажность воздуха 40-60%, скорость движения воздуха 0,1 м/с.

Общая площадь рабочего помещения составляет 24 м^2, объем составляет 67,2 м^3. По СанПиН 2.2.2/2.4.1340-03 санитарные нормы составляют 6,5 м^2 и 20 м^3 объема на одного человека. Так как аудитория рассчитана на 10 человек, исходя из приведенных выше данных, можно сказать, что количество рабочих мест не соответствует размерам помещения по санитарным нормам.

После анализа габаритных размеров рассмотрим микроклимат в этой комнате. В качестве параметров микроклимата рассмотрим температуру, влажность воздуха, скорость ветра.

В помещении осуществляется естественная вентиляция посредством наличия легко открываемого оконного проема (форточки), а также дверного проема. По зоне действия такая вентиляция является общеобменной. Основной

недостаток - приточный воздух поступает в помещение без предварительной очистки и нагревания. Согласно нормам СанПиН 2.2.2/2.4.1340-03, объем воздуха, необходимый на одного человека в помещении без дополнительной вентиляции должен быть более 40 м^3. В нашем случае объем воздуха на одного человека составляет 6,72 м^3, из этого следует, что дополнительная вентиляция требуется. Параметры микроклимата поддерживаются в холодное время года за счет систем водяного отопления с нагревом воды до 100°С, а в теплое время года – за счет кондиционирования. Нормируемые параметры микроклимата, ионного состава воздуха, содержания вредных веществ должны соответствовать требованиям.

4.1.2 Превышение уровней шума

Одним из наиболее распространенных в производстве вредных факторов является шум. Он создается рабочим оборудованием, преобразователями напряжения, рабочими лампами дневного света, а также проникает снаружи. Шум вызывает головную боль, усталость, бессонницу или сонливость, ослабляет внимание, память ухудшается, реакция уменьшается.

Основным источником шума в комнате являются компьютерные охлаждающие вентиляторы. Уровень шума варьируется от 35 до 42 дБА. Согласно СанПиН 2.2.2 / 2.4.1340-03, при выполнении основных работ на ПЭВМ уровень шума на рабочем месте не должен превышать 82 дБА.

При значениях выше допустимого уровня необходимо предусмотреть средства индивидуальной защиты (СИЗ) и средства коллективной защиты (СКЗ) от шума.

Средства коллективной защиты:

1. устранение причин шума или существенное его ослабление в источнике образования;

2. изоляция источников шума от окружающей среды (применение глушителей, экранов, звукопоглощающих строительных материалов);

3. применение средств, снижающих шум и вибрацию на пути их распространения.

Средства индивидуальной защиты;

1. применение спецодежды и защитных средств органов слуха: наушники, беруши, антифоны.

4.1.3 Повышенный уровень электромагнитных излучений

Источником электромагнитных излучений в нашем случае являются дисплеи ПЭВМ. Монитор компьютера включает в себя излучения рентгеновской, ультрафиолетовой и инфракрасной области, а также широкий диапазон электромагнитных волн других частот. Согласно СанПиН 2.2.2/2.4.1340-03 напряженность электромагнитного поля по электрической составляющей на расстоянии 50 см вокруг ВДТ не должна превышать 25 В/м в диапазоне от 5Гц до 2кГц, 2,5В/м в диапазоне от 2 до 400 кГц. Плотность магнитного потока не должна превышать в диапазоне от 5 Гц до 2 кГц 250 нТл, и 25нТл в диапазоне от 2 до 400 кГц. Поверхностный электростатический потенциал не должен превышать 500В. В ходе работы использовалась ПЭВМ типа Acer VN7-791 со следующими характеристиками: напряженность электромагнитного поля 2,5 В/м; поверхностный потенциал составляет 450 В (основы противопожарной защиты предприятий ГОСТ 12.1.004 и ГОСТ 12.1.010 – 76).

При длительном постоянном воздействии электромагнитного поля (ЭМП) радиочастотного диапазона при работе на ПЭВМ у человеческого организма сердечно-сосудистые, респираторные и нервные расстройства, головные боли, усталость, ухудшение состояния здоровья, гипотония, изменения сердечной мышцы проводимости. Тепловой эффект ЭМП характеризуется

увеличением температуры тела, локальным селективным нагревом тканей, органов, клеток за счет перехода ЭМП на теплую энергию.

Предельно допустимые уровни облучения (по ОСТ 54 30013-83):

а) до 10 мкВт/см2, время работы (8 часов);

б) от 10 до 100 мкВт/см2, время работы не более 2 часов;

в) от 100 до 1000 мкВт/см2, время работы не более 20 мин. при условии пользования защитными очками;

г) для населения в целом ППМ не должен превышать 1 мкВт/см2.

Защита человека от опасного воздействия электромагнитного излучения осуществляется следующими способами:

СКЗ

1. защита временем;

2. защита расстоянием;

3. снижение интенсивности излучения непосредственно в самом источнике излучения;

4. экранирование источника;

5. защита рабочего места от излучения;

СИЗ

1. Очки и специальная одежда, выполненная из металлизированной ткани (кольчуга). При этом следует отметить, что использование СИЗ возможно при кратковременных работах и является мерой аварийного характера. Ежедневная защита обслуживающего персонала должна обеспечиваться другими средствами.

2. Вместо обычных стекол используют стекла, покрытые тонким слоем золота или диоксида олова (SnO_2).

4.1.4 Поражение электрическим током

К опасным факторам можно отнести наличие в помещении большого количества аппаратуры, использующей однофазный электрический ток

напряжением 220 В и частотой 50 Гц. По опасности электропоражения комната относится к помещениям без повышенной опасности, так как отсутствует повышенная влажность, высокая температура, токопроводящая пыль и возможность одновременного соприкосновения токоведущих элементов с заземленными металлическими корпусами оборудования.

Аудитория относится к помещению с без повышенной опасностью поражения электрическим током. Безопасными номиналами являются: $I < 0,1$ А; $U < (2\text{-}36)$ В; $R_{зазем} < 4$ Ом. В помещении применяются следующие меры защиты от поражения электрическим током: недоступность токоведущих частей для случайного прикосновения, все токоведущие части изолированы и ограждены. Недоступность токоведущих частей достигается путем их надежной изоляции, применения защитных ограждений (кожухов, крышек, сеток и т.д.), расположения токоведущих частей на недоступной высоте.

Каждому необходимо знать меры медицинской помощи при поражении электрическим током. В любом рабочем помещении необходимо иметь медицинскую аптечку для оказания первой медицинской помощи.

Поражение электрическим током чаще всего наступает при небрежном обращении с приборами, при неисправности электроустановок или при их повреждении.

Для освобождения пострадавшего от токоведущих частей необходимо использовать непроводящие материалы. Если после освобождения пострадавшего из-под напряжения он не дышит, или дыхание слабое, необходимо вызвать бригаду скорой медицинской помощи и оказать пострадавшему доврачебную медицинскую помощь:

- обеспечить доступ свежего воздуха (снять с пострадавшего стесняющую одежду, расстегнуть ворот);

- очистить дыхательные пути;

- приступить к искусственной вентиляции легких (искусственное дыхание);

- в случае необходимости приступить к непрямому массажу сердца.

Любой электроприбор должен быть немедленно обесточен в случае:

- возникновения угрозы жизни или здоровью человека;

- появления запаха, характерного для горящей изоляции или пластмассы;

- появления дыма или огня;

- появления искрения;

- обнаружения видимого повреждения силовых кабелей или коммутационных устройств.

Для защиты от поражения электрическим током используют СИЗ и СКЗ.

Средства коллективной защиты:

1. защитное заземление, зануление;
2. малое напряжение;
3. электрическое разделение сетей;
4. защитное отключение;
5. изоляция токоведущих частей;
6. оградительные устройства.

7. Использование щитов, барьеров, клеток, ширм, а также заземляющих и шунтирующих штанг, специальных знаков и плакатов.

Средства индивидуальной защиты:

1. Использование диэлектрических перчаток, изолирующих клещей и штанг, слесарных инструментов с изолированными рукоятками, указатели величины напряжения, калоши, боты, подставки и коврики.

4.1.5 Освещенность

Согласно СНиП 23-05-95 в аудитории, где происходит периодическое наблюдение за ходом производственного процесса при постоянном нахождении людей в помещении освещенность при системе общего освещения не должна быть ниже 300 Лк.

Правильно спроектированное и выполненное освещение обеспечивает высокий уровень работоспособности, оказывает положительное психологическое действие на человека и способствует повышению производительности труда.

На рабочей поверхности должны отсутствовать резкие тени, которые создают неравномерное распределение поверхностей с различной яркостью в поле зрения, искажает размеры и формы объектов различия, в результате повышается утомляемость и снижается производительность труда.

Расчёт общего равномерного искусственного освещения горизонтальной рабочей поверхности выполняется методом коэффициента светового потока, учитывающим световой поток, отражённый от потолка и стен. Длина помещения A = 5,333 м, ширина B = 4,5 м, высота h = 2,8 м. Высота рабочей поверхности над полом h_p = 1 м. Согласно СНиП 23-05-95 необходимо создать освещенность не ниже 150 лк., в соответствии с разрядом зрительной работы.

Площадь помещения:

$$S = A \times B = 5{,}333 \times 4{,}5 = 24 \text{ м}^2,$$

где A – длина, м;

B – ширина, м.

Коэффициент отражения свежепобеленных стен с окнами, без штор $\rho_{\text{С}} = 50\%$, свежепобеленного потолка $\rho_{\text{п}} = 70\%$. Коэффициент запаса, учитывающий загрязнение светильника, для помещений с малым выделением пыли равен $\text{К}_{\text{З}} = 1{,}5$. Коэффициент неравномерности для люминесцентных ламп $Z = 1{,}1$.

Выбираем лампу дневного света ЛД-40, световой поток которой равен $\Phi_{\text{ЛД}} = 2600$ Лм.

Выбираем светильники с люминесцентными лампами типа ШОД-2-40. Этот светильник имеет две лампы мощностью 40 Вт каждая, длина светильника равна 1228 мм, ширина – 284 мм.

Интегральным критерием оптимальности расположения светильников является величина λ, которая для люминесцентных светильников с защитной

решёткой лежит в диапазоне 1,1–1,3. Принимаем $\lambda = 1{,}1$, расстояние светильников от перекрытия (свес) h_c = 0,3 м.

Высота светильника над рабочей поверхностью определяется по формуле:

$$h = h_n - h_c,$$

где h_n - высота светильника над полом, высота подвеса;

h_c - высота рабочей поверхности над полом.

Наименьшая допустимая высота подвеса над полом для двухламповых светильников ШОД: h_n = 2,5 м.

Высота светильника над рабочей поверхностью определяется по формуле:

$$h = H - h_p - h_c = 2{,}8 - 1 - 0{,}3 = 1{,}5 \text{ м}.$$

Из формулы:

$$\Phi_л = \frac{E_H \cdot S \cdot К_з \cdot Z}{N \cdot \eta}$$

где E_H – нормируемая минимальная освещённость, при использовании ЭВМ и одновременной работе с документами должна быть не менее 300 лк;

S – площадь освещаемого помещения, м2;

$K_з$ – коэффициент запаса, учитывающий загрязнение светильника (источника света, светотехнической арматуры, стен и пр., т.е. отражающих поверхностей), наличие в атмосфере цеха дыма, пыли;

Z – коэффициент неравномерности освещения, отношение $E_{ср}/E_{min}$. Для люминесцентных ламп он равен 1,1;

N – число ламп в помещении;

η – коэффициент использования светового потока.

находим число ламп N:

$$N = \frac{E_H \cdot S \cdot К_з \cdot Z}{\Phi_л \cdot \eta}.$$

η определяем через индекс помещения по формуле:

$$i = \frac{A \cdot B}{h \cdot (A + B)} = \frac{5{,}333 \cdot 4{,}5}{1{,}65 \cdot (5{,}333 + 4{,}5)} = 1{,}48$$

Коэффициент использования светового потока, показывающий какая часть светового потока ламп попадает на рабочую поверхность, для светильников типа ШОД с люминесцентными лампами при $\rho_{\text{п}} = 70\%, \rho_{\text{С}} = 50\%$ и индексе помещения i = 1,48 равен η = 0,46.

Тогда $N = \frac{300 \cdot 24 \cdot 1{,}5 \cdot 1{,}1}{2600 * 0{,}46} = 9{,}9 \approx 10$ ламп.

Принимаем 12 ламп, при этом получается 6 светильников, т.е. 2 ряда по 3 светильника.

Из условий равномерности освещения определяем расстояния L_1 и $L_1/3$ и L_2 и $L_2/3$ по следующим уравнениям:

$5333 = 2 * L_1 + 2/3 * L_1 + 3 * 1228$; $L_1 = 618$ мм; $L_1/3 = 206$ мм;

$4500 = 2 * L_2 + 2/3 * L_2 + 3 * 284$; $L_2 = 1368$ мм; $L_2 = 456$ мм;

На рисунке изображен план помещения и размещения светильников с люминесцентными лампами.

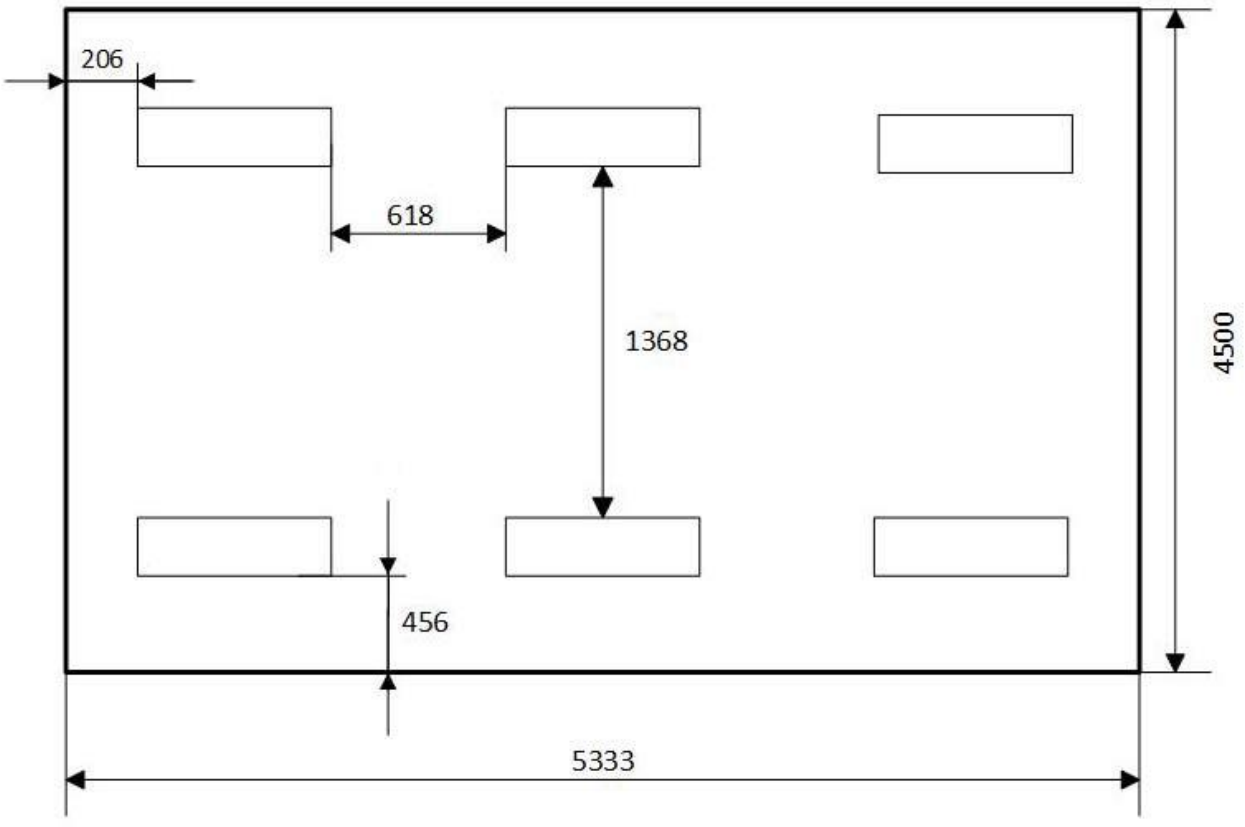

Рисунок 5 – План помещения и размещения светильников с люминесцентными лампами (размеры указаны в мм)

Потребный световой поток группы люминесцентных ламп светильника определяется по формуле:

$$Ф = \frac{300 \cdot 24 \cdot 1{,}5 \cdot 1{,}1}{12 \cdot 0{,}46} = 2\,152 \text{ лм}$$

Делаем проверку выполнения условия:

$$-10\% \leq \frac{Ф_{ЛД} - Ф_{П}}{Ф_{ЛД}} \cdot 100\% \leq 20\%;$$

$$\frac{Ф_{ЛД} - Ф_{П}}{Ф_{ЛД}} \cdot 100\% = \frac{2600 - 2\,152}{2\,600} \cdot 100\% = 17{,}23\%.$$

Таким образом, мы получили, что необходимый световой поток не выходит за пределы требуемого диапазона. Теперь рассчитаем мощность осветительной установки:

$$P = 12 * 40 = 480 Вт$$

4.1.6 Пожарная опасность

По взрывопожарной и пожарной опасности помещения подразделяются на категории А, Б, В1-В4, Г и Д, а здания на категории А, Б, В, Г и Д.

Согласно НПБ 105-03 лаборатория относится к категории В – горючие и трудно горючие жидкости, твердые горючие и трудно горючие вещества и материалы, вещества и материалы, способные при взаимодействии с водой, кислородом воздуха или друг с другом только гореть, при условии, что помещения, в которых находится, не относятся к категории наиболее опасных А или Б.

По степени огнестойкости данное помещение относится к 1-й степени огнестойкости по СНиП 2.01.02-85 (выполнено из кирпича, которое относится к трудносгораемым материалам).

Возникновение пожара при работе с электронной аппаратурой может быть по причинам как электрического, так и неэлектрического характера.

Причины возникновения пожара неэлектрического характера:

а) халатное неосторожное обращение с огнем (курение, оставленные без присмотра нагревательные приборы, использование открытого огня);

Причины возникновения пожара электрического характера: короткое замыкание, перегрузки по току, искрение и электрические дуги, статическое электричество и т. п.

Для локализации или ликвидации загорания на начальной стадии используются первичные средства пожаротушения. Первичные средства пожаротушения обычно применяют до прибытия пожарной команды.

Огнетушители водо-пенные (ОХВП-10) используют для тушения очагов пожара без наличия электроэнергии. Углекислотные (ОУ-2) и порошковые огнетушители предназначены для тушения электроустановок, находящихся под напряжением до 1000В. Для тушения токоведущих частей и электроустановок применяется переносной порошковый огнетушитель, например ОП-5.

В общественных зданиях и сооружениях на каждом этаже должно размещаться не менее двух переносных огнетушителей. Огнетушители следует располагать на видных местах вблизи от выходов из помещений на высоте не более 1,35 м. Размещение первичных средств пожаротушения в коридорах, переходах не должно препятствовать безопасной эвакуации людей.

Для предупреждения пожара и взрыва необходимо предусмотреть:

1. специальные изолированные помещения для хранения и разлива легковоспламеняющихся жидкостей (ЛВЖ), оборудованные приточно-вытяжной вентиляцией во взрывобезопасном исполнении - соответствии с ГОСТ 12.4.021-75 и СНиП 2.04.05-86;

2. специальные помещения (для хранения в таре пылеобразной канифоли), изолированные от нагревательных приборов и нагретых частей оборудования;

3. первичные средства пожаротушения на производственных участках (передвижные углекислые огнетушители ГОСТ 9230-77, пенные огнетушители ТУ 22-4720-80, ящики с песком, войлок, кошма или асбестовое полотно);

4. автоматические сигнализаторы (типа СВК-3 М 1) для сигнализации о присутствии в воздухе помещений довзрывных концентраций горючих паров растворителей и их смесей.

Аудитория полностью соответствует требованиям пожарной безопасности, а именно, наличие охранно-пожарной сигнализации, плана эвакуации, порошковых огнетушителей с поверенным клеймом, табличек с указанием направления к запасному (эвакуационному) выходу.

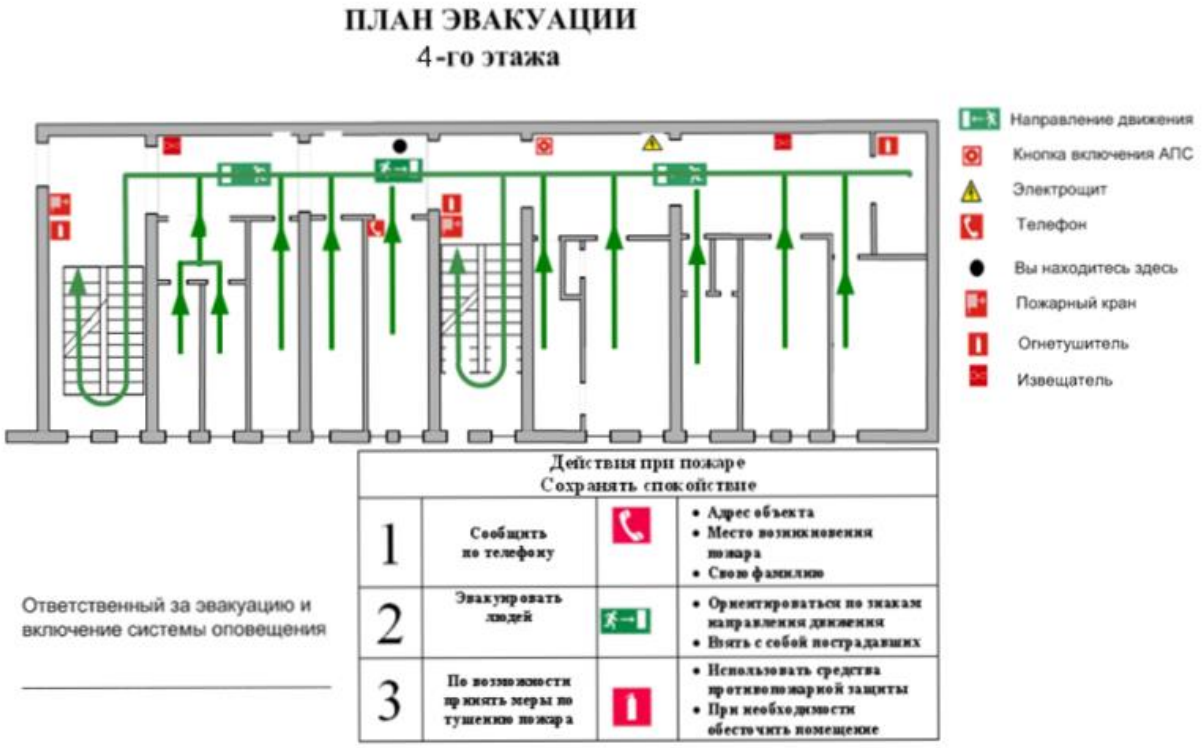

Рисунок 6 – План эвакуации

4.2 Экологическая безопасность

В компьютерах присутствует огромное количество компонентов, которые содержат токсичные вещества и представляют угрозу, как для человека, так и для окружающей среды.

К таким веществам относятся:

- свинец (накапливается в организме, поражая почки, нервную систему);
- ртуть (поражает мозг и нервную систему);

- никель и цинк (могут вызывать дерматит);

- щелочи (прожигают слизистые оболочки и кожу).

Поэтому компьютер требует специальных комплексных методов утилизации. В этот комплекс мероприятий входят:

- отделение металлических частей от неметаллических;

- металлические части переплавляются для последующего производства;

- неметаллические части компьютера подвергаются специальной переработке.

Исходя из сказанного выше перед планированием покупки компьютера необходимо:

- Побеспокоиться заранее о том, каким образом будет утилизирована имеющаяся техника, перед покупкой новой.

- Узнать, насколько новая техника соответствует современным эко-стандартам и примут ее на утилизацию после окончания срока службы.

Утилизировать оргтехнику, а не просто выбрасывать на «свалку» необходимо по следующим причинам:

Во-первых, в любой компьютерной и организационной технике содержится некоторое количество драгоценных металлов. Российским законодательством предусмотрен пункт, согласно которому все организации обязаны вести учет и движение драгоценных металлов, в том числе тех, которые входят в состав основных средств. За несоблюдение правил учета, организация может быть оштрафована на сумму от 20000 до 30000 руб. (согласно ст. 19.14. КоАП РФ);

Во-вторых, предприятие также может быть оштрафовано за несанкционированный вывоз техники или оборудования на «свалку».

Утилизируя технику, мы заботимся об экологии: количество не перерабатываемых отходов минимизируется, а такие отходы, как пластик, пластмассы, лом черных и цветных металлов, используются во вторичном производстве. Электронные платы, в которых содержатся драгметаллы, после

переработки отправляются на аффинажный завод, после чего чистые металлы сдаются в Госфонд, а не оседают на свалках.

Таким образом утилизацию компьютера можно провести следующим образом:

- отделить металлические детали от неметаллов;

- разделить углеродистые металлы от цветмета;

- пластмассовые изделия (крупногабаритные) измельчить для уменьшения объема;

- копир-порошок упаковать в отдельную упаковку, точно также, как и все проклассифицированные и измельченные компоненты оргтехники, и после накопления на складе транспортных количеств отправить предприятиям и фирмам, специализирующимся по переработке отдельных видов материалов.

Люминесцентные лампы утилизируют следующим образом. Не работающие лампы немедленно после удаления из светильника должны быть упакованы в картонную коробку, бумагу или тонкий мягкий картон, предохраняющий лампы от взаимного соприкосновения и случайного механического повреждения. После накопления ламп объемом в 1 транспортную единицу их сдают на переработку на соответствующее предприятие. Недопустимо выбрасывать отработанные энергосберегающие лампы вместе с обычным мусором, превращая его в ртутьсодержащие отходы, которые загрязняют ртутными парами.

4.3 Безопасность в чрезвычайных ситуациях

Природная чрезвычайная ситуация – обстановка на определенной территории или акватории, сложившейся в результате возникновения источника природной чрезвычайной ситуации, который может повлечь или повлек за собой человеческие жертвы, ущерб здоровью людей и (или) окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей.

Аудитория находится в городе Томске с континентально-циклоническим климатом. Природные явления (землетрясения, наводнения, засухи, ураганы и т. д.), в данном городе отсутствуют.

Возможными ЧС на объекте в данном случае, могут быть сильные морозы и диверсия.

Для Сибири в зимнее время года характерны морозы. Достижение критически низких температур приведет к авариям систем тепло- и водоснабжения, сантехнических коммуникаций и электроснабжения, приостановке работы. В этом случае при подготовке к зиме следует предусмотреть а) газобаллонные калориферы (запасные обогреватели), б) дизель или бензоэлектрогенераторы; в) запасы питьевой и технической воды на складе (не менее 30 л на 1 человека); г) теплый транспорт для доставки работников на работу и с работы домой в случае отказа муниципального транспорта. Их количества и мощности должно хватать для того, чтобы работа на производстве не прекратилась.

В аудитории наиболее вероятно возникновение чрезвычайных ситуаций (ЧС) техногенного характера.

Для предупреждения вероятности осуществления диверсии предприятие необходимо оборудовать системой видеонаблюдения, круглосуточной охраной, пропускной системой, надежной системой связи, а также исключения распространения информации о системе охраны объекта, расположении помещений и оборудования в помещениях, системах охраны, сигнализаторах, их местах установки и количестве. Должностные лица раз в полгода проводят тренировки по отработке действий на случай экстренной эвакуации.

Заключение

Проанализировав условия труда на рабочем месте, где была разработана работа, можно сделать вывод, что помещение удовлетворяет практически всем

необходимым нормам и в случае соблюдения техники безопасности и правил пользования компьютером работа в данном помещении не приведет к ухудшению здоровья.

Само помещение и рабочее место в нем удовлетворяет всем нормативным требованиям. Кроме того, действие вредных и опасных факторов сведено к минимуму, т.е. микроклимат, освещение и электробезопасность соответствуют требованиям, предъявленным в соответствующих нормативных документах.

Относительно рассмотренного вопроса об экологической безопасности можно сказать, что рассмотренная деятельность не представляет опасности окружающей среде.

Важно добавить, что монитор компьютера служит источником ЭМП – вредного фактора, который отрицательно влияет на здоровье работника при продолжительной непрерывной работе и приводит к снижению работоспособности. Поэтому во избежание негативного влияния на здоровье необходимо делать перерывы при работе с ЭВМ и проводить специализированные комплексы упражнений для глаз.

Заключение

В данной работе был проведен теоретический обзор алгоритма асимметричного шифрования с помощью эллиптических кривых (ECC), осуществлена программная реализация данного метода шифрования (совместно с симметричным), а также было произведено сравнение с наиболее распространенным методом асимметричного шифрования (методом RSA).

Сделаны замеры времени при создании пар ключей с разной длиной и времени реализации шифрования, используя эти ключи для текста с разным количеством символов.

В результате проделанной работы сделаны следующие основные выводы:

Время шифрования при гибридном шифровании практически не зависит от длины текста;

Время создания пар ключей ECC значительно меньше, чем время создания пар ключей RSA;

Размер пары ключей ECC гораздо меньше, чем пара ключей RSA с аналогичной «криптоустойчивостью».

Список публикаций

1. Адодин А.Н., Адодина К.С. О методе финансово-математической обработки данных для определения состояния промышленных отраслей [Текст] // Синергия наук. – 2022. - № 72 - Свободный доступ из сети Интернет. Режим доступа: http://synergy-journal.ru/archive/article6714

Список литературы

1. Мао В. Современная криптография: теория и практика. Перевод с английского // Вильямс – 2005 – 768 с.
2. Онацкий А.В., Йона Л.Г. Асимметричные методы шифрования. Модуль 2. Криптографические методы защиты информации в телекоммуникационных системах и сетях. Учебное пособие // ОНАС им. А.С.Попова – 2010. – 148 с.
3. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии // Горячая Линия – Телеком – 2001. – 120 с.
4. Эллиптическая криптография: теория [Электронный ресурс] // Режим доступа https://habr.com/ru/post/188958/, свободный. (дата обращения: 01.03.2022).
5. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. — Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы // КомКнига – 2006. – 328 с.
6. Петров А. А. Компьютерная безопасность. Криптографические методы защиты // ДМК Пресс – 2008. – 448 с.
7. Бородин Ю.В., Василевский М.В., Дашковский А.Г., Назаренко О.Б., Свиридов Ю.Ф., Чулков Н.А., Федорчук Ю.М. Безопасность жизнедеятельности: практикум // Изд-во Томского политехнического университета – 2009. – 101 с.
8. ГОСТ 54 30013-83. Электромагнитные излучения СВЧ. Предельно допустимые уровни облучения. Требования безопасности.
9. ГОСТ 12.4.154-85. ССБТ. Устройства экранирующие для защиты от электрических полей промышленной частоты.
10. ГН 2.2.5.1313-03. Предельно допустимые концентрации (ПДК) вредных веществ в воздухе рабочей зоны.
11. СанПиН 2.2.4/2.1.8.055-96. Электромагнитные излучения радиочастотного диапазона (ЭМИ РЧ).
12. СанПиН 2.2.4.548-96. Гигиенические требования к микроклимату производственных помещений.

13. СН 2.2.4/2.1.8.562-96. Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории жилой застройки.

14. ГОСТ 12.4.123-83. Средства коллективной защиты от инфракрасных излучений. Общие технические требования.

15. ГОСТ Р 12.1.019-2009. Электробезопасность. Общие требования и номенклатура видов защиты.

16. ГОСТ 12.1.030-81. Электробезопасность. Защитное заземление. Зануление.

17. ГОСТ 12.1.004-91. Пожарная безопасность. Общие требования.

18. ГОСТ 12.2.037-78. Техника пожарная. Требования безопасности

19. СанПиН 2.1.6.1032-01. Гигиенические требования к качеству атмосферного воздуха.

20. ГОСТ 30775-2001. Ресурсосбережение. Обращение с отходами. Классификация, идентификация и кодирование отходов.

21. СНиП 21-01-97. Противопожарные нормы.

22. ГОСТ 12.4.154. Система стандартов безопасности труда. Устройства экранирующие для защиты от электрических полей промышленной частоты. Общие технические требования, основные параметры и размеры.

Приложение А

(справочное)

Шифрование данных методом ECC

Студент:

Группа	ФИО	Подпись	Дата
0ВМ01	Адодин Андрей Николаевич		

Руководитель ВКР:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Крицкий О.Л.	к.ф-м.н., доцент		

Консультант – лингвист Отделение иностранных языков ШБИП

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель	Кабрышева О.П.			

1 Introduction

Humanity has moved into an era when the exchange of information that is valuable to intruders (for example, such as monetary transactions, private correspondence or the exchange of secret documents, etc.) is carried out using computer communications via the Internet.

In this regard, an urgent and promising topic in the XXI century is working with information, and its protection from being read by third-party users becomes the main priority.

The use of cryptography makes it possible to effectively solve the problem of information exchange through open networks. Most often, security is provided by encryption, using a digital signature or password authentication.

Cryptography is a broad field of knowledge about methods of ensuring confidentiality (the impossibility of reading information to outsiders), data integrity (the impossibility of imperceptibly changing information), authentication (verifying the authenticity of authorship or other properties of an object), encryption (data encoding). Modern cryptography has been developing since the 1970s.

Crypto algorithms are divided into two large groups: symmetric (both parties involved in data exchange have exactly the same keys for encrypting and decrypting data) and asymmetric (the parties involved use two different keys in a pair - public and secret (private)).

Asymmetric algorithms (with a public key) have become widespread, since there is no need to solve the most complex problem of exchanging secret keys. One of the well-known and widespread algorithms of asymmetric encryption is the ECC algorithm, which is based on the idea of using some mathematical problems in encryption.

The ECC algorithm is used in most Internet security systems to encrypt passwords or encryption keys to symmetric algorithms. It is very rarely used to encrypt

texts due to the fact that it can only encrypt messages that are smaller than the key itself.

The purpose of this work is to use the ECC algorithm for data encryption.

To achieve this goal, it is necessary to perform the following tasks:

- conduct a theoretical review of the encryption algorithm;
- make a choice of the software environment for the implementation of the algorithm;
- implement the algorithm in the selected environment;
- test the programmed encryption algorithm.

2 The theoretical part

2.1 Cryptographic systems

Cryptology deals with the problem of protecting information by converting it. Cryptology is divided into two areas - cryptography and cryptanalysis. Cryptography is engaged in the search and research of methods for transforming information in order to hide its content. The field of interests of cryptanalysis is the study of the possibility of decrypting information without knowing the keys.

The main directions of using cryptographic methods are: transmission of confidential information via communication channels (for example, e-mail), authentication of transmitted messages, storage of information (documents, databases) on encrypted media.

So, cryptography makes it possible to transform information in such a way that its reading (recovery) is possible only with knowledge of the key.

Encryption is the process of cryptographically converting a set of open messages into a set of closed messages.

Decryption is the process of cryptographically converting closed messages into open ones.

Decryption is the process of finding an open message corresponding to a given closed one with an unknown cryptographic transformation.

Encryption is a means of achieving the secrecy of information, consisting of two stages: encryption and decryption of the source data.

A private key is the secret information required to decrypt messages.

A public key is the public information required to encrypt messages, the result of encryption and cryptographic strength depends on the length of the key.

A cryptographic system is a family of $\boldsymbol{T}$ plaintext transformations. Members of this family are indexed, or denoted by the symbol *k*; the parameter *k* is usually called a key.

The transformation T_k is determined by the corresponding algorithm and the value of the key *k*.

The key is the information necessary for unhindered encryption and decryption of texts.

The key space $\boldsymbol{K}$ is a set of possible key values. Usually the key is a sequential series of letters of the alphabet.

Cryptosystems are divided into symmetric and asymmetric (or with a public key).

In symmetric cryptosystems, the same key is used for encryption and decryption.

Public key systems use two keys - public and private (secret), which are mathematically related to each other. The information is encrypted using a public key that is available to everyone, and decrypted using a private key known only to the recipient of the message.

2.2 Asymmetric Cryptosystems

Asymmetric systems are characterized by the fact that different keys are used for encryption and decryption, which are interconnected by some dependence. At the same time, this dependence is such that it is very difficult to establish one key, knowing the other, from a computational point of view.

One of the keys (for example, an encryption key) can be made publicly available, and in this case the problem of obtaining a shared secret key for communication disappears. If you make the decryption key publicly available, then on the basis of the received system, you can build an authentication system for transmitted messages.

Since in most cases one key from a pair is made publicly available, such systems are also called public-key cryptosystems.

The public key cryptosystem is defined by three algorithms: key generation, encryption and decryption. The key generation algorithm is open, anyone can give him a random string r of the appropriate length and get a pair of keys (k_1, k_2). One of the keys (for example, k_1) is published, it is called public, and the second, called secret, is kept secret. The encryption algorithms E_{k_1} and decryption D_{k_2} are such that for any plaintext m D_{k_2} (E_{k_1} (m)) = m.

2.3 Elliptic curve

An elliptic curve is a set of points described by the Weierstrasse equation:

$$y^2 = x^3 + ax + b$$

Examples of elliptic curve graphs:

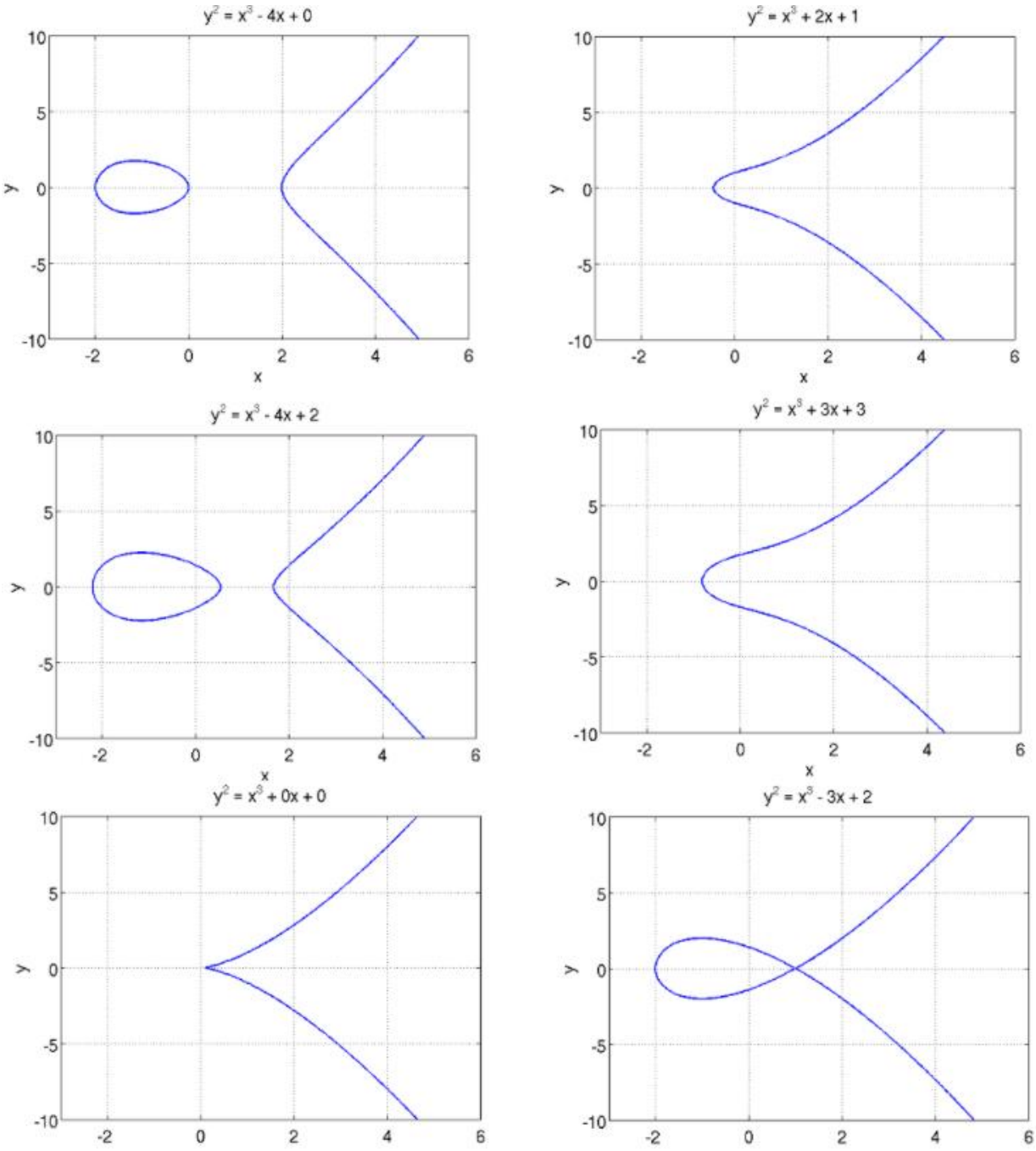

Figure 1 – Examples of elliptic curve graphs

The elliptic curves presented in the first four graphs are called smooth, the two lower curves belong to the so-called singular elliptic curves. For smooth elliptic curves , the following inequality holds:

$$4a^3 + 27b^2 \neq 0$$

Whereas for singular curves this condition is not fulfilled.

Singular curves cannot be used in EDS (electronic digital signature) schemes, since using singular curves can significantly reduce the durability of the EDS scheme.

Arithmetic operations in elliptic cryptography are performed on the points of the curve. The main operation is "addition". The addition of two points is easy to represent graphically:

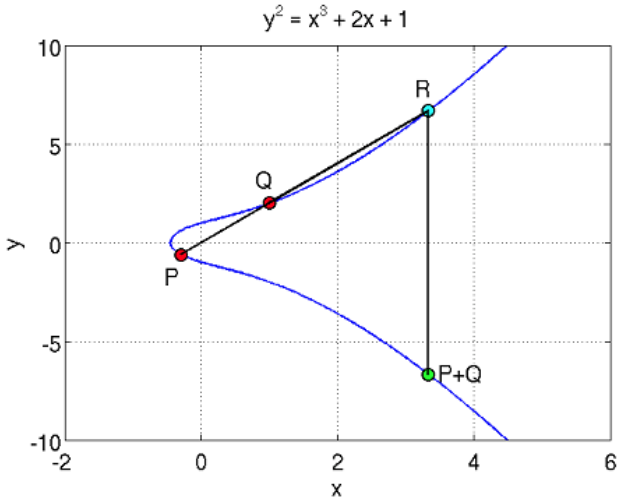

Figure 2 - The addition of two points in elliptical cryptography

As can be seen from the figure, to add points P and Q, it is necessary to draw a straight line between them, which will necessarily intersect the curve at some third point R. Let's reflect the point R relative to the horizontal coordinate axis and get the desired point P+Q.

The algebraic representation of Addition is given by the following rule: the sum of three nonzero points P, Q and R lying on the same line will be equal to P + Q + R = 0.

Let 's write the addition of two points in the form of a formula:

$$P + Q = -R$$

Let the coordinates of the point P be (Xp, Yp), and the coordinates of the point Q, respectively (Xq, Yq).

Calculate

$$\alpha = \frac{y_Q - y_P}{x_Q - x_P}$$

and then the coordinates of the point P+Q will be equal:

$$x_{P+Q} = \alpha^2 - x_P - x_Q$$

$$y_{P+Q} = -y_P + \alpha(x_P - x_R)$$

2.4 Elliptic Curves in Cryptography

All the curves discussed above refer to elliptic curves over the real numbers. And this leads to the rounding problem. That is, using curves over real numbers, we will not be able to get a bijection between the source text and the encrypted data. In order not to round, only curves over finite fields are used in cryptography. This means that an elliptic curve refers to a set of points whose coordinates belong to a finite field.

In cryptography, two types of elliptic curves are considered: over a finite field Z_p, a residue ring modulo a prime number. And over the field $GF(2^m)$ is a binary finite field. Elliptic curves over the $GF(2^m)$ field have one important advantage: field elements can be easily represented as n-bit code words, this allows increasing the speed of hardware implementation of elliptic algorithms.

All mathematical operations on elliptic curves over a finite field are performed according to the laws of the "finite field" over which the elliptic curve is constructed. That is, to calculate, for example, the sum of two points of the curve E over the residue ring Z_p, all operations are performed modulo the number P.

However, if we add two identical elements from a binary finite field, we get 0 as a result, since addition occurs modulo 2. This means that the characteristic of such a field is 2. But an elliptic curve of the form

$$y^2 = x^3 + ax + b,$$

the characteristic 2 or 3 described over the field becomes singular, and as already noted above, it is impossible to use singular curves in cryptography.

Therefore, curves of the form are used over a binary finite field: $y^2 + xy = x^3 + ax^2 + b, \quad b \neq 0$

Another important concept of elliptic cryptography is the order of the elliptic curve, which shows the number of points of the curve over a finite field.

Hasse's theorem states that if N is the number of points of a curve defined over a field Zq with q elements then the equality holds:

$$|N - (q + 1)| \leq 2\sqrt{q}$$

Since the binary finite field $GF(2^n)$consists of 2^n elements , we can say that the order of the curve $E_{2^n}(a, b)$ is $2^n + 1 - t$, where $|t| \leq \sqrt{2^n}$.

The following definition is associated with the number t: an elliptic curve over a binary finite field is called supersingular if *t* is divided by the characteristic of the field (in the case of a binary field, the characteristic is 2) without remainder.

2.5 Cryptography on elliptic curves

The points of an elliptic curve over a finite field represent a group. And as noted above, the addition operation is defined for this group. Accordingly, we can represent the multiplication of the number k by the point G as G+G+...+G with k terms.

Suppose there is a message M, represented as an integer. You can encrypt it using the expression C=M*G. The question is, how difficult is it to recover M knowing

the parameters of the curve E(a,b), ciphertext C and point G. This problem is called a discrete logarithm on an elliptic curve and has no quick solution. Moreover, it is believed that the discrete logarithm problem on an elliptic curve is more difficult to solve than the discrete logarithm problem in finite fields.

The fastest methods developed for finite fields are useless in the case of elliptic curves. So to solve a discrete logarithm, there are sufficiently fast algorithms with complexity $O(\exp(c(\log p \log\log p)^d))$, where c and d are some constants, and p is the size of the field. Such algorithms are called subexponential and make it relatively easy to open a discrete logarithm in a finite field, if the field size is not chosen very large, on the order of 2^{1024}.

At the same time, the fastest methods for solving a discrete logarithm on an elliptic curve have complexity $o(\sqrt{q})$, where q is the number of points of the elliptic curve. Thus, to ensure the level of stability in 2^{80} operations, it is necessary that $q=2^{160}$. In order to obtain a similar level of complexity when calculating a discrete logarithm in a finite field, a field of the order $q=2^{1024}$ is needed.

It should be noted that since the power of computer technology is constantly increasing, the value of q will constantly increase. But since the graphs of the functions $o(\sqrt{q})$ and $O(\exp(c(\log p \log\log p)^d))$ differ sharply from each other, q will grow much slower in the group of points of an elliptic curve than in an arbitrary finite field.

Based on all of the above, we can highlight the main advantages of elliptic cryptography:

1. Much shorter key length compared to "classical" asymmetric cryptography.

2. The speed of elliptic algorithms is much higher than that of classical ones. This is explained both by the size of the field and by the use of a binary finite field structure that is closer to computers.

3. Due to the small key length and high speed of operation, algorithms of asymmetric cryptography on elliptic curves can be used in smart cards and other devices with limited computing resources.

The disadvantages of elliptic cryptography are:

1. All the advantages of elliptic cryptography follow from one specific fact: there are no subexponential algorithms for solving the problem of discrete logarithm on elliptic curves. This allows you to reduce the key length and increase performance. However, if such algorithms appear, it will mean the collapse of elliptical cryptography.

2. Elliptical cryptography is very difficult. This is a huge number of subtleties that need to be taken into account, starting with the choice of an elliptic curve and ending with the generation of keys. With a massive transition to elliptical cryptography, there will necessarily be a large number of errors and vulnerabilities that have already been worked out for more familiar methods.

3 Practical part

The work will be performed on a PC with the following characteristics: intel i5-4670 processor (6 MB of cache memory, clock speed up to 3.80 GHz), other characteristics are not fundamental.

Hybrid encryption will be used to encrypt long texts, which is a common way to get the speed of symmetric-key cryptosystems combined with the advantages of ECC public and private keys.

In my work, I will use encryption keys with different lengths, and also make a comparison with the most common encryption method, the RSA method.

The hybrid scheme works as follows: for a symmetric algorithm (3DES, IDEA, AES or any other), a random session key is generated. Such a key usually has a size

from 128 to 512 bits (depending on the algorithm). Then this symmetric algorithm is used to encrypt the message, which will allow you to encrypt a message with a length exceeding the block length. As for the random key itself, it must be encrypted using the public key of the recipient of the message, and it is at this stage that the ECC public key cryptosystem is used. Since the session key is short, its encryption takes a little time. However, in my work I will also use long keys for session keys to see the speed of the algorithms.

Encrypting a set of messages using an asymmetric algorithm is a computationally more complex task, so it is preferable to use symmetric encryption here. Then it is enough to send a message encrypted with a symmetric algorithm, as well as the corresponding key in encrypted form. The recipient first decrypts the key using his secret key, and then uses the received key to receive the entire message.

To implement the task of encrypting and decrypting text, I will use a program written in Python and using the PyCryptodome and tinyec libraries. Also compare ECC encryption with RSA encryption.

```
1:  # RSA Key Generation Program
2:
3:  from Cryptodome.PublicKey import RSA
4:
5:  # Generate a private and public key:
6:  key = RSA.generate(2048) #bits длина ключа 1024, 2048, 3072, 7680
7:  private_key = key.export_key()
8:  file_out = open("private.pem", "wb")
9:  file_out.write(private_key)
10: file_out.close()
11:
12: public_key = key.publickey().export_key()
13: file_out = open("receiver.pem", "wb")
14: file_out.write(public_key)
15: file_out.close()
```

```
# ECC Key Generation Program
from Cryptodome.PublicKey import ECC
import time

start = time.time()

# Generate a private and public key:
key = ECC.generate(curve='P-256') # длина ключа 192, 224, 256, 384, 521

private_key = key.export_key(format='PEM')
file_out = open("private.pem", "wt") #wb
file_out.write(private_key)
file_out.close()

public_key = key.public_key().export_key(format='PEM')
print("public_key=",public_key)

file_out = open("receiver.pem", "wt")
file_out.write(public_key)
file_out.close()

end = time.time()
print("Время выполнения генерации = {:.{}f}".format(end - start, 3), " сек")
```

The ECC key pair creation time, similar in RSA cryptographic protection, is performed much faster than the RSA method, which gives us greater performance with similar protection.

Table 1. Comparison of key pair generation time for different encryption methods:

RSA Key Size			**ECC Key Size**
1024	0.151	0.082	160
2048	1.864	0.085	224
3072	14.256	0.082	256
7680	104.973	0.100	384
15360	859.899	0.102	521

Note that there is no linear relationship between the sizes of the RSA and ECC keys (in other words: if we double the size of the RSA key, we do not need to double

the size of the ECC key). The table tells us that ECC not only uses less memory, but key generation in it is much faster.

The PyCryptodome module does not provide the ability to encrypt and decrypt text. Therefore, we will use this module partially to encrypt the text in a symmetric AES way, and the ECC asymmetric encryption key itself and the encryption/decryption of the text will be carried out using the Tinyec module.

```
#Program for encrypting and decrypting text using the ECC method. Input method from file
from tinyec import registry
from Cryptodome.Cipher import AES
import hashlib, secrets, binascii, sys
import time

def encrypt_AES_GCM(msg, secretKey):
    aesCipher = AES.new(secretKey, AES.MODE_GCM)
    ciphertext, authTag = aesCipher.encrypt_and_digest(msg)
    return (ciphertext, aesCipher.nonce, authTag)

def decrypt_AES_GCM(ciphertext, nonce, authTag, secretKey):
    aesCipher = AES.new(secretKey, AES.MODE_GCM, nonce)
    plaintext = aesCipher.decrypt_and_verify(ciphertext, authTag)
    return plaintext

def ecc_point_to_256_bit_key(point):
    sha = hashlib.sha256(int.to_bytes(point.x, 64, 'big')) #32 если кривая до 256, 64 для
384 и 512
    sha.update(int.to_bytes(point.y, 64, 'big'))
    return sha.digest()

curve = registry.get_curve('brainpoolP256r1')
#'brainpoolP160r1','brainpoolP224r1','brainpoolP256r1','brainpoolP384r1','brainpoolP512r1'

def encrypt_ECC(msg, pubKey):
    ciphertextPrivKey = secrets.randbelow(curve.field.n)
    sharedECCKey = ciphertextPrivKey * pubKey
    secretKey = ecc_point_to_256_bit_key(sharedECCKey)
    ciphertext, nonce, authTag = encrypt_AES_GCM(msg, secretKey)
    ciphertextPubKey = ciphertextPrivKey * curve.g
    return (ciphertext, nonce, authTag, ciphertextPubKey)

def decrypt_ECC(encryptedMsg, privKey):
    (ciphertext, nonce, authTag, ciphertextPubKey) = encryptedMsg
    sharedECCKey = privKey * ciphertextPubKey
    secretKey = ecc_point_to_256_bit_key(sharedECCKey)
    plaintext = decrypt_AES_GCM(ciphertext, nonce, authTag, secretKey)
    return plaintext

file_in = open("file.txt", "rb") #text utf-8
msg = file_in.read()
file_in.close()
#print("Оригинальный текст: ", msg.decode('utf-8'))
size_msg = sys.getsizeof(msg)
print("Размер текста = ",size_msg, "бит")

privKey = secrets.randbelow(curve.field.n)
pubKey = privKey * curve.g
print("Открытый ключ =", pubKey)
print("Закрытый ключ =", privKey)

start = time.time()
encryptedMsg = encrypt_ECC(msg, pubKey)
#print("Зашифрованный текст:", encryptedMsg)

encryptedMsgObj = {
    'ciphertext': binascii.hexlify(encryptedMsg[0]),
    'nonce': binascii.hexlify(encryptedMsg[1]),
    'authTag': binascii.hexlify(encryptedMsg[2]),
    'ciphertextPubKey': hex(encryptedMsg[3].x) + hex(encryptedMsg[3].y % 2)[2:]
}
#print("Зашифрованный текст:", encryptedMsgObj)
decryptedMsg = decrypt_ECC(encryptedMsg, privKey)
#print("Расшифрованный текст:", decryptedMsg.decode('utf-8'))
end = time.time()
print("Время выполнения шифрования текста = {:.{}f}".format(end - start, 3), " сек")
```

As the encrypted text, we will use the text of the work of L.N. Tolstoy "War and Peace", the number of characters will change to determine the speed of work with each pair of encryption keys.

Encrypted text:

```
-Eh bien, mon prince. Genes et Lucques ne sont plus que des apanages, des поместья, de la famille Buonaparte. Non, je vous previens, que si vous ne me dites pas, que nous avons la guerre, si vous vous permettez encore de pallier toutes les infamies, toutes les atrocites de cet Antichrist (ma parole, j'y crois) - je ne vous connais plus, vous n'etes plus mon ami, vous n'etes plus мой верный раб, comme vous dites. [  Ну, что, князь, Генуа и Лукка стали не больше, как поместьями фамилии Бонапарте. Нет, я вас предупреждаю, если вы мне не скажете, что у нас война, если вы еще позволите себе защищать все гадости, все ужасы этого Антихриста (право, я верю, что он Антихрист) - я вас больше не знаю, вы уж не друг мой, вы уж не мой верный раб, как вы говорите.]  Ну, здравствуйте, здравствуйте. Je vois que je vous fais peur, [  Я вижу, что я вас пугаю,]  садитесь и рассказывайте. <…>
```

What we get in the file containing the encrypted text:

```
b79cfebd46b7f683fea42672cc081d413503182d940d04fe80941d9fecd8eaee3ab09e35b4e876dc535af272fa419
f53c877edf29fc3177c5146b37282f9a9c25bc26449102034ca4d7f0df113f87260e1702cc72f062f0f26c2aba2bf
0f150fb05d45c3541c944e31aefeedc5245d599ac7a75abd122e68401b56901cbac151e86c9a0d3618db6fa43c44c
5dab3732c908a65053044ceabe051d1a04105b65a7b144e29814fbf08aca51e9f50b2bf6ff2e3f55996bf73b81ee2
28cef54f96bfefa853e0f2b4df7cd3079d70c66775a20d3c864f3aa221ab400b5b644724b87f7ec6c1b498af57c49
82adcdc005223fe9428e73d15965789e9c209993586dcfe62dddedc1676079a9124ef29f5b03dd30924d227fa944e
f5313f32c47b6bb957342ca1e2a0ffb94427858d7b93a7d230f6fc40b0880d1dfb16197032c7f0a81d8ef86cf8fd5
1596a27a8cd9cc453467b7f80cd1e99891e4216499d7121dcc51a815d5900fdc57221aaa9abc5f2b8500d9a39472d
3c9491e72f5a7cd67007e1a3d06d32078b1b02997568293f2cc2c2067ba66c31a6ddad6032df2c799eebd31873a40
6e3a98bc664ae4e48f63b38424030db35a4bc3a34c6bd9fb8df389e2f92b5e6c9c00219d0d54a34056966812 <…>
```

When executing this program code for encrypting text and decrypting this text, we have the following time performance indicators, which are listed in Table 2.

In the same table, we will enter data on encryption and decryption of text using the RSA method, using generated keys, since their generation takes a considerable time. The program text is as follows

```
#Program for encrypting and decrypting text using the RSA method. Input method from file
from Cryptodome.PublicKey import RSA
from Cryptodome.Random import get_random_bytes
from Cryptodome.Cipher import AES, PKCS1_OAEP
import time
import math, sys

#entering encrypted text from a file:
file_in = open("file.txt", "rb")
data = file_in.read()
file_in.close()
#print("текст для шифрования:", data.decode("utf-8"))

size_data = sys.getsizeof(data)
print("Размер текста = ",size_data, "бит")

file_out = open("encrypted_data.bin", "wb")

start = time.time()

recipient_key = RSA.import_key(open("receiver.pem").read())
session_key = get_random_bytes(16) #AES_128
#print(session_key)

# Encrypt the session key with the public RSA key
cipher_rsa = PKCS1_OAEP.new(recipient_key)
enc_session_key = cipher_rsa.encrypt(session_key)

# Encrypt the data with the AES session key
cipher_aes = AES.new(session_key, AES.MODE_EAX)
ciphertext, tag = cipher_aes.encrypt_and_digest(data)
[ file_out.write(x) for x in (enc_session_key, cipher_aes.nonce, tag, ciphertext) ]
file_out.close()


# Text decryption

file_in = open("encrypted_data.bin", "rb")

private_key = RSA.import_key(open("private.pem").read())

enc_session_key, nonce, tag, ciphertext = \
   [ file_in.read(x) for x in (private_key.size_in_bytes(), 16, 16, -1) ]

# Decrypt the session key with the private RSA key
cipher_rsa = PKCS1_OAEP.new(private_key)
session_key = cipher_rsa.decrypt(enc_session_key)

# Decrypt the data with the AES session key
cipher_aes = AES.new(session_key, AES.MODE_EAX, nonce)
data = cipher_aes.decrypt_and_verify(ciphertext, tag)

end = time.time()
print("Время выполнения шифрования текста = {:.{}f}".format(end - start, 3), " сек")

#print(data.decode("utf-8"))
```

Table 2. Data on the number of characters of the encrypted text and execution time:

	2^{16} = 65536	2^{18} = 262144	2^{20} = 1048576	2^{22} = 4194304
RSA-1024	0.034	0.035	0.043	0.069
ECC-160	0.038	0.039	0.042	0.058
RSA-2048	**0.073**	**0.075**	**0.083**	**0.108**
ECC-224	0.075	0.075	0.085	0.095
RSA-3072	0.145	0.154	0.157	0.184
ECC-256	**0.098**	**0.100**	**0.107**	**0.118**
RSA-7680	1.113	1.121	1.123	1.153
ECC-384	0.244	0.246	0.246	0.248
RSA-15360	7.108	7.184	7.167	7.153
ECC-512	0.444	0.452	0.456	0.474

We see that the speed of text encryption practically does not depend on the number of source characters, and the execution time of encryption using the hybrid method (ECC-AES) depends on the speed of key generation for asymmetric encryption. Encrypting a small session key using AES and encrypting text using a symmetric key takes a small amount of time.

4 Conclusion

In this paper, a theoretical review of the ECC asymmetric encryption algorithm was carried out, as well as its main advantages and disadvantages were considered, and a comparison was made with asymmetric encryption by the RSA method.

Its software implementation was carried out, performance testing was carried out and time measurements were made when creating key pairs with different lengths and implementing encryption using these keys for text with different numbers of characters.

Due to the lack of an effective method for the problem of discrete logarithm of numbers, 256-bit keys generated once (which are now the most common) can be used for several years, and maybe decades. Since at the moment it was possible to solve the problem of discrete logarithm of an elliptic curve with an interval of 114 bits on the secp256k1 curve, in other words, only 114-bit curves have been successfully hacked to date.

List of literature:

1. Barichev S. G., Goncharov V. V., Serov R. E. Fundamentals of modern cryptography // Hotline – Telecom – 2001. – 120 p.

2. Mao V. Modern cryptography: theory and practice. Translated from English // Williams – 2005 – 768 p.

3. Onatsky A.V., Yona L.G. Asymmetric encryption methods. Module 2. Cryptographic methods of information protection in telecommunication systems and networks. Textbook // ONAS named after A.S.Popov – 2010. – 148 p.

4. Petrov A. A. Computer security. Cryptographic methods of protection // DMK Press - 2008. – 448 p.

5. Elliptical cryptography: theory [Electronic resource] // Access mode habr.com/ru/post/188958/, free. (accessed: 01.06.2022).

Приложение Б

(Обязательное)

Программа генерации ключей RSA

```
from Cryptodome.PublicKey import RSA #для создания ключей

#Сгенерируем закрытый и открытый ключ:
key = RSA.generate(2048) #bits длина ключа 1024, 2048, 3072, 7680
private_key = key.export_key()
file_out = open("private.pem", "wb")
file_out.write(private_key)
file_out.close()

public_key = key.publickey().export_key()
file_out = open("receiver.pem", "wb")
file_out.write(public_key)
file_out.close()
```

Приложение В

(Обязательное)

Программа генерации ключей ECC

```
from Cryptodome.PublicKey import ECC #для создания ключей
import time

start = time.time()

#Сгенерируем закрытый и открытый ключ:
key = ECC.generate(curve='P-256') # длина ключа 192, 224, 256, 384, 521

private_key = key.export_key(format='PEM')
file_out = open("private.pem", "wt") #wb
file_out.write(private_key)
file_out.close()

public_key = key.public_key().export_key(format='PEM')
print("public_key=",public_key)

file_out = open("receiver.pem", "wt")
file_out.write(public_key)
file_out.close()

end = time.time()
print("Время выполнения генерации = {:.{}f}".format(end - start, 3), " сек")
```

Приложение Г

(Обязательное)

Программа шифрования и расшифрования текста методом ECC. Метод ввода из файла

```
from tinyec import registry
from Cryptodome.Cipher import AES
import hashlib, secrets, binascii, sys
import time

def encrypt_AES_GCM(msg, secretKey):
    aesCipher = AES.new(secretKey, AES.MODE_GCM)
    ciphertext, authTag = aesCipher.encrypt_and_digest(msg)
    return (ciphertext, aesCipher.nonce, authTag)

def decrypt_AES_GCM(ciphertext, nonce, authTag, secretKey):
    aesCipher = AES.new(secretKey, AES.MODE_GCM, nonce)
    plaintext = aesCipher.decrypt_and_verify(ciphertext, authTag)
    return plaintext

def ecc_point_to_256_bit_key(point):
    sha = hashlib.sha256(int.to_bytes(point.x, 64, 'big')) #32 если кривая до 256, 64 для 384 и 512
    sha.update(int.to_bytes(point.y, 64, 'big'))
    return sha.digest()

curve = registry.get_curve('brainpoolP256r1')
#'brainpoolP160r1','brainpoolP224r1','brainpoolP256r1','brainpoolP384r1','brainpoolP512r1'

def encrypt_ECC(msg, pubKey):
    ciphertextPrivKey = secrets.randbelow(curve.field.n)
    sharedECCKey = ciphertextPrivKey * pubKey
    secretKey = ecc_point_to_256_bit_key(sharedECCKey)
    ciphertext, nonce, authTag = encrypt_AES_GCM(msg, secretKey)
    ciphertextPubKey = ciphertextPrivKey * curve.g
    return (ciphertext, nonce, authTag, ciphertextPubKey)

def decrypt_ECC(encryptedMsg, privKey):
    (ciphertext, nonce, authTag, ciphertextPubKey) = encryptedMsg
    sharedECCKey = privKey * ciphertextPubKey
    secretKey = ecc_point_to_256_bit_key(sharedECCKey)
    plaintext = decrypt_AES_GCM(ciphertext, nonce, authTag, secretKey)
    return plaintext

file_in = open("file.txt", "rb") #текст в формате utf-8
msg = file_in.read()
file_in.close()
#print("Оригинальный текст: ", msg.decode('utf-8'))
size_msg = sys.getsizeof(msg)
print("Размер текста = ",size_msg, "бит")

privKey = secrets.randbelow(curve.field.n)
pubKey = privKey * curve.g
print("Открытый ключ =", pubKey)
print("Закрытый ключ =", privKey)

```

```
start = time.time()
encryptedMsg = encrypt_ECC(msg, pubKey)
#print("Зашифрованный текст:", encryptedMsg)

encryptedMsgObj = {
    'ciphertext': binascii.hexlify(encryptedMsg[0]),
    'nonce': binascii.hexlify(encryptedMsg[1]),
    'authTag': binascii.hexlify(encryptedMsg[2]),
    'ciphertextPubKey': hex(encryptedMsg[3].x) + hex(encryptedMsg[3].y % 2)[2:]
}
#print("Зашифрованный текст:", encryptedMsgObj)

decryptedMsg = decrypt_ECC(encryptedMsg, privKey)
#print("Расшифрованный текст:", decryptedMsg.decode('utf-8'))
end = time.time()
print("Время выполнения шифрования текста = {:.{}f}".format(end - start, 3), " сек")
```

Приложение Д

(Обязательное)

Программа шифрования и расшифрования текста методом RSA. Метод ввода из файла

```
from Cryptodome.PublicKey import RSA #для создания ключей
from Cryptodome.Random import get_random_bytes #для создания сессионного ключа
from Cryptodome.Cipher import AES, PKCS1_OAEP #
import time
import math, sys

#ввод шифруемого текста из файла:
file_in = open("file.txt", "rb")
data = file_in.read()
file_in.close()
#print("текст для шифрования:", data.decode("utf-8"))

size_data = sys.getsizeof(data)
print("Размер текста = ",size_data, "бит")

file_out = open("encrypted_data.bin", "wb")
start = time.time()

recipient_key = RSA.import_key(open("receiver.pem").read())
session_key = get_random_bytes(16) #AES_128
#print(session_key)

# Encrypt the session key with the public RSA key
cipher_rsa = PKCS1_OAEP.new(recipient_key)
enc_session_key = cipher_rsa.encrypt(session_key)

# Encrypt the data with the AES session key
cipher_aes = AES.new(session_key, AES.MODE_EAX)
ciphertext, tag = cipher_aes.encrypt_and_digest(data)
[ file_out.write(x) for x in (enc_session_key, cipher_aes.nonce, tag, ciphertext) ]
file_out.close()

#Программа расшифровки текста
file_in = open("encrypted_data.bin", "rb")

private_key = RSA.import_key(open("private.pem").read())

enc_session_key, nonce, tag, ciphertext = \
   [ file_in.read(x) for x in (private_key.size_in_bytes(), 16, 16, -1) ]

# Decrypt the session key with the private RSA key
cipher_rsa = PKCS1_OAEP.new(private_key)
session_key = cipher_rsa.decrypt(enc_session_key)

# Decrypt the data with the AES session key
cipher_aes = AES.new(session_key, AES.MODE_EAX, nonce)
data = cipher_aes.decrypt_and_verify(ciphertext, tag)

end = time.time()
print("Время выполнения шифрования текста = {:.{}f}".format(end - start, 3), " сек")

#print(data.decode("utf-8"))
```