|  |
| --- |
| **МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ** |
| **ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО (ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»**  **(ФГБОУ ВО «МГУТУ ИМ. К.Г. РАЗУМОВСКОГО (ПКУ)»)** |
|  |
| **УНИВЕРСИТЕТСКИЙ КОЛЛЕДЖ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ** |

|  |
| --- |
| **КУРСОВОЙ ПРОЕКТ** |
|  |
| по междисциплинарному курсу: МДК.02.02. Технология разработки и защиты баз данных |
|  |
| на тему: Разработка обучающей программы по теме «Криптография данных» |
|  |
| студента группы 090203-9o-20/1  специальности 09.02.03 Программирование в компьютерных системах |
| Смирнова Константина Вадимовича |

|  |  |  |
| --- | --- | --- |
| Студент |  | К.В. Смирнов |
| Руководитель курсового проекта |  | Е.А. Ларионова |
| Председатель ПЦК специальности 09.02.03 Программирование в компьютерных системах |  | А.И. Глускер |

|  |  |  |
| --- | --- | --- |
| Дата защиты «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2023 г. | | |
| Оценка:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| Заведующий отделением № 1 |  | И.А. Миланова | |

Москва

2023

В курсовой работе минимум 30 страниц

Минимум 10 источников (3 книги)

Курсовая работа

**Введение**

Современность сложно представить без использования компьютеров и интернета. Информационные технологии развивались с середины прошлого века вплоть до сегодняшних дней. Распространение персональных компьютеров и смартфонов достигло того, что люди используют устройства не только во время работы, но и в обычной жизни для отдыха, развлечений, общения на расстоянии и обучения.

В следствие взаимодействия людей как с компьютерами, так и между собой по средству соцсетей, данные пользователей, которые используются приложениями, сохраняются в базах данных для дальнейшего использования. Но с ростом объема передаваемой информации возрастает угроза утечки или взлома.

В мире, где информация является одним из самых ценных ресурсов, шифрование данных становится все более актуальной темой. Криптография – это наука, которая занимается защитой информации путем шифрования и дешифрования. К методам криптографии относятся: обеспечение [конфиденциальности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C), [целостности данных](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8), [аутентификации](https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F), [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5). Криптография используется в сферах начиная от финансовых транзакций до военных коммуникаций.

Основная цель проекта - Разработка обучающей программы по теме «Криптография данных» представляющей из себя ознакомление с основными принципами криптографии данных, методами шифрования и дешифрования информации, а приложение для реализации данного материала.

.

В этапы разработки проекта входят:

* Анализ предметной области
* Выбор средств разработки
* Создание и заполнение базы данных
* Разработка приложения
* Разработка документации

В ходе анализа предметной области были изучены основные алгоритмы шифрования, такие как симметричное и асимметричное шифрование. Рассмотрены основные аспекты шифрования. Проведен обзор существующих программ по данной теме для реализации собственного приложения.

В результате прохождения обучения, в приложении можно будет получить знания и навыки, необходимые для защиты своих данных и данных клиентов. Это поможет повысить уровень безопасности бизнеса и укрепить доверие со стороны клиентов.

Основная часть

1. исследование предметной области (что это вообще)
2. обзор аналогов (примеры программ для обучения криптографии)
3. анализ и выбор (анализ выш перечис и выбор как делать самому)
4. среды разработки (c# wpf приложение)
5. анализ и выбор инструментов разработки. (c# wpf приложение)

В разделе «Анализ и выбор инструментов разработки» необходимо

будет описать все используемые языки программирования и инструменты,

участвующие в разработке программного обеспечения. Если при разработке

были использованы какие-либо библиотеки, API и другие подобные

инструменты, то их рекомендуется описать в отдельном разделе, например

«Используемые библиотеки».

// В конце каждого раздела должны содержаться выводы по изложенному

материалу.

1. Исследование предметной области:

В разделе "Исследование предметной области" проводится более глубокий анализ темы криптографии данных и смежных областей, необходимых для успешной разработки обучающей программы.

1.1 Основы криптографии данных:

1.1.1 Определение криптографии данных и ее роль в современном мире.

1.1.2 Основные понятия, такие как шифрование, дешифрование, ключи, алгоритмы шифрования, криптографические протоколы и стандарты.

1.1.3 Классификация криптографии: симметричная и асимметричная криптография.

1.1.4 Примеры применения криптографии в информационной безопасности, банковском секторе, здравоохранении и других отраслях.

1.2 Методы обучения криптографии данных:

1.2.1 Обзор существующих методов и подходов к обучению криптографии данных.

1.2.2 Преимущества и недостатки различных методов обучения.

1.3 Актуальные темы и вызовы в криптографии данных:

1.3.1 Актуальные тенденции и вызовы в области криптографии данных

1.3.2 Важность обеспечения конфиденциальности и целостности данных в современном информационном обществе.

1.3.3 Связь между криптографией данных и законодательством об информационной безопасности.

1.1 Основы криптографии данных:

1.1.1 Определение криптографии данных и ее роль в современном мире.

**Криптография данных** — это наука и практика обеспечения конфиденциальности, целостности и аутентификации данных путем их защиты от несанкционированного доступа, изменения и подделки. Криптография использует различные математические методы и алгоритмы для шифрования данных, делая их непонятными для wdнесанкционированных пользователей, но доступными для тех, у кого есть правильные ключи или средства расшифровки.

Роль криптографии данных в современном мире:

**Защита конфиденциальности данных:** Криптография позволяет защищать чувствительные и личные данные, такие как финансовая информация, медицинские записи, коммерческие секреты и персональная переписка, от несанкционированного доступа. Это особенно важно в цифровом мире, где данные передаются через интернет и хранятся на устройствах.

**Обеспечение целостности данных:** Криптография также гарантирует, что данные не были изменены или повреждены в процессе передачи или хранения. Это важно в сферах, где целостность данных играет критическую роль, например, в финансовых транзакциях и медицинских записях.

**Аутентификация:** Криптографические методы могут подтверждать подлинность отправителя данных и получателя. Это предотвращает подделку данных и обеспечивает безопасную идентификацию пользователей.

**Защита от вредоносных атак:** Киберугрозы и кибератаки становятся все более распространенными, криптография помогает защищать системы и данные от вирусов, хакеров и других вредоносных агентов.

**Соответствие законодательству:** Во многих странах существуют законы и нормативные акты, требующие обеспечения конфиденциальности данных. Криптография помогает организациям соблюдать эти законы и избегать юридических проблем.

**Обеспечение безопасности интернета вещей (IoT):** С ростом числа подключенных устройств в Интернете вещей, криптография играет важную роль в защите данных, передаваемых и получаемых с умных устройств.

Информация стоит в центре многих процессов и транзакций, криптография данных стала неотъемлемой частью обеспечения информационной безопасности и приватности.

1.1.2 Основные понятия, такие как шифрование, дешифрование, ключи, алгоритмы шифрования, криптографические протоколы и стандарты.

**Основные понятия в области криптографии данных**:

**Шифрование (Encryption):** Шифрование - это процесс преобразования исходных данных (открытого текста) в нечитаемую форму (шифротекст) с использованием специального алгоритма и ключа. Целью шифрования является обеспечение конфиденциальности данных, чтобы только авторизованные пользователи могли прочитать их.

**Дешифрование (Decryption):** Дешифрование — обратный процесс, при котором шифротекст преобразуется обратно в исходные данные (открытый текст) с использованием того же алгоритма и ключа, который использовался при шифровании.

**Ключ (Key):** Ключ — параметр, который используется вместе с алгоритмом шифрования для шифрования и дешифрования данных. Ключи могут быть секретными (симметричное шифрование) или публичными/приватными (асимметричное шифрование).

**Алгоритмы шифрования (Encryption Algorithms):** Алгоритмы шифрования — математические функции и процессы, которые определяют, как именно происходит шифрование и дешифрование данных. Существуют различные алгоритмы, такие как AES (Advanced Encryption Standard), RSA, и многие другие.

**Криптографические протоколы (Cryptography Protocols):** Криптографические протоколы - наборы правил и процедур, которые определяют, как выполняется обмен зашифрованными данными между двумя или более участниками. Примеры включают SSL/TLS для безопасных соединений в Интернете и SSH для удаленного доступа.

**Стандарты криптографии (Cryptography Standards):** существуют международные и национальные стандарты криптографии, которые определяют алгоритмы и протоколы, которые должны использоваться для защиты данных. Например, FIPS (Federal Information Processing Standards) в США.

Криптография данных играет важную роль в обеспечении безопасности информации, и эти понятия и технологии служат основой для создания защищенных систем и приложений, обеспечивая конфиденциальность, целостность и аутентификацию данных.

1.1.3 Классификация криптографии: симметричная и асимметричная криптография.

Криптография классифицируется на два основных типа: симметричную и асимметричную (также называемую публичным ключом). Каждый из этих типов имеет свои уникальные характеристики и применения:

**Симметричная криптография (Symmetric Cryptography):**

**Принцип работы:** В симметричной криптографии один и тот же ключ используется как для шифрования, так и для дешифрования данных. Это означает, что отправитель и получатель должны иметь доступ к одному и тому же секретному ключу.

**Применение:** Симметричная криптография идеально подходит для шифрования больших объемов данных, таких как файлы, текстовые сообщения и трафик на высокоскоростных сетях. Она обеспечивает высокую производительность и эффективность шифрования.

**Примеры алгоритмов:** DES (Data Encryption Standard), 3DES, AES (Advanced Encryption Standard).

**Преимущества:** Высокая скорость шифрования, эффективность, подходит для больших объемов данных.

**Недостатки:** Проблема распределения секретных ключей между отправителем и получателем.

**Асимметричная криптография (Asymmetric Cryptography):**

**Принцип работы:** В асимметричной криптографии используется пара ключей - публичный и приватный. Публичный ключ используется для шифрования данных, а приватный ключ - для дешифрования. Это означает, что отправитель может зашифровать данные с помощью публичного ключа получателя, и только получатель, у которого есть соответствующий приватный ключ, сможет их расшифровать.

**Применение:** Асимметричная криптография широко используется в областях аутентификации, цифровых подписей и безопасных обменах ключами. Она обеспечивает безопасную передачу информации между участниками без необходимости предварительной договоренности о секретных ключах.

**Примеры алгоритмов:** RSA (Rivest–Shamir–Adleman), ECC (Elliptic Curve Cryptography), DSA (Digital Signature Algorithm).

**Преимущества:** Безопасная передача данных, отсутствие необходимости в секретном ключе на стороне отправителя.

**Недостатки:** Медленная производительность в сравнении с симметричной криптографией.

Выбор между симметричной и асимметричной криптографией зависит от конкретных требований безопасности и характеристик приложения. В практике часто используется комбинация обоих типов криптографии для достижения максимальной безопасности и эффективности.1.1.4 Примеры применения криптографии в информационной безопасности, банковском секторе, здравоохранении и других отраслях.

Криптография играет важную роль в обеспечении безопасности данных в различных отраслях. Вот некоторые примеры применения криптографии:

**Информационная безопасность:**

**Шифрование данных:** Криптография используется для шифрования конфиденциальных данных в хранилищах, на серверах и во время передачи по сетям. Это обеспечивает защиту данных от несанкционированного доступа и просмотра.

**Аутентификация:** Криптографические методы используются для аутентификации пользователей и устройств. Примеры включают в себя цифровые сертификаты и двухфакторную аутентификацию.

**Цифровые подписи:** Криптография позволяет создавать цифровые подписи, которые подтверждают подлинность электронных документов и сообщений.

**Банковский сектор:**

**Защита финансовых транзакций:** Криптография обеспечивает безопасность финансовых операций, таких как банковские переводы и онлайн-платежи.

**Безопасное хранение данных:** В банковской индустрии криптография используется для защиты личных данных клиентов и финансовых операций.

**Здравоохранение:**

**Защита медицинских записей:** Криптография помогает обеспечить конфиденциальность медицинских данных пациентов и обмена информацией между медицинскими учреждениями.

**Электронная медицинская история:** Криптография обеспечивает безопасное хранение и доступ к электронной медицинской истории пациентов.

**Телекоммуникации:**

**Защита передачи данных:** Криптография применяется для обеспечения конфиденциальности и безопасности в сотовых и интернет-связях.

**VPN (Virtual Private Network):** Криптографические методы используются для создания безопасных VPN-соединений для удаленного доступа к сетям и ресурсам.

**Обеспечение безопасности интернета вещей (IoT):**

**Безопасность умных устройств:** Криптография помогает защитить умные устройства и обеспечить безопасный обмен данными в Интернете вещей.

**Защита от атак:** Криптография играет решающую роль в защите от атак и вторжений в сети IoT.

**Государственные организации:**

**Национальная безопасность:** Криптография используется для защиты государственных секретов, милитаризированных коммуникаций и информации.

**Шифрование обмена данными:** Государственные организации используют криптографию для обеспечения безопасности данных и связи.

Эти примеры демонстрируют разнообразное применение криптографии в различных отраслях, где безопасность данных и конфиденциальность играют важную роль.

1.2 Методы обучения криптографии данных:

**Обзор существующих методов и подходов к обучению криптографии данных.**

Обучение криптографии данных имеет важное значение для обеспечения информационной безопасности. Существует несколько методов и подходов к обучению этой области. Вот обзор некоторых из них:

1. Университетские курсы:

*1.1 Академические курсы:* Многие университеты предлагают курсы по криптографии данных в рамках программ по информационной безопасности, компьютерным наукам или математике. Эти курсы включают лекции, практические задания и тесты.

*1.2 Образовательные программы:* существуют магистерские и докторские программы, специализирующиеся на криптографии данных. Они предоставляют более глубокие знания и исследовательский опыт.

2. Онлайн-курсы и MOOCs:

*1.1 Online-курсы:* Множество онлайн-платформ предоставляют курсы по криптографии данных, которые доступны для широкой аудитории. Эти курсы могут быть бесплатными или платными и предоставлять видео-лекции, задания и тесты.

*1.2 MOOCs (Massive Open Online Courses):* Крупные учебные платформы, такие как Coursera, edX и Udacity, предлагают MOOCs по криптографии данных, разработанные ведущими университетами и экспертами.

3. Специализированные курсы и тренинги:

*1.1 Курсы обучения на рабочем месте:* Некоторые компании и организации предоставляют своим сотрудникам обучение по криптографии данных, чтобы повысить компетентность в области информационной безопасности.

*1.2 Сертификационные программы:* существуют сертификационные программы, такие как Certified Information Systems Security Professional (CISSP), которые включают обучение криптографии данных и тестирование для получения сертификата.

4. Самообразование:

*4.1 Специализированные книги и ресурсы:* Множество книг и онлайн-ресурсов доступно для самостоятельного изучения криптографии данных. Примеры включают "Криптография и сетевая безопасность" Уильяма Сталлинга и онлайн-курс "Crypto101".

Каждый из этих методов и подходов имеет свои преимущества и может быть адаптирован к разным уровням знаний и интересам. Обучение криптографии данных важно для специалистов по информационной безопасности, разработчиков и всех, кто заботится о безопасности данных в шифрование.

1.2.2 Преимущества и недостатки различных методов обучения.

Каждый метод обучения имеет свои преимущества и недостатки, и выбор конкретного метода зависит от ваших целей, предпочтений и контекста обучения. Вот обзор преимуществ и недостатков различных методов обучения, включая университетские курсы, онлайн-курсы, самообразование и обучение с помощью практических проектов:

1. Университетские курсы:

*1.1 Преимущества:*

Структурированное обучение с определенной программой.

Доступ к квалифицированным преподавателям и экспертам.

Возможность сетевого взаимодействия с однокурсниками и обмена опытом.

Получение академической поддержки и оценок.

*1.2 Недостатки:*

Дорогостоящие в обучении и требующие временных затраты.

Ограниченное гибкое расписание, что может быть неудобным для работающих.

Возможно, ограниченный выбор университетов и мест для обучения.

1. Онлайн-курсы и MOOCs:

*1.1 Преимущества:*

Гибкий график обучения и доступность для широкой аудитории.

Разнообразие предлагаемых курсов и тем.

Многие бесплатные курсы и доступ к высококачественным материалам.

Возможность самостоятельного обучения.

*1.2 Недостатки:*

Ограниченное взаимодействие с преподавателями и однокурсниками.

Не всегда предоставляют оценку и сертификаты (платные курсы и сертификационные программы исключение).

Требует высокой самодисциплины для завершения курса.

1. Самообразование:

*1.1 Преимущества:*

Полная гибкость в планировании и темпе обучения.

Бесплатный доступ к ресурсам и учебным материалам.

Возможность выбора конкретных тем и углубленного изучения.

*1.2 Недостатки:*

Отсутствие структуры и направления, что может привести к фрагментации знаний.

Недостаток оценки и внешней мотивации.

Может потребовать больше усилий для поиска и выбора качественных ресурсов.

1. Обучение с помощью практических проектов:

*1.1 Преимущества:*

Практическое применение знаний.

Развитие навыков решения реальных задач.

Мотивация и углубленное понимание.

*1.2 Недостатки:*

Могут потребовать предварительных знаний.

Ограничен доступ к экспертам и обратной связи.

Не всегда структурированы и несут риски неудачи при выполнении проектов.

Обычно успешное обучение включает в себя комбинацию разных методов в зависимости от ваших целей и ресурсов. Например, вы можете начать с онлайн-курсов для ознакомления, а затем погрузиться в более глубокое изучение с помощью учебников и самостоятельных проектов.

1.3 Актуальные темы и вызовы в криптографии данных:

1.3.1 Актуальные тенденции и вызовы в области криптографии данных

Блокчейн и криптовалюты:

*Вызов:* Развитие блокчейна и криптовалют создает новые сценарии для криптографии данных, так как безопасность и приватность транзакций играют важную роль в этой области.

*Тенденция:* Разработка новых протоколов конфиденциальности и улучшенных алгоритмов шифрования для обеспечения безопасности и анонимности пользователей в блокчейне и криптовалютах.

Защита от атак на стороннюю сторону (Side-Channel Attacks):

*Тенденция:* Развитие методов и алгоритмов для защиты от атак, которые используют утечку информации через различные каналы, такие как временные и энергетические характеристики работы устройств.

Обучение машин и искусственный интеллект (ИИ):

*Вызов:* Обучение машин и ИИ требуют обработки и хранения больших объемов данных, что делает их уязвимыми для атак.

*Тенденция:* Разработка методов криптографии данных, которые обеспечивают конфиденциальность и безопасность данных при использовании алгоритмов машинного обучения и ИИ.

Биометрическая криптография:

*Тенденция:* Использование биометрических данных, таких как отпечатки пальцев и сканы лица, в криптографии для более сильной аутентификации и безопасности.

Криптовалюты и цифровые активы:

*Тенденция:* Разработка новых методов защиты цифровых кошельков и активов для обеспечения безопасной работы с криптовалютами и цифровыми активами.

Регулирование и законодательство:

*Вызов:* Регулирующие органы во многих странах разрабатывают законодательство в области криптографии и криптовалют.

*Тенденция:* Стремление к разработке стандартов и законодательных актов, которые сбалансированно учитывают потребности в конфиденциальности и безопасности данных.

Актуальные вызовы и тенденции в области криптографии данных продолжают формироваться, и их эффективное управление требует постоянного обновления методов и подходов для обеспечения безопасности информации.

1.3.2 Важность обеспечения конфиденциальности и целостности данных в современном информационном обществе.

Обеспечение конфиденциальности и целостности данных является критически важным аспектом в современном информационном обществе. Вот почему это так важно:

1. **Защита Личной Информации:** Конфиденциальность данных играет ключевую роль в защите личной информации граждан. Утечка таких данных, как социальные номера, медицинские записи или финансовая информация, может привести к краже личности, мошенничеству и другим видам преступлений.
2. **Защита Коммерческой Информации:** В бизнес-среде, конфиденциальность данных о компании, клиентах, проектах и стратегиях является критически важной. Утечка такой информации может повредить репутацию, вызвать финансовые убытки и даже угрожать выживанию компании.
3. **Защита Национальной Безопасности:** В государственных и оборонных организациях, целостность и конфиденциальность данных критически важны для национальной безопасности. Утечка важной информации может привести к потере стратегических преимуществ и риску национальной безопасности.
4. **Борьба с Киберугрозами:** Конфиденциальность и целостность данных играют роль в защите от киберугроз, таких как вирусы, вредоносные программы и хакерские атаки. Нарушение конфиденциальности может быть первым шагом к атаке.
5. **Соблюдение Законодательства:** В разных странах и отраслях существует законодательство, требующее соблюдения конфиденциальности данных. Нарушение этого законодательства может привести к юридическим последствиям и штрафам.
6. **Защита Инфраструктуры:** Важная информация о критической инфраструктуре, такой как энергосистемы, телекоммуникации и здравоохранение, должна быть защищена для обеспечения стабильности и надежности этих систем.
7. **Доверие Пользователей:** Защита конфиденциальности и целостности данных способствует доверию пользователей к организациям и сервисам. Пользователи ожидают, что их данные будут обрабатываться с заботой и безопасностью.
8. **Инновации и Исследования:** Обеспечение конфиденциальности данных также важно для стимулирования инноваций и научных исследований. Когда организации и исследователи уверены в конфиденциальности своих данных, это способствует обмену информацией и коллаборации.

Современное информационное общество зависит от обработки, передачи и хранения данных. Поэтому безопасность данных имеет огромное значение для защиты интересов людей, организаций и государств. Эффективные меры по обеспечению конфиденциальности и целостности данных являются ключевым фактором в современном мире информационных технологий.

**1.3.3 Связь между криптографией данных и законодательством об информационной безопасности.**

Связь между криптографией данных и законодательством об информационной безопасности в Российской Федерации (РФ) существует, и законы и нормативные акты играют важную роль в регулировании использования криптографии для обеспечения безопасности данных. Ключевые аспекты связи между криптографией данных и законодательством об информационной безопасности в РФ:

**Федеральный закон "О персональных данных" (152-ФЗ):** Этот закон устанавливает правила и требования для обработки и защиты персональных данных в России. Он также определяет обязанности организаций по обеспечению конфиденциальности персональных данных и обязанность применения криптографии для защиты таких данных.

**Закон РФ "Об информации, информационных технологиях и о защите информации" (149-ФЗ):** Этот закон определяет основные положения в области информационной безопасности и информационной защиты. Он также регулирует использование криптографии для защиты информации и требует, чтобы организации, обрабатывающие информацию, соблюдали нормы безопасности.

**Постановление Правительства РФ № 313 "Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных" (313-ПП):** Это постановление устанавливает конкретные требования и стандарты для защиты персональных данных, включая использование криптографии.

**Федеральный закон "О государственной тайне" (98-ФЗ):** Этот закон регулирует обработку и хранение информации, отнесенной к государственной тайне, и включает в себя требования к криптографической защите такой информации.

**Государственные стандарты и нормативные документы:** Российская система стандартизации (ГОСТ) включает множество стандартов, связанных с криптографией и информационной безопасностью. Эти стандарты устанавливают требования к криптографическим алгоритмам и протоколам, которые используются для защиты информации.

**Лицензирование и сертификация:** В РФ существуют органы, ответственные за сертификацию и лицензирование продуктов и решений в области информационной безопасности, включая криптографические средства.

Следует отметить, что в РФ правительство стремится ужесточить требования к использованию криптографии и обеспечению информационной безопасности, особенно в отношении критически важных объектов и систем. Поэтому организации, работающие с данными, обязаны соблюдать соответствующие нормы и требования, включая обязательное применение криптографии для защиты информации.

Обеспечение соблюдения законодательства об информационной безопасности, включая требования к криптографии, является важным аспектом в деятельности организаций и государственных учреждений в России, чтобы защитить конфиденциальность, целостность и доступность данных.

**Вывод**

Выводы: Исследование предметной области выявило основные аспекты криптографии данных, методы ее обучения и актуальные темы в этой области. Эти знания будут служить основой для разработки обучающей программы, которая позволит студентам и специалистам овладеть этой важной областью информационной безопасности.

1. **Обзор аналогов**

Обзор аналогов помогает выявить существующие программы и ресурсы, которые могут быть схожи с вашей разработкой. Это позволяет оценить конкурентное пространство и выделить уникальные особенности вашей программы.

1. Coursera: Cryptography Specialization

Coursera предоставляет специализацию по криптографии, включающую в себя несколько курсов, охватывающих основы криптографии и современные методы шифрования данных.

Преимущество: Онлайн-курсы от ведущих университетов и экспертов.

1. edX: Introduction to Cryptography

edX предлагает курс по введению в криптографию, который рассматривает основные принципы и методы шифрования данных.

Преимущество: Бесплатный доступ и возможность получения сертификата.

1. Khan Academy: Computer Science - Cryptography

Khan Academy предоставляет бесплатные учебные материалы по криптографии, включая видеоуроки и интерактивные задания.

Преимущество: Бесплатность и доступность для широкой аудитории.

1. Codecademy: Learn Cryptography

Codecademy предлагает интерактивный курс, который позволяет студентам изучать криптографию через практические упражнения и программирование.

Преимущество: Практический подход к обучению криптографии.

1. Crypto101: Introduction to Modern Cryptography

Эта бесплатная книга доступна онлайн и предоставляет введение в современную криптографию, включая примеры кода.

Преимущество: Бесплатный источник, который может использоваться как учебник.

Проекты с открытым исходным кодом:

Существуют проекты с открытым исходным кодом, предоставляющие библиотеки и инструменты для реализации криптографии данных. Например, OpenSSL и Bouncy Castle.

1. **Анализ и выбор**

На основе имеющейся информации и аналогов был сделан выбор в пользу создания собственной обучающей программы по теме “Криптография данных”.

Доступ к теоретической части будет осуществлён непосредственно в самом приложение перед практической частью, принцип работы которой будет объяснён ранее.

После теоретической части следует практическая часть, в которой в которой пользователь сможет взаимодействовать с программой по шифрованию данных. За основу взята переносная шифровальная машина «**Эни́гма**» (от [нем.](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BC%D0%B5%D1%86%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Änigma* — загадка)

Источники:  
1) <https://practicum.yandex.ru/blog/chto-takoe-kriptografiya/>

2) <https://www.bibliofond.ru/view.aspx?id=650737>

Книги:  
1) <https://books.ifmo.ru/file/pdf/56.pdf>

2) <https://new-disser.ru/_avtoreferats/01002612632.pdf>