**Слайд 1: //титульник**

Здравствуйте уважаемые члены экзаменационной комиссии, вашему внимаю представляется дипломная работа на тему: «Разработка программы шифрования файлов».

Актуальность этой разработки связана с интенсивным развитием технологий и постоянным повышением значимости информации. Так как на сегодняшний день информация стала одним из важнейших стратегических ресурсов, её производство и потребление составляют необходимую основу эффективного функционирования и развития различных сфер общественной жизни. Отсюда возникает такая важная проблема современности как защита информации.

**Слайд 2: //объект и предмет**

Наука, изучающая способы сокрытия данных и обеспечения их конфиденциальности, называется - криптография. Криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности.

Переоценить возможности криптографии для человечества сложно. С момента появления она прошла множество модификаций и сейчас представляет собой систему безопасности, которая практически не может быть взломана. Современные методы криптографии применяются во всех отраслях, в которых присутствует необходимость безопасной передачи или хранения данных.

**Слайд 3: //цель и задачи**

Цель проекта заключается в разработке программы шифрования файлов. Программа призвана защитить важную для пользователя информацию на тот случай, если злоумышленник каким-либо образом сможет получить к ней доступ, а для защиты информации в программе используются популярные и относительно надёжные алгоритмы.

Для достижения цели необходимо решить ряд задач.

Нужно ознакомиться с наукой, которая называется криптология, а именно с двумя её направлениями: криптографией, о которой я уже упомянул и криптоанализом. Ознакомится с криптоанализом нужно для того, чтобы понимать каким образом зашифрованная информация может быть дешифрована без использования ключа. К тому же изучение этого направления помогло при выборе методов для реализации.

Помимо этого, нужно продумать внешний вид, составить необходимые схемы, выбрать инструменты для разработки и, после написания кода программы и отладки её работы, написать руководство по использованию.

**Слайд 4: //криптосистемы**

Прежде чем перейти к методам шифрования, которые реализованы в программе хочу кратко рассказать про существующие криптосистемы и принципы их работы.

Все существующие методы шифрования по числу применяемых ключей можно разделить на симметричные и асимметричные.

**Слайд 5: //симметричная криптосистема**

Симметричная криптосистема базируется на том, что отправитель и получатель данных имеют одинаковые ключи для разгадки шифра. Соответственно, чтобы зашифровать и дешифровать сообщение нужно использовать один и тот же ключ.

**Слайд 6: //асимметричная криптосистема**

Асимметричная криптосистема задействует открытый и закрытый ключи. Ключи взаимосвязаны, а это значит, что информация, зашифрованная открытым ключом, может быть раскрыта только связанным с ним закрытым ключом. Применять для разгадки ключи из разных пар невозможно, поскольку они связаны между собой математической зависимостью.

**Слайд 7: //методы шифрования**

Методы шифрования для реализации выбирались долго. В первую очередь хотелось, чтобы они имели высокую скорость шифрования и дешифрования текста и при этом были достаточно криптографически стойкими. Помимо этого, хотелось, чтобы методы, по принципу работы относились к разным типам.

В итоге были выбраны следующие методы. Здесь есть шифры перестановки, шифры подстановки и шифры типа гаммирования.

**Слайд 8: //конт. диаг. потоков данных**

Контекстная диаграмма потоков данных представляет собой взаимодействие пользователя и программы, связанных потоками данных. Пользователь взаимодействует с программой передавая ей некоторые данные, это может быть исходный текст, ключи, выбранная операция и другое. Обработав данные, программа выдаёт пользователю результат, соответствующий введённым данным.

**Слайд 9: //конт. функ. диаграмма**

Функциональная диаграмма отражает взаимосвязи функций разрабатываемого программного обеспечения. Эта диаграмма была нужна на ранней стадии проектирования для того, чтобы выделить основные функции и составные части разрабатываемой программы, а также по возможности устранить некоторые ошибки проектирования.

**Слайд 10: //структурная схема**

Структурная схема дала достаточно полное представление о проектируемой программе, помогла определить структурные компоненты и связи между ними. Как видно на схеме структура программы делится на два блока. В левом блоке находятся основные функции, в правом дополнительные.

**Слайд 11: //интерфейс**

Интерфейс программы менялся много раз. На картинке видно, что он выполнен в нейтральных цветах и минималистическом стиле. Так как программа имеет большое количество функций, при разработке интерфейса одной из главных задач было сделать его интуитивно понятным. Нужно было обеспечить видимость всех элементов управления, которые необходимы для выполнения конкретной задачи, при этом интерфейс должен был иметь множество подсказок, обладать ненавязчивостью в своём стремлении помочь пользователю и минимизировать количество возможных ошибок.

Перейду к демонстрации программы.

**Слова при демонстрации программы:**

//Рассказать про прогу

**Слайд 12: //заключение**

Подводя итоги можно сказать, что программа имеет множество достоинств и возможностей для дальнейшего развития.

Благодаря структурированному коду в будущем не составит никакой труда к примеру, добавить новый метод шифрования или новый язык, с которым сможет работать программа. Сейчас она работает только с русским и английским.

На мой взгляд все задачи проекта были выполнены, функции реализованы и протестированы.

Проведённые испытания показали корректность работы программы, что позволяет рекомендовать её для защиты информации.

Считаю выпускную квалификационную работу успешно завершённой.

**Слайд 13: //спасибо за внимание**

Доклад окончен, спасибо за внимание.