**Слайд 1**

Здравствуйте уважаемые члены приёмной комиссии. Я,Гарапов Тимур ПавловичЬ представляю на защиту выпускную квалификационную работу на тему “Разработка программного обеспечения для”

**Слайд 2**

Целью данной работы является разработка программного обеспечения осуществляющего шифрование данных для мобильных устройств под управлением мобильной ОС Android с возможностью портирования приложения ну другие ОС.

**Слайд 3**

Задачами работы являются:

1. Обзор мобильных устройств с точки зрения разработчика ПО.

2. Раскрытие алгоритмического процесса шифрования.

3. Рассмотреть существующие решения в области защиты данных на мобильных устройствах.

4. Выработка требований к создаваемому ПО на основе анализа существующих решений и анализа алгоритмов шифрования.

5. Разработка кроссплатформенного приложения.

**Слайд 4**

Итак, исходя из популярности данной системы, целесообразно будет начать разработку приложения для данной ОС – по причине большего охвата пользовательской аудитории.

Android – это мобильная операционная система, основанная на монолитном модифицированном ядре Linux.

Генерация информации велика из-за мобильных устройств.

Например:

1. Фотографии, на которых запечатлён владелец устройства или его имущество.

2. Список и контакты друзей и родственников владельца.

3. Информация о религиозных и политических предпочтениях владельца устройства.

4. Информация о прочих предпочтениях и интересах.

5. Ежедневный график.

6. Информация о медицинском обслуживании и состоянии здоровья владельца устройства

7. Прочая информация, которую владелец устройства не желает предавать огласке.

**Слайд 5**

Были проанализированы 3 приложения: Boxcryptor Classic, Encryption Manager и SSE Шифрование.

Оценены по критериям:

* количество доступных алгоритмов шифрования;
* дополнительный функционал ;
* наличие платной версии;
* кросс-платформенность;
* удобство интерфейса;
* частота Обновления.

На основании оценки были сформулированные основные требования к разрабатываемом программному обеспечению.

Таким образом, проанализировав существующие на платформе Android приложения, осуществляющие шифрование данных, были выявлены следующие требования и критерии, которые необходимо учитывать при разработке приложения.

При проектировании и создании приложения необходимо учитывать:

• скорость работы;

• удобство интерфейса для конечного пользователя;

• наличие встроенного файлового менеджера;

• отсутствие критически узких мест, например - использования 1-го Мастер пароля для последующего шифрования всех данных, без возможности альтернативных вариантов защиты;

• возможность Передачи защищённых файлов по открытым каналам, и возможность использовать эти файлы различных устройствах.

**Слайд 6**

Было проанализировано 3 алгоритма шифрования:

1. ГОСТ 28147-89 (Известный как “Магма”).
2. AES.
3. TwoFish.

В ходе их изучения и оценки:

* Произведено сравнение задокументированных характеристик алгоритмов.
* Оценено количество опубликованных научных работ по анализу каждого из алгоритмов.
* Изучены предполагаемые варианты атак на алгоритмы, представленные в некоторых работах по их криптоанализу.
* Оценена популярность и частота применения каждого из алгоритмов.

По итогам анализа выбран алгоритм AES.

**Слайд 7**

В случае обработки персональных данных владельца устройства создаваемым приложением, на создаваемое ПО накладывает ограничение Федеральный закон РФ № 152 "О персональных данных" [] . В частности, нас интересуют следующие положения:

*“ Статья 7. - Конфиденциальность персональных данных. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.”*

Несмотря на тот факт, что как-таковые персональные данные в случае шифрования при помощи ПО, с точки зрения разработчика ничем не отличаются от прочих возможных данных, данная статья накладывает на нас требование соблюдать конфиденциальность обрабатываемых данных.

В случае же, учитывающем возможность шифрования данных, составляющих коммерческую тайну предприятия, нам следует опираться на Федеральный закон N 98-ФЗ "О коммерческой тайне" [] , а в частности на *Статью 6.1, пункт 2, который гласит:* -

“*2. Обладатель информации, составляющей коммерческую тайну, имеет право:*

*1) устанавливать, изменять, отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;*

*2) использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;*

*3) разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;*

Таким образом целесообразно будет в ТЗ к разрабатываемому программному средству добавить требование по обработке(шифрованию) данных исключительно средствами мобильного устройства, на котором находятся шифруемые данные, дабы исключить возможность перехвата и нанесения вреда защищаемой информации.

**Слайд 8.**

Microsoft Visual Studio Community Edition включающую в себя средства для разработки на ООП языке C#, с установленным дополнением Xamarin .

Для описания интерфейса используется расширяемый язык разметки для приложений XAML. XAML – это основанный на XML язык разметки разработанный Microsoft.

**Слайд 9**

Созданный функции

Функционал приложений описывается в соответствующих файлах, являющихся либо описанием классов объектов, используемых в приложении, либо эти функции описаны в файле Functions.cs, описывающих класс, предоставляющий объектам доступ к статическим методам, обеспечивающим функциональность приложения.

Реализованы:

* DoAes – функция, принимающая на вход адрес файла, путь к выходной папке, куда следует записать результирующий файл, и пароль, используемый для генерации ключа шифрования;
* UndoAes – функция, обратная предыдущей. Получает на вход адрес зашифрованного файла, путь к результирующей папке, и пароль, используемый для генерации ключа;
* GetPath – функция, вызывающая окно выбора файла и возвращающая упорядоченный адрес результирующего файла;
* GetPassword – функция, принимающая на вход длину требуемого пароля и осуществляющая его генерацию. Возвращает строку, представляющую собой сгенерированный пароль;