# Введение

Прежде чем говорить об актуальности темы необходимо разобраться с самим понятием смартфона - мобильного телефона, дополненного функциональностью карманного персонального компьютера.

При расширении функциональности мобильных устройств увеличился объём и тип хранимой на мобильных устройствах информации, вследствие чего появилась проблема защиты информации, находящейся на мобильном устройстве. Современные операционные системы на смартфонах только начали встраивать поддержку шифрования пользовательских данных, однако не все мобильные устройства поддерживают переход на новые версии ОС со встроенной защитой данных.

Создание же программного обеспечения, предоставляющего возможность защиты данных посредством шифрования, позволит пользователям самостоятельно осуществлять защиту информации, находящейся на мобильном устройстве.

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.

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.

Дипломная работа состоит из введения, основной части (три главы), заключения, библиографического списка и приложения. В библиографический список включены наименования N работ, среди которых M интернет ресурсы.

# Глава 1.

## 1.1 Обзор мобильных устройств.

Современный мир невозможно представить без компьютеров. Мощные вычислительные устройства позволили человечеству качественно продвинуться вперёд в своём развитии, помогая производить сложные расчёты с считанные секунды, а создание и развитие сети Internet и сети World Wide Web(WWW), которая работает на базе сети Internet, и в большинстве случаев, под сетью Internet люди понимают именно WWW, позволило распространять и получать данные независимо от того, насколько далеко мы находимся от источника или получателя этих данных. Сеть WWW совместно с веб-технологиями построения сайтов позволила большинству людей пользоваться достижениями современных технологий без необходимости изучения основ работы всемирной сети.

Согласно данным, указанным в книге [1], в период с 2012 по 2015 год количество пользователей сети Internet увеличилось на 800 миллионов человек, достигнув 3,3 миллиардов. Столь взрывной рост был вызван в том числе тем, что в данный период началось широкое распространение Мобильный устройств, поддерживающих стандарт связи 3G и уменьшение стоимости мобильного интернета в мире.

Для начала следует разобраться с самим понятием мобильного устройства, а так-же тем, что из себя представляют мобильные устройства на 2016 год.

Для начала рассмотрим определение мобильных устройств. Согласно определению с сайта SecurityLab.ru:

Мобильные устройства – ряд устройств, который включает в себя смартфоны, планшеты, электронные книги, телефоны, КПК и нетбуки, главной особенностью которых является размер, а также количество выполняемых ими функций

Таким образом к мобильным устройствам относятся:

* Телефоны
* Нетбуки
* КПК
* Электронные книги
* Смартфоны
* Планшеты

Учитывая ситуацию на 2016 год следует отметить, что современные нетбуки по функциональности приближаются к ноутбукам, отличаясь лишь размерами, КПК были вытеснены с рынка смартфонами, а современные телефоны, как правило, не имеют возможности устанавливать ПО ввиду своей простоты. Электронные книги же бывают в двух вариантах:

1. Электронная книга без избыточной функциональности. Такие книги, как правило используют закрытую ОС на базе ядра Linux, и их функциональность ограничена чтением электронных книг.
2. Электронная книга с дополнительной функциональностью. На данный момент, в качестве ОС для подобных книг в подавляющем большинстве случае использует мобильная ОС Android c частично урезанной функциональностью, что позволяет устанавливать на электронную книгу приложения от сторонних разработчиков, например, таковым устройством является электронная книга SonyReader.

Таким образом, в данной работе для нас представляют интерес 2 вида устройств:

1. Смартфоны
2. Планшетны

Смартфон - мобильный телефон, дополненный функциональностью карманного персонального компьютера. Смартфоны имеют достаточно развитую операционную систему, под которую возможно создание приложений сторонними разработчиками. Наличие полнофункциональной операционной системы делает смартфоны более привлекательными в глазах большинства пользователей. Современные смартфоны прекрасно справляются со многими задачами, выходящими за рамки функциональности, которая ожидают от телефона: работа с электронной почтой, просмотр текстовых документов и электронных таблиц, обработка изображений. Некоторые модели телефонов достаточно производительны для произведения сложных вычислений при установке соответствующего программного обеспечения. Важно отметить, что программы, написанные специально для операционной системы смартфона, являются полноценными скомпилированными в двоичный код последовательностями низкоуровневых микропроцессорных команд.

Наиболее распространёнными мобильными операционными системами на смартфонах являются (по данным 2015 года) :

Таблица 1

|  |  |
| --- | --- |
| Название ОС | Количество устройств, % |
| Android | 79,9 |
| iOS | 13,6 |
| Windows 10 Mobile и Windows phone | 5,3 |

Планшетные Компьютеры – в общем смысле – это собирательное понятие, включающее в себя различные виды переносных мобильных устройств оснащённых сенсорным экраном, основной способ взаимодействия с планшетным компьютером - при помощи рук или стилуса, в зависимости от типа сенсора. Под планшетными компьютерами могут подразумеваться большое количество устройств, и основные из них - :

1. Планшетный персональный компьютер – IBM PC – cовместимый компьютер. Например, ноутбуки-транcформеры являются планшетными ПК, так как являются IBM совместимыми и при этом имеют возможность полноценного взаимодействия с пользователем посредством сенсорного экрана.
2. Интернет-планшет – Подвид планшетных компьютеров, которые не являются IBM PC-совместимыми, и предназначены в основном для веб-серфинга, работы с веб-приложениями, а также – запуска лишь специально написанных для них приложений. Для управления интернет-планшетом используется сенсорный экран, взаимодействие с которым реализуется при помощи пальцев или специального стилуса, без использования аппаратной клавиатуры или мыши. Современные планшеты поддерживают мультитач – касание несколькими пальцами (до 10 касаний) , и управлением планшетом специальными жестами.

В планшетных компьютерах используются Операционные системы, аналогичные операционным системам смартфонов. Соответственно, основные ОС на планшетах представлены в Таблице 2 :

Таблица 2

|  |  |
| --- | --- |
| Название ОС | Количество устройств, % |
| Android | 75 |
| iOS | 14,3 |
| Windows RT и Windows 10 | 9,1 |

Здесь следует отметить, что планшетны под управлением Windows 10 могут являться IBM PC – совместимыми компьютерами, в зависимости от аппаратной части.

Как можно заметить из указанных выше данных – семейство Android является доминирующим на рынке мобильных ОС. Более того, в абсолютных числах – в 2014 году количество активных Android устройств перешагнуло рубеж в 1 миллиард устройств, и , по оценкам аналитиков, в 2016-2017 году количество активных Android устройств может достичь 2 миллиардов.

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 сильно ядре Linux, подвергшемуся сильной переработке. Изначально разрабатывалась компанией Android Inc., которую затем купила Google. Впоследствии Google инициировала создание альянса Open Handset Alliance , который сейчас занимается поддержкой и развитием платформы. Android позволяет создавать приложения, управляющие устройством через разработанные Google библиотеки. Android Native Development Kit позволяет портировать библиотеки и компоненты приложений, написанные на C, С++ и других языках. Приложения под операционную систему Android являются программами в нестандартном байт-коде для виртуальной машины Dalvik, для них был разработан формат установочных пакетов .APK. Начиная с версии Android 5.0 виртуальная машина Dalvik была заменена системой, под названием Android Runtime (ART) , которая, в отличии от Dalvik, использующего Just-In-Time компиляцию, производил компиляцию в момент установки. При этом ART использует тот-же байт код, что и Dalvik, для обеспечения совместимости приложений.

Последняя выпущенная версия Android на данный момент – Android 6.0 Marshmallow.Однако, большинство устройств до сих пор используют предыдущие версии ОС. На настоящий момент выпущено 12 версий системы. Распределение версий ОС показано в Таблице 3 на основе статистики на 4 мая 2016 года.

Таблица 3 Распределение версий ОС Android

|  |  |
| --- | --- |
| Версия ОС | Количество устройств, % |
| 2.2.x (Froyo) | 0,1 |
| 2.3.x (Gingerbread) | 2,2 |
| 4.0.x (Ice Cream Sandwich) | 2,0 |
| 4.1.x (Jelly Bean) | 7,2 |
| 4.2.x (Jelly Bean) | 10,0 |
| 4.3.x (Jelly Bean) | 2,9 |
| 4.4.x (KitKat) | 32,5 |
| 5.0.x (Lollipop) | 16,2 |
| 5.1.x (Lollipop) | 19,4 |
| 6.0.x (Marshmallow) | 7,5 |

На основе этой статистики можно сделать вывод о том, что большинство пользователей ОС Android используют 4.х версию, при этом абсолютное большинство пользователей используют на своих устройствах версию Android 4.4. Таким образом, приложение будет разработано с использованием средств, которые поддерживаются данной версией ОС, с целью охвата большого количества мобильных устройств и их пользователей.

## 1.2 Основы и история криптографии

Криптография - наука о методах обеспечения конфиденциальности, целостности данных и аутентификации . Она изучает методы преобразования информации, направленные на сокрытие ее содержания.

Дэвид Кон (David Kohn) в книге о криптоанализе «Выдающиеся взломщики шифров» привел данные о том, что криптография использовалась в Египте в 1900 г. до н.э. В Древней Греции и Древнем Риме криптография уже широко использовалась в разных областях деятельности, особенно в государственной сфере. (Юлий Цезарь «Записки о галльской войне», 1 век до н.э.)

Период развития криптографических наук с древних времен до 1940-х годов принято называть эрой донаучной криптографии, так как изыскания тех времен основаны на интуиции и не подкреплены доказательствами.

Вторая мировая война явилась поворотным пунктом в истории криптографии: если до войны криптография представляла собой достаточно узкую область, то после войны она стала широким полем деятельности.

В 70-х годах 20-ого века произошло два события, серьезно повлиявших на дальнейшее развитие криптографии. Первое - был принят первый стандарт шифрования данных (DES). Второе – на основе работы американских математиков У.Диффи и М.Хеллмана был разработан новый раздел криптографии - криптография с открытым ключом. Эти события были закономерным итогом того, что развивающиеся компьютерные сети и информация циркулирующая в них требовали всё большей надёжности и защищённости. Криптография стала широко востребованной не только в военной, дипломатической, государственной сферах, но также в коммерческой, банковской и т.д..

Основной инструмент современной криптографии – шифрование. Шифрование – это обратимое преобразование информации с использованием одного из алгоритмов, осуществляемое с целью сокрытия информации от неавторизованных лиц, и в то же время - с предоставлением доступа к информации доверенным лицам.

Основные алгоритмы шифрования, применяемые в наше время, можно разделить на 2 группы:

1. Симметричные алгоритмы шифрования.
2. Ассиметричные алгоритмы шифрования.

Разница между этими двумя видами алгоритмов состоит в следующем –в симметричных алгоритмах шифрования для шифрования и расшифровывания информации используется один ключ шифрования. Такие системы дешевле и проще в реализации, они быстрее работают и обладают большей гибкостью, но при этом, в случае компрометации секретного ключа, система становится полностью открыта для злоумышленника, а в случае симметричного алгоритма – точек, где используется секретный ключ больше, что даёт в итоге больше мест потенциальных утечек ключа.

В ассиметричных алгоритмах шифрования используется два ключа. Секретный ключ используется для расшифровывания сообщения. Открытый ключ генерируется с использованием секретного ключа и используется для шифрования сообщения. Ассиметричные системы дороже в применении, они дольше обрабатывают информацию, и обладают меньшей гибкостью, однако их сложнее взломать. Некоторые виды ассиметричных алгоритмов практически невозможно взломать на доступных человечеству вычислительных мощностях.