МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Электронная подпись документа с использованием отпечатка пальца

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Бабич Павла Николаевича

Научный руководитель
к.п.н., доцент _____ А. С. Гераськин
22.01.2022 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
22.01.2022 г.

Саратов 2022

ВВЕДЕНИЕ

Благодаря развитию информационных технологий наблюдается тенденция к вытеснению бумажного документооборота электронным, все больше предприятий сдают отчетность, участвуют в закупках, подают арбитражные иски, обращаются в госорганы, начинают вести юридически значимый документооборот в электронном виде. Защитных атрибутов бумажных документов – подписей, печатей, штампов, водяных знаков, специальной фактуры бумажной поверхности и т. п. – у электронных документов нет. Необходимость их защиты очевидна. Поэтому задача разработки механизмов упрощения взаимодействия с аппаратом электронной защиты, который смог бы заменить подпись и печать на бумажных документах, важна и актуальна. То есть необходим механизм электронной подписи (далее ЭП), которая представляет собой дополнительную информацию, прикрепляемую к защищаемым данным. Законы об ЭП сегодня имеют 62 государства. С 2002 года в этот список вошла и Россия. 10.01.2002 г выходит Федеральный закон «Об электронной цифровой подписи» (далее с изменениями и дополнениями), целью которого является обеспечение правовых условий использования ЭП в электронных документах, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

Электронная подпись позволяет:

- аутентифицировать лицо, подписавшее сообщение;
- контролировать целостность сообщения;
- защищать сообщение от подделок;
- доказать авторство лица, подписавшего сообщение.

Подделать ЭП практически невозможно – для этого требуется большое количество вычислений, которые не могут быть реализованы при современном уровне развития вычислительной техники и математики за приемлемое время

(т.е. пока информация, содержащаяся в подписанном документе, сохраняет актуальность). Дополнительная защита от подделки обеспечивается сертификацией удостоверяющим центром открытого ключа подписи. Кроме того, по желанию клиента удостоверяющий центр может застраховать его ЭП.

Целью данной работы является изучение видов и алгоритмов электронной подписи, анализа механизма работы ЭП, исследование особенностей использования ЭП в операционной системе Android, анализ существующих методов биометрического распознавания, изучение возможностей применения отпечатка пальца при формировании ЭП, реализация алгоритма ГОСТ Р 34.10-2012 для подписания документов формата PDF с использованием инструментов ОС Android.

Для достижения поставленной цели необходимо выполнения следующих задач:

- определить правовую природу электронной цифровой подписи;
- провести анализ существующих видов ЭП;
- реализовать практический проект мобильного приложения, позволяющего формировать ЭП для выбранного документа с использованием биометрических механизмов ОС Android.

Предметом исследования являются теоретические и практические аспекты понятия электронной цифровой подписи, содержание норм Российского права, регламентирующих использование электронной подписи, алгоритм цифровой подписи с использованием ГОСТ Р 34.10-2012, механизм биометрической аутентификации в операционной системе Android.

Дипломная работа состоит из введения, 5 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 67 страниц, из них 47 страниц – основное содержание, включая 21 рисунок и 2 таблицы, список использованных источников из 18 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел дипломной работы «Понятие и виды ЭП» содержит описание и объяснение, что такое электронная подпись (ЭП), где она применяется, подробно рассмотрены применяемые в России виды ЭП и их юридическая сила:

1) Простая электронная подпись (ПЭП) – это коды доступа из СМС, коды на скретч-картах, пары «логин-пароль» в личных кабинетах на сайтах и в электронной почте.

2) Неквалифицированная электронная подпись (НЭП):

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

3) Квалифицированная электронная подпись (КЭП) соответствует все признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате, структура которого определена приказом ФСБ № 795 от 27.12.2011г;
- для создания и проверки используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным ФЗ №63 «Об электронной подписи» от 06.04.2011г.

В разделе описаны основные процедуры ЭП, такие как процедура формирования электронной подписи и процедура проверки электронной подписи.

Были детально рассмотрены применяемые на данный момент алгоритмы ЭП, проанализированы их недостатки и преимущества:

- алгоритм цифровой подписи RSA (аббревиатура от фамилий Rivest, Shamir и Adleman);
- алгоритм цифровой подписи Эль Гамаля (EGSA);
- алгоритм цифровой подписи DSA.

Второй раздел «Алгоритм электронной подписи ГОСТ Р 34.10-2012» посвящен анализу Российского стандарта «ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», описывающий алгоритмы формирования и проверки электронной подписи.

Данный алгоритм разработан главным управлением безопасности связи Федерального агентства правительственной связи и информации при Президенте Российской Федерации при участии Всероссийского научно-исследовательского института стандартизации. Разрабатывался взамен ГОСТ Р 34.10-94 для обеспечения большей стойкости алгоритма. Стойкость алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001 основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости хэш-функции.

Во второй части данного раздела были подробно рассмотрены алгоритмы формирования и проверки ЭП ГОСТ Р 34.10-2012, а также описаны преимущества и недостатки в сравнении с международным стандартом DSA.

В третьем разделе «Особенности реализации ЭП в ОС Android» описана операционная система Android с открытым исходным кодом, созданная для мобильных устройств на основе модифицированного ядра Linux. Под управлением Android работают два с половиной миллиарда различных устройств, что делает данную ОС самой распространённой на рынке мобильных устройств. На рисунке 1 приведена иллюстрация сегментации рынка ОС мобильных устройств.

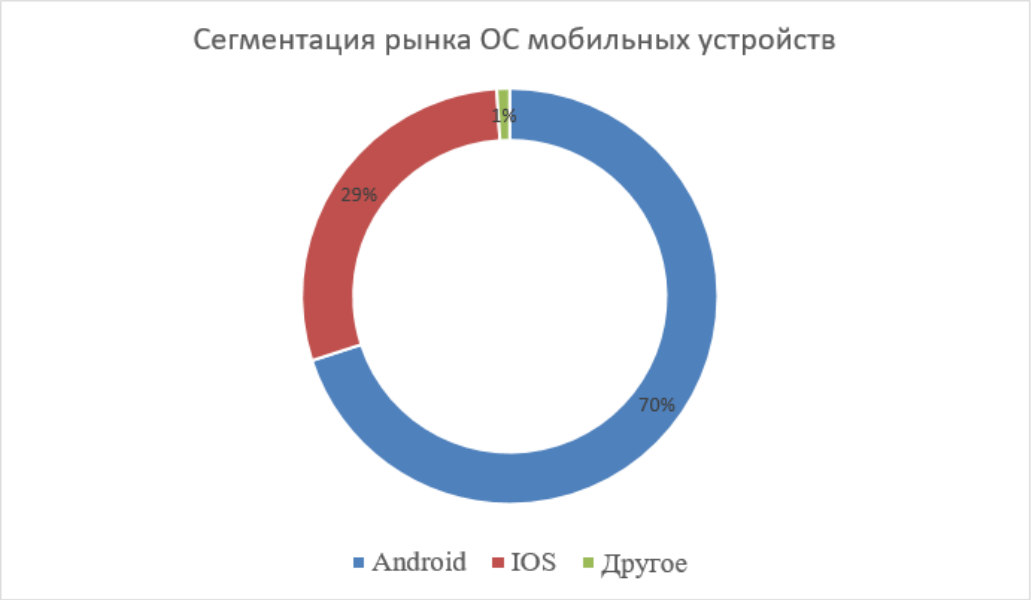

Рисунок 1 – Сегментация рынка ОС мобильных устройств

Во второй части раздела описана архитектура ОС Android и используемая в практической части библиотека Bouncy Castle, в которой представлена обширная функциональность из области криптографии. Библиотека обладает следующими основными характеристиками:

- содержит провайдер для JCE и JCA (компоненты безопасности в Java: JCA – архитектура криптографии Java и JCE – расширении криптографии Java с функцией шифрования);
- поддерживает спецификации ASN.1 (стандарт записи, описывающий структуры данных для представления, кодирования, передачи и декодирования) кодирования объектов;
- поддержка сертификатов X.509 (стандарт для инфраструктуры открытого ключа) различных версий;
- поддержка стандартов OpenPGP (открытый протокол шифровая электронной почты с использованием криптографии с открытым ключом), OCSP (протокол состояния сетевого сертификата), TSP («штамп времени» – криптографический протокол, позволяющий создавать доказательство факта существования электронного документа на определенные момент времени) и др.

В четвёртом разделе работы рассматриваются биометрические средства аутентификации, их преимущества и недостатки. Биометрические системы образуются аппаратной и программной частями. Аппаратная часть представляет собой биометрические сканеры, которые считывают биометрические особенности с физического объекта и создают их цифровую копию (модель). Программное обеспечение предназначено для обработки сформированной в результате считывания сканером биометрической информации и сверки ее с базой данных для идентификации личности.

Также приведена классификация современных биометрических средств, что показано на рисунке 2.

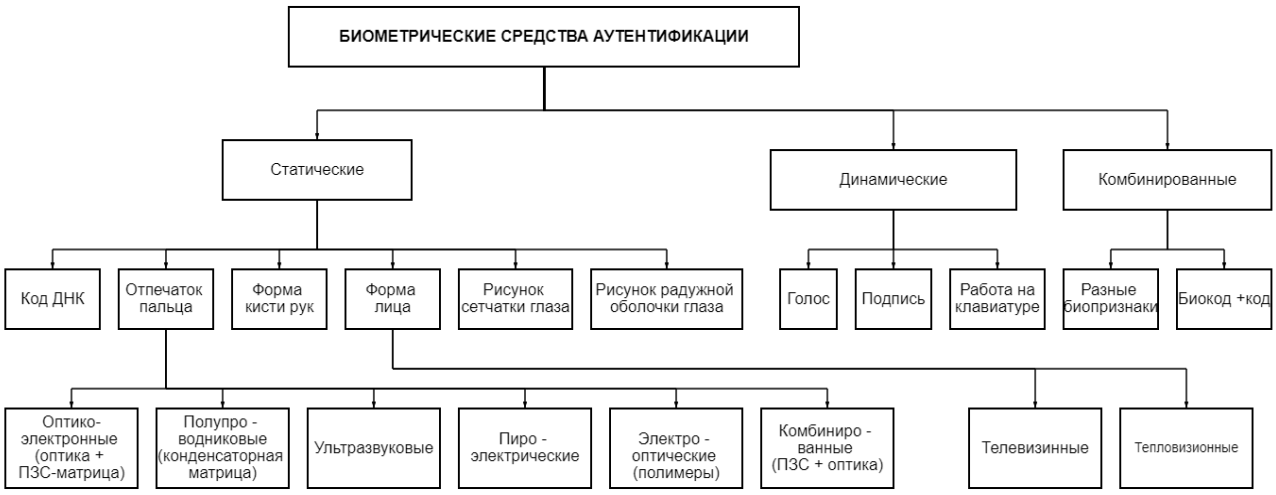

Рисунок 2 – Классификация современных биометрических средств аутентификации

Во второй части раздела более подробно рассмотрена аутентификация с использованием отпечатков пальцев. Эта технология доминирует на рынке, занимая более 50% от его объема (по данным Acuity Marcet Intelligence). Метод сканирования отпечатков пальцев легок в использовании и надежен. Основным устройством данного метода биометрической аутентификации является сканер, имеющий небольшие размеры и относительно низкую цену.

В третьей части раздела описаны основные параметры оценки точности биометрических средств:

- FAR (False Acceptance Rate) – коэффициент ложного пропуска, т.е. процент возникновения ситуаций, когда система разрешает доступ пользователю, незарегистрированному в системе.
- FRR (False Rejection Rate) – коэффициент ложного отказа, т.е. отказ в доступе настоящему пользователю системы.

На основании данных параметров проведён статистический сравнительный анализ популярных на текущий момент методов биометрический аутентификации, который пкоазан в таблице 1.

Таблица 1 – Статистические характеристики методов биометрической аутентификации

Метод биометрической аутентификации	FAR	FRR
Отпечаток пальца	0,001%	0,6%
Распознавание лица 2D	0,1%	2,5%
Распознавание лица 3D	0,0005%	0,1%
Радужная оболочка глаза	0,00001%	0,016%
Сетчатка глаза	0,0001%	0,4%
Рисунок вен	0,0008%	0,01%

Пятый раздел – это раздел программной реализации мобильного приложения. В данном разделе были описаны преимущества файлов формата PDF, в силу которых данный тип документов был выбран для формирования ЭП:

- возможность открыть в любой ОС;
- документ PDF может содержать не только текстовые и табличные данные, но и аудио и видеозаписи, инженерную графику, трехмерные модели;
- для дополнительной обработки PDF-документов в данный формат включен такой мощный инструмент как поддержка JavaScript для изменения содержимого в формах и полях по наступлению какого-то события или выполнению действия пользователя;
- инструменты Adobe Systems (разработчика формата PDF) поддерживают использование электронной подписи;

- в отличие от сообщений с присоединенной усиленной электронной подписью стандарта PKCS#7 и его усовершенствования CAdES, для просмотра документа PDF с подписью не требуется дополнительное специальное ПО, кроме криптографического провайдера, который требуется во всех случаях.

Приведено описание структуры проекта с особенностями программной реализации отдельных модулей. Описан интерфейс программы, с помощью которого происходит управление функционалом приложения. Также в данном разделе рассмотрены процессы формирования и проверки подписи PDF документов с использованием разработанного приложения. Примеры работы прогрыммы приведены на рисунке 3.

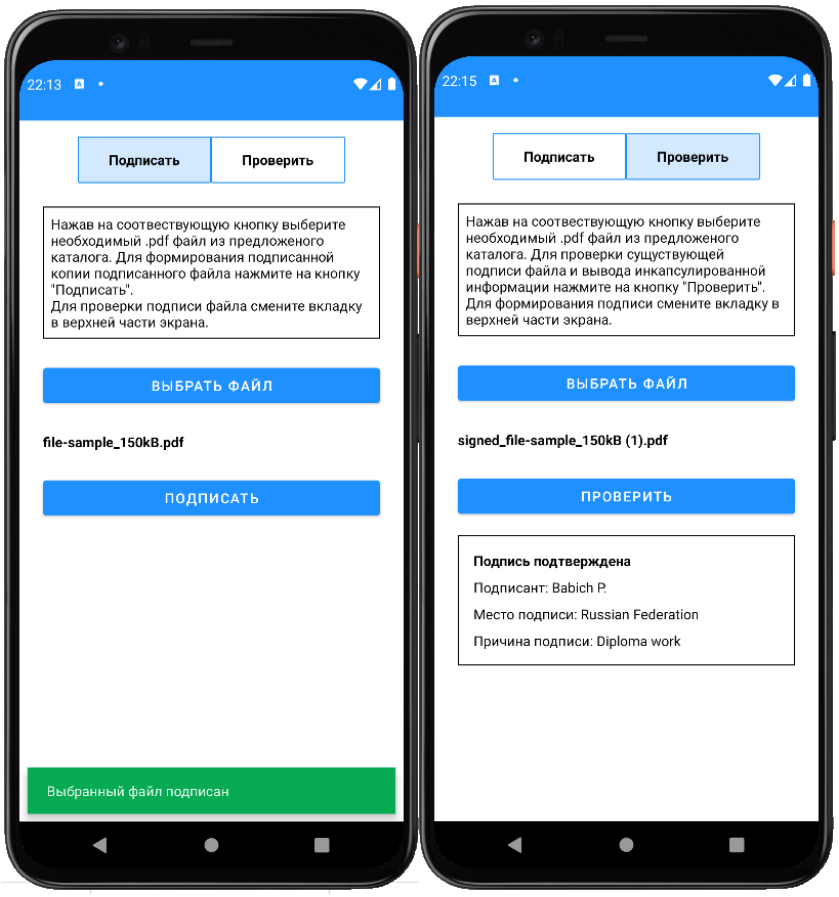

Рисунок 3 – Результат работы приложения

В конце раздела дано описание оборудования, на котором проводилось тестирование разработанного приложения, описаны данные совместимости с различными версиями ОС Android.

ЗАКЛЮЧЕНИЕ

Основными преимуществами использования ЭП является скорость, надежность, уход от традиционного бумажного документооборота, независимость от территориальной расположенности двух сторон сделки. Применение ЭП имеет широкие перспективы внедрения во многих сферах деятельности современного общества. Наиболее востребованной электронная подпись может быть в следующих сферах:

- электронный документооборот государственных (корпоративных) структур;
- электронная отчетность;
- банковская сфера;
- электронная медицина;
- энергетика;
- кредитные бюро;
- рынок ценных бумаг.

Требования, предъявляемые к электронной подписи в России, содержатся в Федеральном законе от 06.04.2011 №63-ФЗ и в Приказе ФСБ РФ от 27.12.2011 №796. Они определяют структуру и содержание требований к ЭП, к средствам ЭП, требований к средствам удостоверяющего центра.

В настоящей работе был проведен анализ алгоритмов цифровой подписи, с помощью языков программирования Kotlin и Java разработана программа, которая осуществляет процедуру подписи сообщения и процедуру проверки подписи на операционной системе Android. Реализованное приложение осуществляет формирование и проверку электронной подписи по алгоритму ГОСТ Р 34.10-2012, что позволяет быть ей при необходимости быть сертифицированной на территории России. Согласно предъявляемым требованиям к ЭП созданный программный комплекс формирует неквалифицированную электронную подпись к документу.

Программных продуктов, основанных на отечественных алгоритмах и использующих мобильное приложение крайне мало на текущий момент на рынке. Приложение, реализованное в ходе данной работы, предоставляет пользователям функционал формирования и проверки ЭП на некоммерческой основе в купе с удобным, интуитивно понятным интерфейсом.