Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Реализация защищенного электронного документооборота для платформы Android с использованием ГОСТ-шифрования

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Стрепетова Евгения Геннадьевича

Научный руководитель

доцент, к. п. н. _____ А.С. Гераськин

31.12.2016 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

31.12.2016 г.

Саратов 2017

ВВЕДЕНИЕ

Тема внедрения электронного документооборота в данный момент является интересной и актуальной для организации любого типа.

Автоматизация документооборота дает новые возможности любой организации по ускорению работы и оптимизации внутренних процессов. Автоматизация документооборота позволяет организациям существенно упростить вопросы, связанные с поиском, доступом и хранением документов, и как следствие избежать многих проблем, возникающих в процессе ведения документооборота.

В настоящее время широко применяются мобильные устройства и в связи с этим одно из требований, которое предъявляется к любой системе, работающей с документами – это возможность работы с мобильных устройств. На данным момент самой распространенной мобильной платформой является Android.

Целью данной работы является создание программного продукта, реализующего систему электронного документооборота факультета университета с использованием мобильного клиента на платформе Android с двухфакторной аутентификацией.

Для достижения поставленной цели ставятся следующие задачи:

1) Изучить теоретические сведения, связанные с юридической значимостью электронных документов и электронным документооборотом;

2) Рассмотреть существующие СЭД, поддерживающие работу с мобильных устройств;

3) Провести анализ токен-устройств в качестве средств электронной подписи и выбрать наиболее подходящее для работы с мобильных устройств;

4) Разработать систему электронного документооборота с мобильным клиентом на платформе Android.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 3 приложений. Общий объем работы – 90

страниц, из них 42 страницы – основное содержание. Список использованных источников состоит из 17 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В главе 1 приводятся необходимые определения, используемые в работе, в том числе электронный документ, электронный документооборот, СЭД, метаданные электронного документа, электронная подпись и т.д. Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. Система электронного документооборота (СЭД) - организационно-техническая система, обеспечивающая процесс создания, управления доступом и распространения электронных документов в компьютерных сетях, а также обеспечивающая контроль над потоками документов в организации.

Так же в первом разделе производится анализ некоторых существующих программных продуктов, реализующих электронный документооборот и поддерживающих работу с мобильных устройств (EOSmobile, 1С Документооборот). По результатам анализа были выявлены недостатки обоих программных продуктов. Мобильный клиент «1С Документооборот» не поддерживает электронную подпись документов. Программный продукт EOSMobile обладает высокой стоимостью для внедрения в рамках университета.

В Главе 2 приводятся определения аутентификации, многофакторной аутентификации, токен-устройства. Аутентификация – это проверка принадлежности субъекту доступа предъявленного им идентификатора. Многофакторной аутентификацией называют аутентификацию, при которой используются аутентификационные признаки разных типов. Принято выделять следующие факторы: «нечто, нам известное» (пароль), «нечто, нам присущее»

(биометрика) и «нечто, у нас имеющееся» (например, токен-устройство). Токен-устройство представляет собой компактное устройство в виде USB-брелока, которое служит для авторизации пользователя, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения любых персональных данных. В токене могут храниться пароли, цифровые сертификаты, ключи шифрования и электронно-цифровые подписи.

Далее в разделе проводится сравнительный анализ токен-устройств линейки Рутокен. По результатам анализа было выявлено, что модели Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП Flash и Рутокен ЭЦП Bluetooth поддерживают работу с мобильными устройствами на платформе Android и могут выступать в качестве средства электронной подписи. Принимается решение об использовании Рутокен ЭЦП в качестве средства двухфакторной аутентификации, так как данная модель обладает самой низкой стоимостью. А так же рассматривается стандарт PKCS#11, описывающий взаимодействие с криптографическими токен-устройствами.

В главе 3 описываются рабочие процессы и участники электронного документооборота на примере работы факультета университета, для которых разрабатывается система электронного документооборота предназначенная для контроля и учета успеваемости студентов. В системе законные пользователя могут иметь 3 различные роли: документовед, преподаватель, декан. В качестве документов в системе выступают ведомости различного вида: зачетная, экзаменационная и ведомость посещаемости. Сам программный продукт состоит из 3 модулей: сервера, клиента для PC-устройств и клиента для мобильных устройств на платформе Android. Все 3 модуля написаны на языке Java версии 1.7. Далее подробно описываются все этапы взаимодействия с реализованным программным продуктом: двухфакторная аутентификация в систему, создание ведомостей, подпись ведомости и проверка электронной

подписи, отправка ведомости в архив. Описание работы программы сопровождается соответствующими снимками экрана.

Работа завершается следующими приложениями с исходным кодом модулей программного продукта:

1) Приложение А. Листинг серверного модуля;
2) Приложение Б. Листинг клиента для PC-устройств;
3) Приложение В. Листинг мобильного клиента.

ЗАКЛЮЧЕНИЕ

В данной работе были изучены сведения, связанные с электронными документами и электронным документооборотом, рассмотрены некоторые программные продукты, реализующие защищенный электронный документооборот на мобильных устройствах.

В ходе дипломной работы был изучен протокол взаимодействия с токен-устройствами, проведен анализ существующих token-устройств фирмы «Актив». По результатам исследования было выбрано устройство Рутокен ЭЦП в качестве средства электронной подписи и средства двухфакторной аутентификации.

По результатам проделанной работы был разработан и реализован программный продукт, с помощью которого пользователи могут обмениваться документами, подписанными электронной подписью в соответствии ГОСТ Р 34.10-2001.

В системе реализована двухфакторная аутентификация на основе token-устройств линейки Рутокен, подпись и проверка подписи документов на основе стандарта ГОСТ Р 34.10-2001, а также удобный интерфейс для работы с документами.

Разработанная в рамках данной работы информационная система является примером настоящей системы, использующейся в университетах для контроля учебной дисциплины учащихся. Таким образом, все поставленные задачи были полностью решены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Янковая, В.Ф. Электронный документ как объект документоведения [Электронный ресурс] // журнал «Вестник Волгоградского государственного университета. Серия 2: Языкознание». 2013. №3.

2 Куняев, Н.Н., Дёмушкин, А.С., Фабричнов, А.Г. Конфиденциальное делопроизводство и защищенный электронный документооборот // М : Логос, 2011. 452 с.

3 Кириллов, А.Г., Коуров, А.В. Подготовка ВУЗа к внедрению системы электронного документооборота // Современные научные исследования и инновации. 2012. №1. [Электронный ресурс]. URL: http://web.snauka.ru/issues/2012/01/6734 (дата обращения: 19.11.2016).

4 Без росчерка пера [Электронный ресурс] // URL: https://cryptopro.ru/sites/default/files/blog/2014-11_14-lan.pdf (дата обращения 10.11.2016). Загл. с экрана. Яз. рус.

5 Корпоративная мобильность в СЭД/ECM: достижения, проблемы, перспективы [Электронный ресурс] // URL: https://www.pcweek.ru/ecm/article/detail.php?ID=164746 (дата обращения 15.10.2016). Загл. с экрана. Яз. рус.

6 Особенности организации бумажного и электронного документооборота [Электронный ресурс] // Elcomrevue [Электронный ресурс]: основы электронной коммерции. URL: http://elcomrevue.ru/osobennosti-organizatsii-bumazhnogo-i/ (дата обращения: 18.12.2016). Загл. с экрана. Яз. рус.

7 Android Market Share [Электронный ресурс] // Idc.com [Электронный ресурс]: сайт. URL: http://www.idc.com/promo/smartphone-market-share/os (дата обращения 21.12.2016). Загл.с экрана. Яз. англ.

8 Обзоры и сравнения систем электронного документооборота [Электронный ресурс] // Ecm-obzor.blogspot.ru [Электронный ресурс]: сайт http://ecm-obzor.blogspot.ru/2015/02/blog-post.html (дата обращения 20.11.2016). Загл. с экрана. Яз. рус.

9 Федеральный закон от 06.04.2011 No 63-ФЗ «Об электронной подписи» [Электронный ресурс] // КонсультантПлюс [Электронный ресурс]: надежная правовая поддержка. URL: http://www.consultant.ru/document/cons_docLAW148793/ (дата обращения: 18.12.2016). Загл. с экрана. Яз. рус.

10 Обзор Рутокен Web [Электронный ресурс] // Rutoken.ru [Электронный ресурс]: сайт. URL: http://www.rutoken.ru/press-center/publication/2011-09-29.html (дата обращения 15.09.2016). Загл. с экрана.

11 PKCS #11: CRYPTOGRAPHIC TOKEN INTERFACE STANDARD [Электронный ресурс]. URL: http://www.emclink.net/emc-plus/rsa-labs/standards-initiatives/pkcs-11-cryptographic-token-interface-standard.html (дата обращения 15.11.2016). Загл. с экрана. Яз. англ.

12 Встраивание устройств Рутокен через PKCS#11 [Электронный ресурс] // Портал документации проекта Рутокен [Электронный ресурс] : сайт. URL: http://developer.rutoken.ru/pages/viewpage.action?pageId=13795364 (дата обращения 15.11.2016). Загл. с экрана. Яз. рус.

13 Форматы электронной подписи [Электронный ресурс] // Хабрахабр [Электронный ресурс] : сайт. URL: https://habrahabr.ru/company/aktiv-company/blog/191866/ (дата обращения 10.12.2016). Загл. с экрана. Яз. рус.

14 Криптографические возможности Рутокен [Электронный ресурс] // URL: http://developer.rutoken.ru/pages/viewpage.action?pageId=2228237 (дата обращения 16.09.2016). Загл. с экрана. Яз. рус.

15 Android Authentication [Электронный ресурс]. URL: https://source.android.com/security/authentication/index.html (дата обращения 21.09.2016). Загл. с экрана. Яз. англ.

16 Введение в Android NDK [Электронный ресурс]. URL: https://habrahabr.ru/post/203014/ (дата обращения 16.09.2016). Загл. с экрана. Яз. рус.

17 JavaFX Documentation [Электронный ресурс]. URL: http://docs.oracle.com/javase/8/javase-clienttechnologies.htm (дата обращения 10.09.2016). Загл. с экрана. Яз. рус.