Министерство образования и науки Российской Федерации

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

Кафедра теоретических основ компьютерной безопасности и криптографии

Система электронного документооборота с криптографической защитой информации

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы
специальности 090102.65 «Компьютерная безопасность»
факультета компьютерных наук и информационных технологий
Лазоренко Александра Павловича

Научный руководитель
доцент, к.ф.-м.н. А.В. Жаркова

Заведующий кафедрой
профессор, к.ф.-м.н. В.Н. Салий

Саратов 2016

ВВЕДЕНИЕ

В настоящее время широко применяются системы защиты и проверки подлинности информации, в которых используются электронные подписи. Они используются в определенных случаях, когда необходимо обеспечение полноты и достоверности. Для корректной реализации схем их внедрения и использования требуется немало усилий, однако они значительно уменьшают бумажный документооборот, упрощают идентификацию лица и являются полноценной заменой собственноручной подписи для документов, предусмотренных законом.

Целью данной работы является рассмотрение основных положений, связанных с юридической значимостью электронных документов, изучение необходимых стандартов и алгоритмов, в результате чего требуется разработать и реализовать безопасную корпоративную информационную систему для обеспечения эффективного документооборота между ее участниками.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В подразделе 1.1 «Необходимые определения» раздела 1 «Необходимые сведения» приводятся основные определения, которые используются в дальнейших разделах при описании алгоритмов, протоколов и другой информации. В подразделе 1.2 «О юридической значимости электронных документов» приводятся основные положения из Федерального закона «Об электронной подписи» и общая информация об электронной подписи.

В разделе 2 «Некоторые программные продукты, реализующие электронную подпись» описываются в качестве примеров три программных продукта: КриптоАРМ, набор средств разработки Platform SDK CAPICOM и КриптоПро ЭЦП Browser plug-in.

В подразделе 3.1 «Хеш-функция ГОСТ Р 34.11-2012» раздела 3 «Необходимые алгоритмы» рассматриваются общие сведения о хеш-функциях, а также описание и сам алгоритм генерации хеша-кода из соответствующего стандарта. В подразделе 3.2 «Стандарт ГОСТ Р 34.10-2012» описывается процессы формирования и проверки электронной подписи соответственно стандарту.

В разделе 4 «Программное средство электронного документооборота» описывается структура разработанной и реализованной автором системы электронного документооборота, в которой законные пользователи могут обмениваться документами, подписанными электронной подписью в соответствии со стандартом ГОСТ Р 34.10-2012. Подробно описываются протоколы взаимодействия пользователей в системе, все этапы работы в системе, а именно регистрация, авторизация, загрузка и подпись документов, а также отправка их другим пользователям, приводится действующий в системе регламент. Описание работы программы сопровождается соответствующими снимками экрана.

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной работы были изучены законы и стандарты, связанные с авторизацией и обеспечением юридической значимости электронных документов, рассмотрены некоторые программные продукты, реализующие электронную подпись, изучены отечественные стандарты – функция хеширования ГОСТ Р 34.11-2012 и электронная цифровая подпись ГОСТ Р 34.10-2012.

В результате проделанной работы была разработана и реализована информационная система, с помощью которой законные пользователи могут обмениваться документами, подписанными электронной подписью в соответствии с ГОСТ Р 34.10-2012.

В системе реализованы регистрация и авторизация, подпись и проверка подписи документов на основе стандарта ГОСТ Р 34.10-2012, а также удобный обмен документами.

Разработанная в рамках данной работы информационная система может быть примером настоящей корпоративной системы, использующейся в организациях для ведения электронного документооборота.

Таким образом, все поставленные задачи были полностью решены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Авторизация [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/Авторизация (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

2 Салий, В. Н. Криптографические методы и средства защиты информации : учеб. пособие // СГУ – Саратовский государственный университет [Электронный ресурс] : [сайт]. URL: http://www.sgu.ru/sites/default/files/textdocsfiles/2015/11/09/saliy_v.n._kriptograficheskie_metody_i_sredstva_zashchity_informacii.pdf (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

3 Веб-приложение [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/Веб-приложение (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

4 Браузер [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/Веб-приложение (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

5 Регламент [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/Регламент (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

6 ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» [Электронный ресурс] // Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ) [Электронный ресурс]. URL: http://protect.gost.ru/document.aspx?control=7&id=180209 (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

7 Богомолов, А. М. Алгебраические основы теории дискретных систем / А. М. Богомолов, В. Н. Салий. М. : Наука. Физматлит, 1997. 368 с. : ил.

8 Основы криптографии : учеб. пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. М. : Гелиос АРФ, 2002. 480 с. : ил.

9 ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» [Электронный ресурс] // Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ) [Электронный ресурс]. URL: http://protect.gost.ru/document.aspx?control=7&id=180151 (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

10 Особенности организации бумажного и электронного документооборота [Электронный ресурс] // Elcomrevue [Электронный ресурс] : основы электронной коммерции. URL: http://elcomrevue.ru/osobennosti-organizatsii-bumazhnogo-i/ (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

11 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // КонсультанПлюс [Электронный ресурс] : надежная правовая поддержка. URL: http://www.consultant.ru/document/cons_doc_LAW_156802/ (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

12 Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» [Электронный ресурс] // КонсультанПлюс [Электронный ресурс] : надежная правовая поддержка. URL: http://www.consultant.ru/document/cons_docLAW148793/ (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

13 Электронная цифровая подпись [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/Электронная_цифровая_подпись (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

14 КриптоАРМ [Электронный ресурс] // Цифровые технологии [Электронный ресурс]. URL: http://www.trusted.ru/products/cryptoarm/ (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

15 Platform SDK CAPICOM [Электронный ресурс] // Microsoft Россия [Электронный ресурс] : устройства и сервисы. URL: http://www.microsoft.com/ru-ru/download/details.aspx?id=25281 (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

16 КриптоПро ЭЦП Browser plug-in [Электронный ресурс] // Криптопро [Электронный ресурс] : ключевое слово в защите информации. URL : http://www.cryptopro.ru/products/cades/plugin/ (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.

17 Hash function of Stribog or in a city the new sheriff [Электронный ресурс] // Sysmagazine [Электронный ресурс]. URL: http://sysmagazine.com/posts/188152/ (дата обращения: 18.12.2015). Загл. с экрана. Яз. рус.