УДК 681.3.06

РАЗРАБОТКА ПОДСИСТЕМЫ УПРАВЛЕНИЯ КЛЮЧАМИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В РАМКАХ ТЕРМИНАЛЬНОЙ ФЕРМЫ

© 2017 В. Д. Камакин

Воронежский институт высоких технологий (г. Воронеж, Россия)

В данной работе дано описание основных характеристик подсистемы управления ключами в компании. Описаны основные модули, входящие в подсистему.

Ключевые слова: электронная цифровая подпись, модель ЭЦП.

Потоки документов отображают деятельность любой организации. От их правильного обращения напрямую зависит успех бизнеса, поэтому во все времена правильной организации документооборота уделялось достаточно внимания. С появлением компьютерных технологий в документообороте произошел прорыв – с документами стало возможным работать намного эффективнее, проще и быстрее, чем раньше.

Дело здесь не только в замене готовых типографских форм на электронные шаблоны, хранящиеся в компьютере, хотя одно это способно значительно увеличить производительность офисного труда. Прежде всего, электронный документооборот выгоден с точки зрения перемещения документов.

Документ в компьютерной форме – это набор кодов, которые легко пересылаются по компьютерным сетям, по электронной почте, легко тиражируются, редактируются и дополняются. Значительно проще разослать электронное письмо, чем отправлять с курьером или по обычной почте письмо бумажное.

В электронном делопроизводстве приняты следующие термины:

– база данных – совокупность взаимосвязанных данных, организованных по определенным правилам на машинных носителях;

– делопроизводство – деятельность, охватывающая документирование и организацию работы с документами;

– документ – структурированная совокупность информации, предназначенной для восприятия человеком, которая может быть цельным объектом обмена между пользователями и/или информационными системами;

– документационное обеспечение управления (ДОУ) – процесс производства, передачи и переработки документированной информации, необходимой для управления организацией;

– файл – идентифицированная совокупность информации на машинном носителе, поддерживаемая операционной системой, в среде которой осуществляется создание файла и/или обеспечивается доступ к нему;

– файл документа – файл, обеспечивающий передачу содержательной части электронного документа в неструктурированном электронном виде;

– формат файла – способ организации элементов информации в файле;

– электронный конверт – файл формата, предназначенный для передачи электронных документов из одной системы АСДОУ в другую; формат XML (Extensible Markup Language – открытый язык разметки) позволяет системам, использующим разные программные средства обработки и хранения данных, обмениваться структурированной информацией, обеспечивать ее правильное преобразование и представление в любой среде.

Электронные документы легко объединяются и формируют базы данных и знаний. Электронные библиотеки практически заменили неудобные и ограниченные библиотеки бумажных документов. Электронные каталоги открывают доступ к нужной информации в сотни раз быстрее, чем это было возможно при работе с бумажными или карточными каталогами.

Подсистема автоматизирует решение следующих задач в сфере работы ООО «СервисКлауд» по работе с ключами электронной цифровой подписи в рамках терминальной фермы:

Камакин Виктор Дмитриевич – ВИВТ-АНОО ВО, kam13akin2045@yandex.ru.

– повышение конфиденциальности информационного обмена даже при использовании открытых каналов связи сети Интернет;

– снижение вероятности возникновения конфликтных ситуаций, связанных с обеспечением подлинности электронных документов по сравнению с аналогичными документами на бумажных носителях;

– обеспечение максимально возможной автоматизации документооборота и интеграции с корпоративной учётной системой;

– обеспечение возможности согласования документов в электронной форме, отправки уведомлений о получении и принятии электронных документов к исполнению в режиме реального времени;

– сокращение сроков и упрощение порядка формирования документов; обмен электронными документами осуществляется в любое время суток, что важно для контрагентов из других регионов;

– сокращение непроизводственных издержек на печать, пересылку и хранение документов (в том числе подтверждающих внутренние операции в компании);

– снижение расходов на курьерскую и почтовую связь.

В рамках создания подсистемы четыре модуля с соответствующими функциями для создания ключей ЭЦП, хранения ключей ЭЦП, подписания документов с помощью ключей ЭЦП, распространение ключей ЭЦП в рамках терминальной фермы. Эти модули позволят автоматизировать работу с ключами ЭЦП в рамках терминальной фермы.

В результате использования подсистемы «ЭЦП» в процессе производственной деятельности компании планируется повышение уровня информационной безопасности компании ООО «СервисКлауд».

Нами были представлены основные этапы проектирования и программной реализации подсистемы «ЭЦП»:

- концептуальное проектирование;
- общесистемные решения;
- математическое обеспечение подсистемы «ЭЦП»;
- информационное обеспечение подсистемы «ЭЦП»;
- техническое обеспечение подсистемы «ЭЦП»;
- программное обеспечение;
- организационное обеспечение.

ООО «СервисКлауд» – компания в сфере информационных технологий. Основное направление деятельности – предоставление полного доступа к программам 1С через Интернет. Основана в 2011 году.

Главным приоритетом в работе «СервисКлауд» является стабильность и предсказуемость работы систем. При этом везде, где это возможно, компания использует самые современные технологии. На сегодняшний день ключевыми компетенциями компании «СервисКлауд» являются:

– системы производственного учёта и планирования;

– разработка и сопровождение систем для торговли - в том числе и для торговли товарами с различными особенностями партионного учета (наличие сроков годности, дат розлива, сертификатов и т. п.);

– подключение и настройка торгового оборудования (сканеры штрихкода, принтеры этикеток, терминалы сбора данных, системы контроля допуска, карт-ридеры магнитных и прокси-карт);

– сопровождение бухгалтерского программного обеспечения с внесением изменений по требованиям заказчика, поддержка в актуальном состоянии регламентированной отчётности и релизов конфигураций;

создание систем распределенной обработки информации (в режиме он-лайн, пакетном режиме или в смешанном он-лайн/пакетном режиме).

В состав разрабатываемой системы будут входить следующие модули:

– модуль создания крипто-ключей пользователей в рамках терминальной фермы. Модуль должен обеспечивать возможность создания ключей ЭЦП в рамках терминальной фермы.

— модуль хранения списка крипто-ключей пользователей. Модуль должен обеспечивать возможность проверки ЭЦП при загрузке документов.

– модуль взаимодействия пользователей с крипто-ключами ЭЦП в облачной среде. Модуль должен обеспечивать получение пользователем ЭЦП подтверждающего сообщения.

– модуль подписания файлов с помощью ЭЦП. Модуль должен обеспечивать возможность подписания ЭЦП всех файлов в рамках терминальной фермы.

Реализация данных модулей позволит обеспечить автоматизацию работы с

ключами ЭЦП в рамках терминальной фермы.

Входными данными будут являтся

- список пользователей
- документ для подписания ЭЦП

Ключи для подписания документов с помощью ЭЦП генерирутся в процессе работы подсистемы

Выходными данными являются документы, подписанные ЭЦП.

В подсистеме «ЭЦП», субъект, желающий пересылать подписанные им документы, должен сформировать два ключа алгоритма RSA: открытый и закрытый.

Пару значений (*KO, r*), которая является открытым ключом подписи, отправитель передает всем возможным получателям его сообщений. Именно эти значения будут использоваться для проверки подлинности и принадлежности отправителю полученных от него сообщений.

В ходе работы подсистемы «ЭЦП», выполняеются следующие этапы:

- подсистема «ЭЦП», используя сетевую модель дотупа, обращается к совокупности доступных терминальных серверов. На каждом сервере анализируется ветвь реестра Windows, в которой хранятся ЭЦП.
- данные, полученные в результате анализа накапливаются в массиве данных о ключах ЭЦП по каждому терминальному серверу. ключевым параметром, построенного массива является уникальный идентификатор сети (SSID)
- выполняется сортировка массива данных о ключах ЭЦП на основе SSID
- выводит список данных о ключах ЭЦП, хранящихся на терминальных сереверах для пользователя.

ЛИТЕРАТУРА

1. Кострова В. Н. Оптимизация распределения ресурсов в рамках комплекса общеобразовательных учреждений / В. Н. Кострова, Я. Е. Львович, О. Н. Мосолов // Вестник Воронежского государственного технического университета. – 2007. – Т. 3. – № 8. – С. 174-176.

2. Преображенский Ю. П. Разработка методов формализации задач на основе семантической модели предметной области / Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 075-077.

3. Львович И. Я. Факторы угрозы экономической безопасности государства / И. Я. Львович, А. А. Воронов, Ю. П. Преображенский // Информация и безопасность. – 2006. – Т. 9. – № 1. – С. 36-39.

4. Черников С. Ю. Использование системного анализа при управлении организациями / С. Ю. Черников, Р. В. Корольков // Моделирование, оптимизация и информационные технологии. – 2014. – № 2 (5). – С. 16.

5. Воронов А. А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А. А. Воронов, И. Я. Львович, Ю. П. Преображенский, В. А. Воронов // Информация и безопасность. – 2006. – Т. 9. – № 2. – С. 8-11.

6. Фомина Ю. А. Принципы индексации информации в поисковых системах / Ю. А. Фомина, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2010. – № 7. – С. 98-100.

7. Преображенский Ю. П. Информационная безопасность – вызовы современного мира / Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2017. – № 2 (21). – С. 60-63.

8. Маричев А. В. Вопросы социальной инженерии в корпоративной информационной безопасности / А. В. Маричев, И. В. Любимов, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2017. – № 2 (21). – С. 64-67.

9. Львович И. Я. Основы информатики / И. Я. Львович, Ю. П. Преображенский, В. В. Ермолова // Воронеж, Издательство: Воронежский институт высоких технологий (Воронеж), 2014. – 339 с.

10. Паневин Р. Ю. Структурные и функциональные требования к программному комплексу представления знаний / Р. Ю. Паневин, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 061-064.

THE COMPARATIVE ANALYSIS OF CLASSICAL AND SPECIAL ALGORITHMS AND SCHEMES OF THE DIGITAL SIGNATURE

© 2017 V. D. Kamakin

Voronezh Institute of High Technologies (Voronezh, Russia)

In this work the main characteristics of the subsystem key management in the company. Describes the basic modules included in the subsystem.

Key words: electronic digital signature algorithms.