Список использованных источников

1. Модельные системы поддержки принятия решений в АСУ ТП доменной плавки / Н.А. Спирин, В.В. Лавров, В.Ю. Рыболовлев, А.В. Краснобаев, О.П. Онорин, И.Е. Косаченко ; под ред. Н.А. Спирина. Екатеринбург: УрФУ, 2011. 462 с.
2. Компьютерные методы моделирования доменного процесса / О.П. Онорин, Н.А. Спирин, В.Л. Терентьев, Л.Ю. Гилева, В.Ю. Рыболовлев, И.Е. Косаченко, В.В. Лавров, А.В. Терентьев ; под ред. Н.А. Спирина. Екатеринбург: УГТУ–УПИ, 2005. 301 с.
3. *Троелсен Э.* Язык программирования C# 2010 и платформа .NET 4 : [пер. с англ.] / Э. Троелсен. СПб.: Вильямс, 2010. 1392 с.

СИСТЕМА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ДОКУМЕНТОВ НА ПРИМЕРЕ КРУПНОГО ВУЗА

© А.С. Добрынин, 2012

ФГБОУ ВПО «Сибирский государственный индустриальный университет», г. Новокузнецк

Проблема обработки большого количества документов стоит перед высшими учебными заведениями достаточно остро. Несмотря на большое количество систем электронного документооборота, на практике работа с документами осуществляется вручную, бумаги циркулируют по отделам, теряются, сотрудникам приходится решать множество дополнительных, рутинных задач на своем рабочем месте. Внедрение систем безбумажного документооборота и подписи документов позволит ускорить бизнес-процессы, связанные с обработкой документов.

Ежедневно высшие учебные заведения решают множество задач, связанных с оформлением на работу новых сотрудников, подготовкой распоряжений и актов, созданием рабочих программ и учебно-методических комплексов, формированием карт поручений для профессорско-преподавательского состава и т.д. Решение этих задач в учебном заведении, как и в абсолютном большинстве других организаций, упирается в том или ином виде в обработку бумажных носителей информации, поскольку требуются подписи ответственных лиц. Абсурдность подобного подхода очевидна – современные информационные технологии позволяют решать поставленные задачи без использования бумажных носителей вообще. Более того, использование бумажных носителей информации в учебном заведении, скорее, приносит вред организации, чем пользу. Значительные денежные средства переводятся впустую, так как закупка принтеров, бумаги, новых картриджей – достаточно дорогостоящие мероприятия, не говоря о неэффективном использовании рабочего времени сотрудников, которые занимаются бесполезной работой.

Формирование безбумажного документооборота в организации может быть реализовано путем решения двух взаимосвязанных задач:

1) Разработка цифрового аналога подписи должностного лица на документе, вместо росписи лица на бумажном документе.
2) Реализация механизмов проверки подлинности документа и обеспечение невозможности отказа от авторства документа для должностного лица, выполнившего подпись цифрового документа.

Цифровым аналогом бумажной подписи для документа может являться уникальный идентификатор, однозначно идентифицирующий сотрудника в организации и закрепленный за конкретным должностным лицом. В данной работе в качестве такого идентификатора (аналога росписи на документе) предлагается использовать GUID – глобальный уникальный

идентификатор. Современные мощные алгоритмы генерации GUID позволяют решать задачи генерации уникальных номеров в пределах мировых компьютерных систем. Таким образом, сгенерированный уникальный GUID для сотрудника в организации не может быть одинаковым не только для сотрудника в отдельной организации, но и во всем мире.

Реализация механизмов подлинности документа и обеспечение невозможности отказа от авторства может базироваться на механизмах современной криптографии [1; 2] с открытым ключом. В данной работе рассматривается возможность применения алгоритма RSA (Rivest Shamir Adelman) для решения поставленной задачи. По аналогии с задачами защиты данных в крупных распределенных системах, задача подписи документа может быть решена в два этапа:

1) Создание хэша цифрового документа (файла) с использованием известных методик, таких как CRC, MD5, SHA1 [2]. В данной работе рекомендуется использовать алгоритм SHA1.

2) Шифрование хэша закрытой составляющей ассиметричного ключа по алгоритму RSA [2] и запись полученного значения в файл или базу данных, которые, в свою очередь, могут быть зашифрованы по определенной технологии симметричного ключа.

В силу ограниченного объема статьи, вопросы формирования цифрового аналога бумажной росписи для сотрудника здесь подробно не рассматриваются.

Ключевая идея, заложенная в реализации данной системы, предполагает применение клиент-серверного механизма взаимодействия между компонентами распределенной системы, в котором клиенты обладают полной информацией о фрагменте собственной базы данных ключей и подписанных файлов, не имея информации о фрагментах базы данных сотрудников других отделов. Таким образом, сотрудники отдельно взятого отдела могут подписывать только свои собственные файлы. В процессе выполнения процедуры репликации ключей и подписанных файлов на сервер последний формирует единую общую базу данных ключей и подписанных файлов, состоящую из фрагментов локальных баз данных клиентов. Рассмотренная процедура представлена на рис. 1.

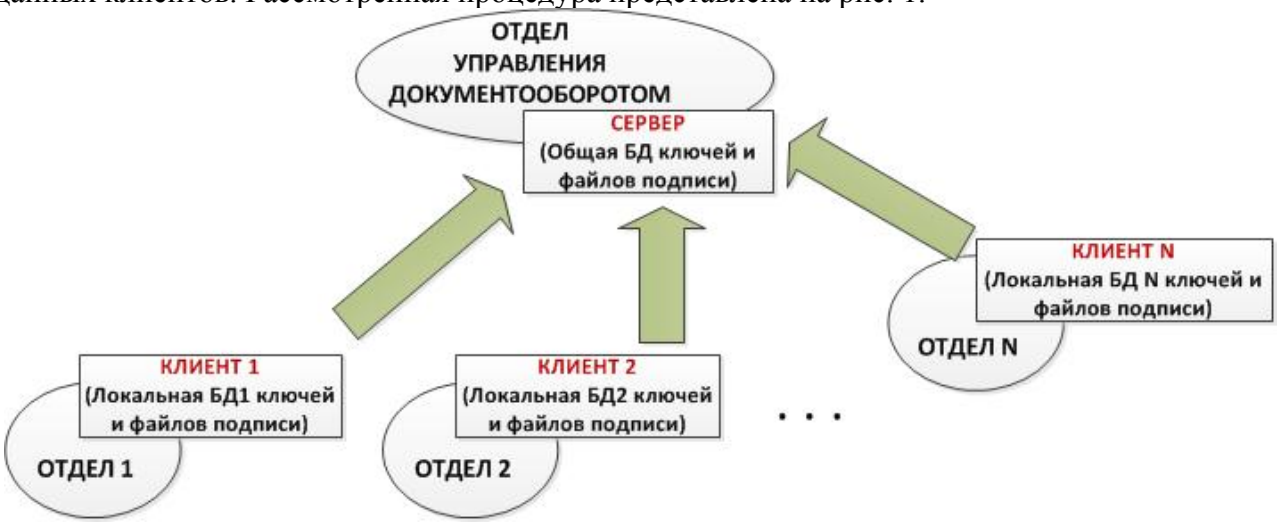

Рис. 1. Схема взаимодействия компонентов системы цифровой подписи

Данный механизм может функционировать как в файловом варианте, так и на базе реляционных систем управления базами данных, таких как MS SQL Server 2008 или Oracle 11g. Использование баз данных для хранения цифровых ключей и сигнатур цифровой подписи – более предпочтительный вариант, поскольку позволяет существенно повысить уровень безопасности системы в целом [1]. Репликация ключей может осуществляться двояко:

- *Репликация по расписанию*. Все изменения, внесенные в файлы ключей и файлы подписи документов, передаются на сервер в определенный момент времени. Данный режим

может использоваться для снижения нагрузки на корпоративную сеть организации (например, запуск процедур репликации в момент простоя сети, по вечерам).

- *Непосредственная репликация*. Все изменения, внесенные в файлы ключей и файлы электронной подписи, передаются на сервер немедленно, после внесения изменений.

В данной работе приведен обзор механизмов, предназначенных для клиентской части системы цифровой подписи документов. Клиентская часть может быть использована как в составе серверной части, так и отдельно, для небольших организаций. Упрощенно клиентскую часть можно рассматривать как систему, включающую пять основных подсистем:

1. Подсистему регистрации нового автора.
2. Подсистему цифровой подписи документов.
3. Подсистему проверки цифровой подписи документов.
4. Подсистему внесения цифровой росписи руководящего лица (GUID) в электронный документ.
5. Подсистему репликации данных.

Ниже представлено описание первых двух механизмов клиентской части системы. Обобщенно подсистема 1 регистрации нового автора предусматривает запись основных идентификационных параметров автора в файл ключей или базу данных. К идентификационным параметрам относятся: Имя, фамилия, должность, отдел [опционально], а также ассиметричный ключ и GUID. Соответствующий алгоритм показан на рис. 2.

Рис. 2. Алгоритм добавления нового автора документа

В клиентской части системы предусмотрено хранение файла ключей как в открытом виде (с использованием текстовых файлов), для упрощения работы с системой отдельных пользователей, так и в зашифрованном виде с применением симметричного алгоритма шифрования файла ключей AES (Advanced Encryption Standard) [2].

Алгоритм цифровой подписи документа включает следующие основные этапы: преобразование подписываемого документа в массив байт; применение процедуры хэширования документа по SHA1 [2]; преобразование полученного хэш-значения закрытой составляющей ассиметричного RSA [2] ключа. Принцип работы алгоритма представлен на рис. 3.

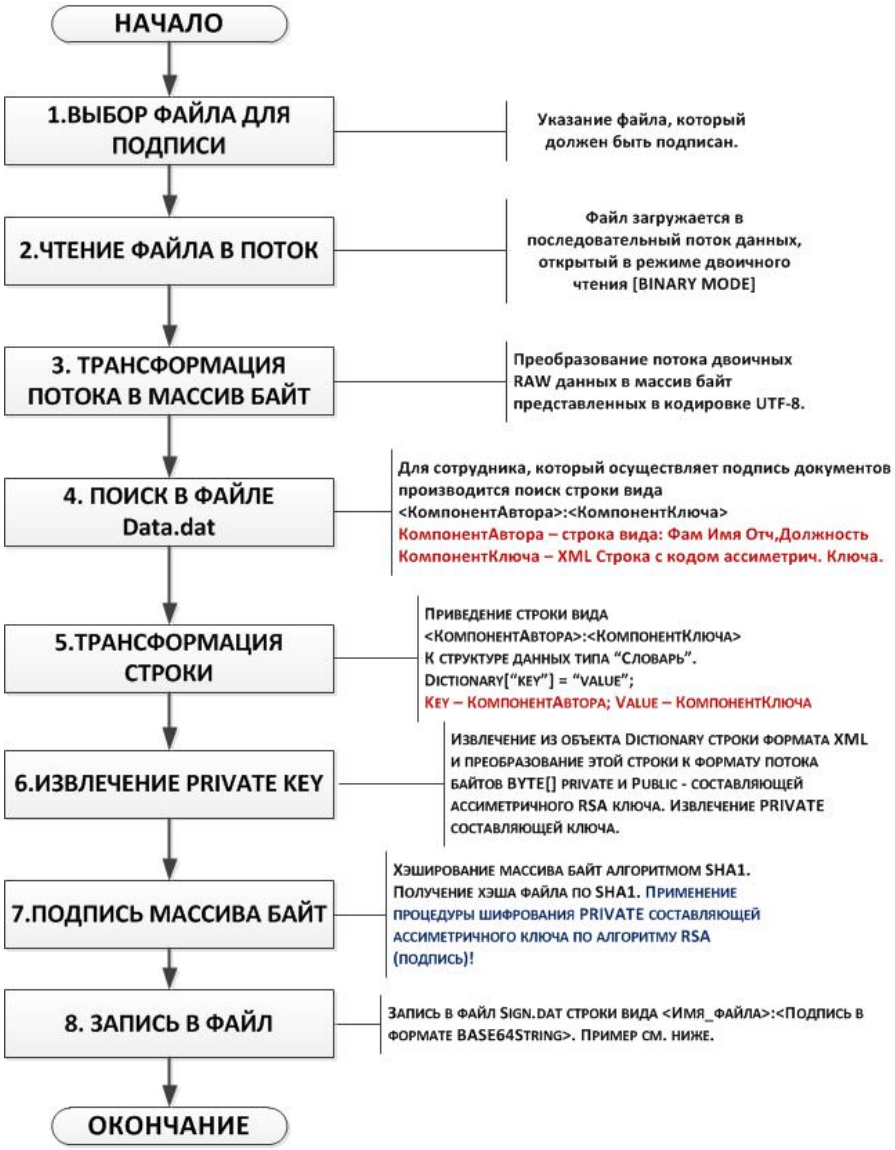

Рис. 3. Алгоритм цифровой подписи документа

Разработка и применение систем электронной цифровой подписи, реализованных по рассмотренному в данной статье принципу, позволит внедрить безбумажные технологии документооборота в высших учебных заведениях и в других коммерческих или промышленных организациях.

Список использованных источников

1. *Степанов Е.А.* Информационная безопасность и защита информации : учеб. пособие / Е.А. Степанов, И.К. Корнеев М.: Инфра, 2001. 304 с.

2. *Бабаш А.В., Шанкин Г.П., Применко Э.А.* Криптография / под редакцией В.П. Шерстюка. М.: СОЛОН, 2002. 512 с.

3. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты. М.: ДМК, 2000. 448 с.

4. Введение в криптографию / под. ред. В.В. Ященко. М.: Высшая школа, 2000. 169 с.

5. *Жельников В.В.* Криптография от папируса до компьютера. М.: ABF, 1996. 123 с.

5. *Баричев С., Серов Р.* Основы современной криптографии. М.: ПАИМС, 2001. 123 с.

6. *Молдовян Н.А.* Скоростные блочные шифры. СПб.: Издательство СПбГУ, 1998.

7. *Ярочкин В.И.* Информационная безопасность : учеб. пособие. М.: Международные отношения, 2001. 400 с.

РАЗРАБОТКА КОМПЛЕКСА ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ВЫПОЛНЕНИЯ РАСЧЕТОВ И ИССЛЕДОВАНИЯ ТЕПЛОВОГО БАЛАНСА ДОМЕННЫХ ПЕЧЕЙ

© Д.А. Жидков, В.В. Лавров, Н.А. Спирин, 2012
ФГАОУ ВПО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», г. Екатеринбург

Анализ эффективности тепловой работы любого теплотехнического агрегата, в том числе доменной печи, осуществляется на основе составления его теплового баланса. Исследование теплового баланса позволяет выявить узкие места в тепловой работе агрегата и предложить меры по их устранению или снижению их влияния [1].

Выполнение расчета теплового баланса доменной плавки – довольно трудоемкий процесс. Для его вычисления используется свыше тридцати показателей, не учитывая множества промежуточных величин, получаемых в ходе расчета. Расчет статей теплового баланса вручную занимает продолжительное время и может в итоге содержать в себе ошибки (необходимо учитывать влияние человеческого фактора).

Следует обозначить и иную проблему. Для того чтобы инженер-технолог мог выявить проблемы в тепловой работе печи или подобрать оптимальный тепловой режим, ему необходимо исследовать тепловой баланс агрегата за несколько отчетных периодов работы теплотехнического агрегата.

В связи с этим актуальными являются задачи автоматизации расчетов теплового баланса доменной печи, хранения исходных данных расчета и его результатов, предоставления инженерно-технологическому персоналу инструментария для просмотра и изучения полученных данных.

Цель данной работы заключалась в разработке информационной системы, которая выполняла бы перечисленные выше функции, предоставляя инженерам-технологам средства для реализации математического аппарата расчета теплового баланса, формирования отчетной документации и исследования закономерностей в полученных данных.

Для достижения этой цели были решены следующие задачи:

- определение требований к разрабатываемой системе;
- проектирование архитектуры системы, выбор программной платформы для ее реализации;
- изучение методики расчета теплового баланса доменной печи;
- разработка расчетной математической библиотеки dll, ее отладка и тестирование;
- разработка клиентского программного модуля для моделирования теплового режима плавки;
- проектирование (концептуальное, даталогическое, функциональное) и реализация базы данных для хранения исходных данных и результатов расчетов теплового баланса доменных печей;
- разработка хранимых процедур, реализующих расчет теплового баланса на базе функций, заложенных в математической dll-библиотеке;
- создание заданий серверу баз данных для автоматизации процесса расчета теплового баланса по расписанию;
- создание шаблонов отчетов Reporting Services для просмотра данных из базы с помощью Web-браузера;