Автономная работа с документами в СЭД

П. А. Куратов, Н. А. Петрова, Е. Л. Плискин

Аннотация. Для расширения возможностей использования системы электронного документооборота (СЭД) в качестве инфраструктуры для создания и движения документов в статье рассматривается задача организации работы участников документооборота в автономном режиме, без постоянного подключения к СЭД. Для поддержки автономной работы с документами предлагается включать в документы определенный объем сведений из СЭД. Такой внедренный в документ «контекст документооборота» может отображаться и изменяться при работе с документом в автономном режиме, с последующей загрузкой изменений в СЭД. Описывается пилотная реализация автономной работы с документами MS Office на базе СЭД Е1 Евфрат, включая сценарии исполнения поручений и создания новых поручений в автономном режиме.

Ключевые слова: *система электронного документооборота, безбумажная технология, автономный режим работы, контекст документооборота, цифровая подпись, MS Office, СЭД Е1 Евфрат.*

Введение

Основным режимом работы клиентов с системами электронного документооборота (СЭД) является режим «on-line», который характеризуется наличием постоянного подключения к СЭД. В начале сеанса связи клиент входит в СЭД, авторизуется, получает доступ к документам, и работает с ними под контролем СЭД.

Очевидно, что клиентам может быть не всегда удобно подключаться к СЭД, для того, чтобы получить доступ к документам для просмотра или редактирования. Иногда участник документооборота хотел бы некоторое время поработать с документами на своем компьютере в автономном режиме «офлайн», без подключения к СЭД. К сожалению, автономная работа с документами во многих СЭД поддерживается недостаточно. Некоторые СЭД позволяют редактировать документы только в пределах сеанса связи и отказываются принимать обратно документы, выгруженные из СЭД и отредактированные в режиме «офлайн». С выгруженными из СЭД документами сложно вести работу по исполнению поручений или визированию.

Многие ли СЭД поддерживают наложение резолюций на первичные документы, поступившие в электронном виде, но еще не зарегистрированные в СЭД? Такую возможность не назовешь обычной для СЭД. В реальной жизни наложение резолюции может стать причиной регистрации документа в СЭД, а не следствием. Если, например, первичный документ поступил извне по электронной почте автору резолюции, то безбумажная технология легко может дать сбой. Почту напечатают, резолюцию наложат на бумажный документ, а затем документ зарегистрируют в СЭД. Желательно было бы сделать все в электронном виде и в правильной последовательности: сначала наложение резолюции на электронный документ, а затем регистрация в СЭД и контроль исполнения. Но без поддержки со стороны СЭД такой порядок действий может оказаться чересчур сложным для выполнения.

Невнимание разработчиков к автономному режиму частично можно объяснить издержками бюрократии. Некоторые группы пользователей СЭД плотнее общаются с разработчиками и лучше защищают свои интересы, и это может влиять на функции СЭД. Мы считаем, что разработчикам СЭД не следует ограничиваться пониманием СЭД как рабочего пространства, где бережно хранятся папки с документами, собранные нелегким трудом администраторов, регистраторов, секретарей, контролеров и делопроизводителей, для удобства которых придуманы бюрократические правила документооборота.

Более перспективным кажется нам понимание СЭД как инфраструктуры для создания и движения документов, переносящих драгоценные крупицы знаний между разумными существами, способными придавать документам отпечаток своей неповторимой индивидуальности. Такое понимание СЭД ориентируется на более широкий круг пользователей.

Чтобы на деле приблизиться к пониманию СЭД как инфраструктуры для создания и движения доку-

ментов, в этой статье мы рассматриваем задачу организации работы участников документооборота в автономном режиме, без постоянного подключения к СЭД.

Для поддержки автономной работы с документами мы предлагаем включать контекст документооборота в документы, как выгружаемые из СЭД, так и первичные. Внедренный в документ контекст документооборота может отображаться и изменяться при работе с документом в автономном режиме, а изменения контекста могут импортироваться в СЭД.

Практическая реализация данной работы базируется на СЭД E1 Евфрат [1] (далее «E1»). Основное внимание уделяется обработке документов в форматах приложений Word, Excel и PowerPoint, для версий от 2007 SP3 и выше пакета MS Office [2] (далее «офисные документы» и «офисные приложения»). Указанные приложения поддерживают формат файлов Open XML [3]. Этот формат файлов документирован и поддержан программными интерфейсами (API), которые позволяют включать в офисные документы дополнительную информацию без запуска офисных приложений. В состав решения включены программная надстройка клиентского приложения E1и программная надстройка указанных офисных приложений.

1. Постановка задачи

В этой статье описывается программное решение для реализации таких сценариев документооборота, которые могут включать периоды работы с документами в автономном режиме, без постоянного подключения к СЭД. Рассматриваются два основных сценария:

- Сценарий выгрузки документа из СЭД для исполнения задач по документу в среде MS Office, с последующей загрузкой документа в СЭД для регистрации хода исполнения задач.
- Сценарий создания новых задач по документу в среде MS Office, с последующей регистрацией документа в СЭД для формирования маршрута движения документа.

Постановка задачи ограничена предположением, что в каждый момент времени документ может редактироваться лишь одним участником документооборота, после чего документ может переходить к следующему участнику по маршруту движения в СЭД. Мы не рассматриваем более сложную задачу координации параллельного редактирования документа несколькими авторами одновременно.

2. Отличительные особенности решения

- Решение включает две программные компоненты: надстройку СЭД E1 Евфрат и надстройку приложений MS Word, MS Excel, MS PowerPoint, для версий от 2007 SP3 и выше.
- В документ MS Office добавляется XML-часть с контекстом документооборота. Содержимое XML-части может формироваться программой при выгрузке документа из СЭД, а также может создаваться и изменяться клиентом в автономном режиме.
- При импорте в СЭД документа MS Office XML-часть извлекается и удаляется из документа.
- Записанные в автономном режиме действия с задачами могут импортироваться в СЭД под контролем выполняющего импорт зарегистрированного пользователя СЭД.
- При импорте документа в СЭД может автоматически формироваться маршрут движения документа, с учетом очередности записанных задач.
- Надстройка MS Office позволяет подключаться к СЭД, для обновления текущей информации о документе из СЭД.
- Адресная книга СЭД может скачиваться из СЭД и храниться на компьютере клиента для создания новых задач в автономном режиме.
- Проверка подлинности участника в автономном режиме не производится. Пользователь MS Office указывает в настройках свое учетное имя в СЭД для автономной работы, но без ввода пароля.
- Цифровые подписи документа MS Office могут проверяться лицом, выполняющим импорт документа MS Office в СЭД.
- Для проверки авторства документов MS Office при импорте в СЭД может применяться предварительная регистрация в СЭД сертификатов ЭЦП клиентов, желающих работать с документами в автономном режиме.

3. План статьи

В п. 1 описана модель документа СЭД E1 Евфрат и ее расширение в данном решении. В п. 2 описаны два базовых сценария автономной работы с документами: сценарий исполнения задач и сценарий создания новых задач. В п. 3 описана информационная модель контекста документооборота (КД), который внедряется в офисные документы в виде XML-части. В п. 4 описаны функции офисной надстройки — программной компоненты, которая поддерживает автономную работу с документами СЭД в среде MS Office. В п. 5 описан порядок импорта документов в СЭД, с учетом записанных в КД действий с задачами. В п. 6 описано автоматическое формирование маршрута движения при импорте документа в СЭД с учетом очередности записанных в КД задач. В п. 7 обсуждается использование ЭЦП для верификации импортируемых в СЭД документов.

1. Модель документа СЭД

1.1. Оригинальная информационная модель СЭД Е1 Евфрат

Наиболее крупным информационным объектом СЭД Е1 Евфрат (далее Е1) можно считать «поток документов». Поток есть коллекция пронумерованных однотипных документов. Поток характеризуется определенной формой «регистрационной карточки» документа. Форма включает логическую составляющую (модель содержания) и графическое представление. Модель содержания определяет содержание регистрационной карточки. Регистрационная карточка документа заполняется регистратором и хранится в формате XML.

Документ Е1 включает регистрационную карточку, форма которой зависит от потока, а также контрольную карточку фиксированной формы. Контрольная карточка включает такие реквизиты, как срок исполнения, состояние контроля, контролер и ответственный по документу.

Документ может включать один или несколько присоединенных файлов. В документе могут храниться несколько версий каждого присоединенного файла, созданных различными авторами. В потоке документов может быть настроен шаблон документа с присоединенными файлами. При создании нового документа к нему автоматически будут прикреплены копии присоединенных к шаблону файлов. Таким образом, заготовки присоединенных файлов могут автоматически создаваться при регистрации документа.

Документ может включать один или несколько «маршрутов». Маршрут характеризует плановое и фактическое движение документа между участниками документооборота. Движение документа по маршруту контролируется контролером маршрута. Контролером маршрута может быть либо создатель маршрута, либо другой участник, обычно выбираемый создателем маршрута. Контролер получает уведомления о таких событиях, как начало выполнения задачи участником, прием поручения к исполнению или отказ от поручения, завершение задачи, превышение срока исполнения, комментарии участников к задачам.

Маршрут изображается в виде графа, состоящего из узлов и направленных переходов. Узел маршрута содержит либо одну системную деятельность, либо одну пользовательскую деятельность, также называемую «задачей». Примеры системных типов узлов маршрута: узел «начало маршрута», или узел «синхронизация» для ожидания завершения нескольких предшествующих задач.

Ответственный исполнитель пользовательской задачи может создать подмаршрут и сформулировать одну или несколько подзадач, обычно своим сотрудникам. Подмаршрут изображается графически как бы упакованным внутри узла родительского маршрута. Предполагается, что для выполнения родительской задачи подмаршрут должен быть завершен.

Переход между узлами маршрута А и Б характеризует запуск задачи Б после завершения задачи А. После того как задача А будет выполнена, исполнитель задачи Б получит уведомление о том, что ему назначена задача Б, и начнется отсчет срока выполнения задачи Б. Если в узел Б ведет несколько переходов из задач A1..An, то завершение любой из задач A1..An приведет к запуску задачи Б. Если же нужно напротив, дожидаться завершения всех предшествующих задач, то перед узлом Б вставляют системный узел типа «синхронизация».

Типы пользовательских задач следующие: поручение, согласование или ознакомление. Каждая пользовательская задача характеризуется следующими основными реквизитами: автор, ответственный исполнитель, название, текст.

Поручение есть наиболее сложный тип пользовательской задачи:

- Поручение может включать наряду с ответственным исполнителем несколько соисполнителей.
- Порядок исполнения поручения предполагает два действия: ответственный исполнитель поручения сначала принимает поручение к исполнению, а позднее отчитывается в исполнении поручения.

В документе могут храниться связи с другими документами. Например, в исходящем документе могут храниться связи с входящими документами от того же корреспондента.

1.2. Расширение модели документа: связи между задачами и файлами

В оригинальной модели документа Е1 задачи по документу не связаны с присоединенными к документу файлами. В рамках данного решения мы предлагаем поддерживать связи между задачами и файлами по типу отношения «многие ко многим». Каждая задача может быть связана с несколькими файлами, а каждый файл может быть связан с несколькими задачами. Связи фиксируются при создании задачи ее автором и могут храниться в скрытом поле регистрационной карточки.

По смыслу связь между задачей и файлом может означать, что для выполнения задачи исполнителю необходимо прочесть файл и может быть, отредактировать его. Такие связи могут учитываться для выгрузки из СЭД необходимых для исполнения данной задачи файлов.

2. Сценарии автономной работы с документами

2.1. Сценарий исполнения задач по документу в автономном режиме

1. Документ СЭД с присоединенным офисным файлом регистрируется, и в нем создаются задачи как обычно.
2. Исполнитель задачи открывает документ в СЭД и нажимает на кнопку «выгрузить» в таблице присоединенных файлов.
3. Перед выгрузкой файла программа предупреждает о том, что в файл может быть включена информация о документообороте, в том числе конфиденциальная.
4. В выгруженный файл включается XML-часть со сведениями о документе СЭД, о задачах и обо всех участниках документа, включая исполнителей задач.
5. Далее исполнитель задачи может продолжать работу с офисным файлом в автономном режиме в среде MS Office.
6. Перед началом работы с офисными файлами на данном компьютере исполнитель один раз подключается к СДО и скачивает адресную книгу. Учетное имя пользователя запоминается на локальном компьютере, но может быть изменено позднее.
7. Исполнитель открывает документ в соответствующем офисном приложении. В левой части окна документа отображается панель задач «Документооборот». На ней изначально отображается активная задача, которую нужно исполнить, с возможностью просмотра всех задач по документу.
8. Исполнитель вносит в документ необходимые изменения.
9. Исполнитель указывает на панели задач свое решение по задаче, например «отчитаться в исполнении поручения», или «одобрить согласование» и свой комментарий.
10. Исполнитель сохраняет файл MS Office.
11. Далее работа продолжается в клиентском приложении СЭД. Исполнитель либо сам запускает это приложение, либо передает файл MS Office со своими записанными действиями другому пользователю СЭД, выполняющему импорт документа в СЭД.
12. В СЭД исполнитель выбирает пункт меню «Обновить документ из файла». При этом автоматически открывается документ СЭД, из которого ранее был выгружен указанный офисный файл и запускается процесс импорта документа.
13. В процессе импорта отображается диалог «Действия». В нем пользователь может выбрать для исполнения все или некоторые из записанных в офисном документе действий.
14. В результате в документ СЭД загружается новая версия файла, а также выполняются записанные в офисном файле и подтвержденные текущим пользователем СЭД действия с задачами.

2.2. Сценарий создания новых задач по документу в автономном режиме

1. Пользователь офисного приложения — будущий автор задач (далее для краткости «автор») открывает или создает документ MS Office как обычно.
2. В главном меню приложения MS Office автор выбирает меню «Надстройки». Отображается лента кнопок «Документооборот». На ней в частности, есть кнопки для создания новых задач.
3. Автор создает новые задачи: поручения, согласования и ознакомления, которые сохраняются в XML-части офисного документа.
4. Дальнейшие действия совершаются в клиентском приложении СЭД: либо самим автором документа, либо другим пользователем СЭД, например, регистратором или секретарем.
5. Офисный файл прикрепляется к новому или существующему документу СЭД.
6. При загрузке файла в СЭД автоматически открывается диалог «Действия», в котором пользователь может подтвердить создание каждой новой задачи.
7. Из подтвержденных задач автоматически формируется новый маршрут или под-маршрут, с учетом очередности задач.

3. Контекст документооборота

Для автономной работы в документ MS Office может включаться контекст документооборота (КД) в виде XML-части. Контекст документооборота может включать полную информацию о состоянии документа СЭД, в том числе:

- регистрационную карточку,
- контрольную карточку,
- список присоединенных файлов,
- описание маршрутов и задач,
- ход исполнения задач с комментариями участников,
- сведения обо всех упомянутых в документе участниках, включая тех, кто принимал участие в создании документа, а также исполнителей задач, контролеров и т. д.

В автономном режиме в КД могут вноситься записи о действиях клиента с задачами:

- В КД может быть записано изменение состояния задачи. Например, клиент может зафиксировать выполнение поручения, или одобрить согласование.

- В КД может быть записан комментарий клиента к задаче, адресованный контролеру маршрута или ответственному исполнителю.
- В КД могут быть записаны новые задачи, с выбором исполнителей из адресной книги.

Контекст документооборота может быть создан не только в документе, выгруженном из СЭД, но и в первичном документе MS Office, который еще не регистрировался в СЭД. В таком документе КД инициализируется при создании первой задачи по документу. В дальнейшем документ MS Office может быть присоединен в качестве файла к новому или существующему документу СЭД.

Записанные в КД действия с задачами могут учитываться при импорте документа в СЭД. Из новых задач автоматически формируется маршрут.

4. Функции офисной надстройки

Графический интерфейс офисной надстройки в данном решении включает следующие компоненты (см. рис. 1):

- Группа кнопок «Документооборот» на ленте меню офисного приложения.
- Панель задач «Документооборот», которая отображается в окне документа. На панели задач имеется список выбора задач по документу и подробное отображение выбранной задачи, а также кнопки для действий с выбранной задачей.

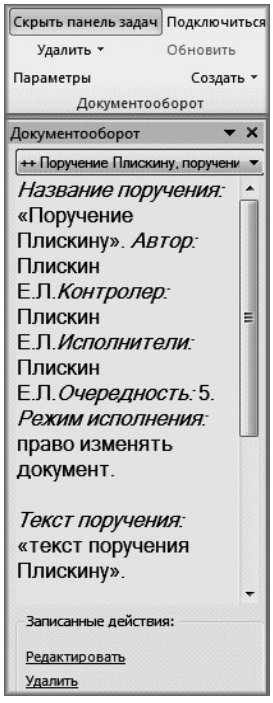

Рис. 1. Элементы графического интерфейса офисной надстройки на ленте меню и на панели задач

На ленте меню имеются следующие функции:

- Показать/скрыть панель задач.
- Удалить записанные действия с задачами.
- Удалить полностью контекст документооборота.
- Настроить параметры офисной надстройки.
- Подключиться к СЭД или отключиться от СЭД.
- Обновить контекст документооборота из СЭД.
- Создать задачу: поручение, согласование, ознакомление.

На панели задач могут быть доступны следующие действия с выбранной задачей:

- Редактировать новую задачу, созданную клиентом в автономном режиме.
- Удалить новую задачу.
- Записать комментарий по ходу выполнения задачи.
- Принять решение о выполнении задачи: задача выполнена, одобрить согласование, отклонить согласование.

4.1. Создание новых задач в автономном режиме

Рассмотрим создание новой задачи на примере поручения. При выборе функции «Создать новое поручение» в офисном приложении открывается диалог «Поручение» (рис. 2).

При помощи кнопки «…» открывается диалог выбора исполнителей из адресной книги. При этом используется файл адресной книги, который хранится на компьютере клиента, без подключения к СЭД.

Помимо стандартных для СЭД Е1 Евфрат реквизитов поручения, в диалоге дополнительно имеется поле «Очередность» с возможными значениями от 1 до 9. Очередность задач используется для автоматического формирования маршрута при импорте в СЭД.

4.2. Параметры офисной надстройки

При выборе функции настройки параметров открывается диалог, показанный на рис. 3.

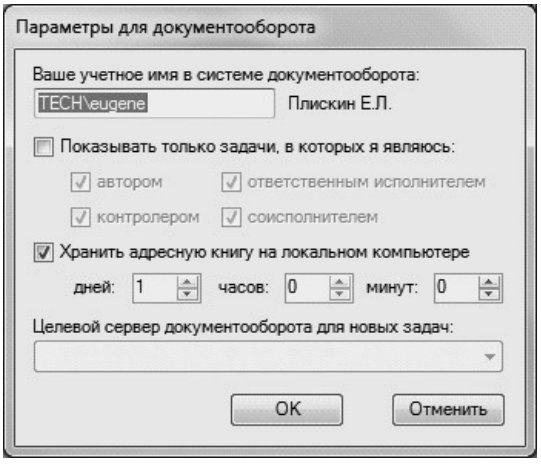

Рис. 2. Параметры офисной надстройки

Диалог «Параметры для документооборота» служит для ввода предпочтений пользователя. Введенные в этом диалоге сведения запоминаются в личных настройках текущего пользователя на данном компьютере и используются для работы со всем последующими офисными документами во всех офисных приложениях.

Диалог включает следующие элементы:

- Поле ввода «Ваше учетное имя в системе документооборота». Это поле активно, если не открыто ни одного офисного документа с внедренным контекстом документооборота. По умолчанию используется учетное имя пользователя Windows. См. подробнее об этом поле в п. 4.4 ниже.
- Флажки для фильтрации списка выбора задач на панели задач.
- Флажок «Хранить адресную книгу на локальном компьютере» и поля для указания срока хранения: количество дней, часов и минут. Если этот флажок не отмечен, то адресная книга не хранится на компьютере клиента и новые задачи можно создавать только при условии подключения к серверу СЭД.
- Список выбора «Целевой сервер документооборота для новых задач». В этот список добавляются имена серверов, с которых были получены файлы адресных книг. Выбранное значение определяет файл адресной книги, который будет использован для создания новых задач.

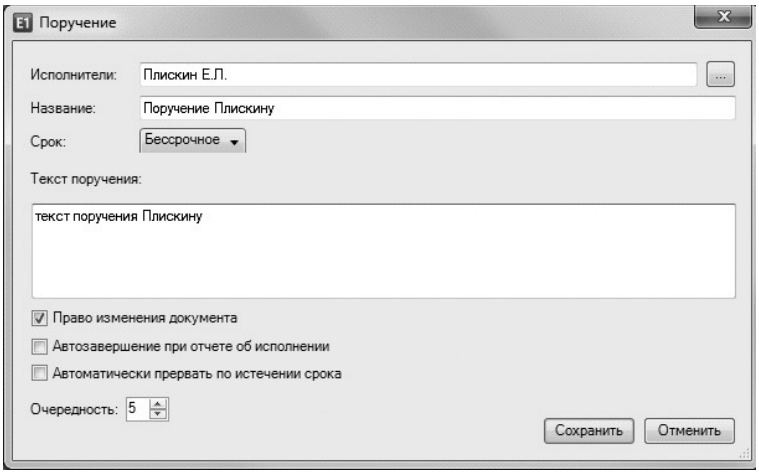

Рис. 3. Диалог для создания поручения

4.3. Обновление информации в документе

Функция обновления информации в активном документе доступна при помощи кнопки «Обновить» на ленте кнопок. Кнопка «Обновить» активируется при следующих условиях:

- В документ имеется выгруженный из СЭД контекст документооборота (КД).
- Установлено подключение к серверу при помощи кнопки «Подключить».

Если в КД записаны действия с задачами, то перед выполнением данной функции выдается предупреждение о том, что все записанные действия будут удалены. Пользователь может либо отказаться от обновления, либо согласиться на удаление записанных действий.

При выполнении данной функции свежая информация о документе СЭД скачивается с сервера, внедряется в офисный файл и отображается на панели задач «Документооборот». Все ранее записанные в документе действия с задачами удаляются.

4.4. Учетное имя пользователя

Клиент вводит учетное имя пользователя один раз на данном компьютере перед началом работы в автономном режиме. Нет необходимости вводить учетное имя, если учетное имя клиента в СЭД совпадает с учетным именем пользователя Windows на данном компьютере.

Указанное учетное имя пользователя используется в автономном режиме следующим образом:

- При открытии документа в офисном приложении указанное учетное имя отыскивается в КД. Если участник не найден в КД, то из КД удаляются все записанные действия, и у пользователя не будет возможности записывать действия с задачами.
- Если участник с заданным учетным именем найден в КД, то при работе в офисном приложении:
  - Код участника сохраняется в документе в реквизите автора всех записанных действий.
  - При загрузке документа «чужие» записанные действия удаляются из КД. Это означает, что одновременно в КД могут быть записаны действия только одного участника.
  - Имеется возможность фильтрации списка задач, для выбора задач, относящихся к данному участнику.

5. Импорт документа MS Office в СЭД

При импорте документа MS Office в СЭД могут быть автоматически созданы следующие информационные объекты:

- Новый документ СЭД, если данный документ MS Office не был ранее выгружен из СЭД.
- Присоединенный файл — документ MS Office, если данный документ MS Office не был ранее выгружен из СЭД.

- Маршрут с импортированными новыми задачами.
- Связи между новыми задачами и присоединенным файлом — документом MS Office, из которого импортированы задачи.

Автор записанных действий учитывается при импорте следующим образом:

- При загрузке документа в СЭД «чужие» записанные действия со старыми задачами игнорируются. Учитываются только записанные исполняющим импорт пользователем СЭД действия со старыми задачами.
- Однако новые задачи могут быть импортированы в СЭД от имени другого автора, чем текущий пользователь СЭД, исполняющий импорт. Текущий пользователь СЭД по своему усмотрению может импортировать новые задачи либо от собственного имени, либо от имени записанного автора задач.

6. Формирование маршрута

Все новые задачи из офисного файла помещаются в один новый маршрут или под-маршрут. При формировании маршрута учитывается очередность задач. Сначала создаются задачи меньшей очередности, затем большей. При необходимости в маршрут добавляются узлы синхронизации для ожидания завершения нескольких задач одинаковой очередности.

Для каждого из нескольких исполнителей согласования или ознакомления создается отдельная задача той же очередности.

Пример. Предположим, что в офисном файле созданы следующие задачи:

- Поручение П1, очередность = 2.
- Поручение П2, очередность = 2.
- Согласование, исполнители С1, С2, С3, очередность 4, порядок исполнения «последовательный».
- Ознакомление, исполнители О1, О2, О3, очередность 5, порядок исполнения «параллельный».

При загрузке файла в СЭД может быть сформирован следующий маршрут (рис. 4).

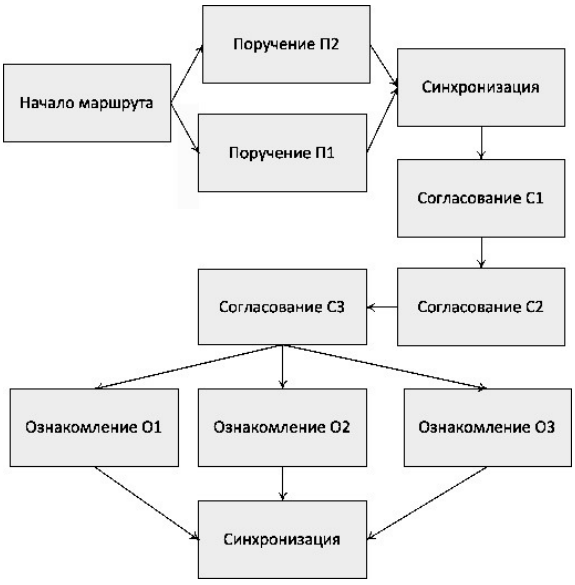

Рис. 4. Формирование маршрута с учетом очередности задач

7. Использование ЭЦП

7.1. Проверка подлинности документа

В автономном режиме документы могут подвергаться несанкционированному воздействию. Поэтому при импорте документа в СДО может возникать необходимость проверки подлинности документов в двух аспектах:

- проверка целостности документа, то есть неизменности документа на пути от автора к получателю, и
- установление личности автора документа или записанных в документе изменений.

Для предупреждения и обнаружения несанкционированных изменений документы могут подписываться цифровой подписью (ЭЦП). Технология ЭЦП предполагает использование пары из «закрытого» и «открытого» ключа. Для создания ЭЦП используется закрытый ключ, а для проверки ЭЦП используется открытый ключ. Считается, что располагая опубликованным открытым ключом автора подписи, получатели документа могут проверять ЭЦП, но не могут ее подделывать.

Приложения пакета MS Office снабжены удобными средствами цифровой подписи, как описано в [4]. Для создания ЭЦП требуется сертификат, или цифровое удостоверение. Технология ЭЦП во многом определяется процедурами создания, хранения, экспорта, импорта, просмотра и верификации сертификатов.

Сертификат ЭЦП может включать закрытую и открытую части, либо только открытую часть. Открытая часть сертификата связывает имя пользователя с открытым ключом. Открытая часть сертификата может рассылаться владельцем ЭЦП всем его корреспондентам. Открытая часть сертификата обычно включается в ЭЦП.

Закрытая часть сертификата содержит закрытый ключ и обрабатывается по более строгим правилам. Закрытый ключ хранится в зашифрованном виде и для доступа к закрытому ключу при создании ЭЦП всякий раз может требоваться пароль. Предполагается, что закрытый ключ никому не сообщается и тщательно оберегается владельцем от компрометации. Иначе, если закрытый ключ подписи заведомо небрежно хранится владельцем, то проверка цифровой подписи данного автора может лишь создавать иллюзию безопасности там, где ее нет.

7.2. Человеческий фактор при проверке ЭЦП

Результаты проверки ЭЦП могут неформально интерпретироваться участником, принимающим решение об импорте в СЭД документа с записанными поручениями в контексте документооборота. Документ может включать не одну, а несколько подписей, причем каждая ЭЦП может заверять не весь документ, а только некоторые части документа. Проверка цифровых подписей в общем случае дает не булевский результат «истина/ложь», а определенный объем информации о выполненных проверках:

- Возможен полностью отрицательный результат — очевидное нарушение целостности документа.
- Возможен полностью положительный результат — подтверждение каждой подписи, плюс успешная проверка каждого сертификата по цепочке удостоверяющих центров, плюс установление принадлежности каждой подписи зарегистрированному участнику документооборота, плюс проверка охвата подписями всех частей документа.
- Возможны различные промежуточные ситуации, когда часть условий выполнена, но решение о подлинности документа может приниматься неформально.

Примеры неформальных действий при проверке ЭЦП:

- Сертификат заверен надежным удостоверяющим центром и выдан на имя, совпадающее с именем генерального директора данной компании: «Алексей Петрович Иванов, Россия». Поскольку сертификат не содержит фотографии, то трудно сказать, действительно ли это генеральный директор, или его полный тезка. Для решения вопроса проверяющий может учитывать такие обстоятельства, как источник получения документа, или аналогию с предыдущими документами, подлинность которых была установлена неформально.
- Сертификат ЭЦП выдан удостоверяющим центром известной организации, но сертификат самого удостоверяющего центра не может быть проверен. Строго говоря, такой сертификат ЭЦП не должен приниматься, ведь нарушитель может создать фальшивый удостоверяющий центр с любым названием. Однако пользователь может решить иначе и включить сертификат ЭЦП в число доверенных. Это неформальное действие.

Выводы из вышесказанного:

- Результаты проверки ЭЦП документа не всегда однозначны.
- Автоматическое принятие решения о достоверности документа при импорте в СЭД на основании проверки ЭЦП не представляется возможным.
- Программа, выполняющая проверку ЭЦП документа и отображающая результаты проверки, должна разрабатываться с учетом человеческого фактора. В частности, предлагается при отображении результатов проверки ЭЦП акцентировать внимание проверяющего на успешном определении участника документооборота, которому принадлежит сертификат. Подробнее об этом в п. 7.5 ниже.

7.3. Структура подписи офисного документа

Приложения пакета MS Office, начиная с версии 2007, поддерживают стандарт ЭЦП «XMLDSIG» [5], а начиная с версии 2010, поддерживают расширенный стандарт ЭЦП «XAdES» [6]. Документ MS Office представляет собой не что иное, как zip-архив, в котором хранятся XML-части документа и дополнительные данные, такие как графические и медиа-файлы. Основное содержание документа хранится в формате XML. Также в формате XML создается часть для ЭЦП, формат которой отвечает указанным стандартам. Не все части документа обязательно используются при вычислении ЭЦП. В структуре ЭЦП записываются ссылки на части документа, использованные для вычисления ЭЦП, и значение хэш-кода каждой такой части.

Наши опыты с MS Word 2010 показали, что добавленная в документ XML-часть с контекстом документооборота (КД) не включается в вычисление ЭЦП офисным приложением. Если «нарушитель» распакует zip-архив документа, внесет изменения в текст КД и запакует измененный КД обратно в zip-архив, то ЭЦП документа не пострадает. Офисное приложение «не заметит» подмены КД. Вероятно, у авторов MS Word есть свои резоны для того, чтобы исключать «пользовательские» XML-части из вычисления ЭЦП. Однако в рамках нашего решения для автономной работы с документами это означает дырку в безопасности.

Для защиты КД от несанкционированных изменений можно включать в документ дополнительную подпись, которая будет формироваться офисной надстройкой, и вычисляться по содержимому КД. Эту подпись можно дополнительно проверять при импорте документа в СЭД. А если удастся сформировать ЭЦП КД в соответствии со стандартом [5], то можно надеяться на корректное отображение ЭЦП КД офисным приложением.

7.4. Самоподписанные сертификаты

Для самостоятельного создания сертификата ЭЦП с парой из открытого и закрытого ключей проще всего воспользоваться программой Adobe Reader 9, как описано в [8]. В процессе создания сертификата пользователь указывает сведения о себе: имя, подразделение, организацию, адрес электронной почты и страну. Полученный таким образом сертификат подписан своим собственным закрытым ключом. Такие сертификаты называют самоподписанными.

Альтернативой самоподписанному сертификату является «боевой» сертификат, полученный при помощи удостоверяющего центра. Организация собственного удостоверяющего центра под силу не всякой организации, где может эксплуатироваться СЭД.

А коммерческие удостоверяющие центры берут годовую плату за каждый сертификат в размере от десятков до тысяч долларов. Поэтому актуальной задачей является возможность использования самоподписанных сертификатов для проверки подлинности документов при импорте в СЭД, включая оба аспекта подлинности: целостность документа и удостоверение личности автора подписи.

Регистратору, выполняющему импорт документа в СЭД достаточно проверить ЭЦП документа, чтобы удостовериться в целостности документа. Надежность результата проверки целостности документа не зависит от достоверности сведений в сертификате. Для проверки целостности документа самоподписанный сертификат может быть ничем не хуже боевого.

Сложнее обстоит дело с проверкой личности автора ЭЦП. Самоподписанный сертификат, очевидно, не может удостоверить личность своего владельца, поскольку при создании сертификата владелец сам указывал сведения о себе и эти сведения никем не заверены.

Для установления личности автора ЭЦП можно регистрировать в СЭД сертификаты ЭЦП участников, желающих работать с документами в автономном режиме. Практика регистрации сертификатов часто применяется организациями, выдающими сертификаты клиентам для проверки подлинности клиентов при удаленном доступе через Интернет, например, в системах дистанционного банковского обслуживания. В нашем решении регистрация может применяться к сертификатам любого происхождения. Надежность этого метода обусловлена предположением, что процедура генерации открытых ключей обеспечивает их уникальность. Уникальность открытых ключей позволяет использовать сертификаты для идентификации авторов ЭЦП.

7.5. Регистрация сертификатов в СЭД

Регистрация сертификата в СЭД позволяет установить связь между открытым ключом ЭЦП и зарегистрированным участником документооборота. Если сертификат зарегистрирован в СЭД, то достоверность указанных в нем сведений о владельце сертификата не имеет решающего значения. Сертификат, зарегистрированный в СЭД участником документооборота или администратором СЭД от имени данного участника, может быть использован для установления личности автора ЭЦП при импорте подписанных документов в СЭД.

В данном решении в СЭД добавлен специальный поток «Сертификаты». Любой участник документооборота может создать в этом потоке один или несколько документов. При создании документа в данном потоке клиент должен указать сертификат ЭЦП. Содержимое открытой части сертификата записывается в поля документа СЭД. Кроме того, регистрирующий устанавливает на форме документа флажок «Разрешается использовать данный сертификат для проверки ЭЦП». Дополнительно администратор может указать, кому принадлежит сертификат, в то время как рядовые участники могут регистрировать только собственные сертификаты.

При импорте подписанного документа в СЭД из него извлекаются программой такие ключевые реквизиты, как серийный номер сертификата, имя издателя и имя владельца сертификата. Затем программа ищет в СЭД документ в потоке «Сертификаты» с такими реквизитами сертификата. Найденный в СЭД сертификат сравнивается с сертификатом, извлеченным из ЭЦП, не только по ключевым реквизитам, но по всему содержанию сертификатов, включая открытый ключ. Если сертификаты полностью совпадают, то в диалоге проверки ЭЦП отображается информация об участнике, которому принадлежит ЭЦП.

Литература

1. Система электронного документооборота и автоматизации бизнес-процессов E1 Евфрат. http://www.evfrat.ru
2. Microsoft Office Development. http://msdn.microsoft.com/en-us/library/bb726434(v=office.12).aspx
3. About Open XML. http://openxmldeveloper.org/wiki/w/wiki/about-open-xml.aspx
4. Добавление или удаление цифровой подписи в файлах Office. http://office.microsoft.com/ru-ru/word-help/HA010354308.aspx?CTT=5&origin=HA102247419
5. Стандарт XMLDSIG. http://www.w3.org/Signature/
6. Стандарт XML Advanced Electronic Signatures, XAdES. http://www.w3.org/TR/XAdES/
7. Office Digital Signature. http://msdn.microsoft.com/en-us/library/ff535210(v=office.12).aspx
8. Создание нового цифрового удостоверения. http://help.adobe.com/ru_RU/Acrobat/9.0/Professional/WS58a04a822e3e50102bd615109794195ff-7d92.w.html

Куратов Павел Александрович. Научный сотрудник ИСА РАН. Окончил в 1978 г. механико-математический факультет МГУ им. М. В. Ломоносова. Количество печатных работ: 14. Область научных интересов: теория и методы распознавания образов. E-mail: paul@cognitive.ru

Петрова Наталия Александровна. Инженер-программист ООО «Когнитивные технологии». Окончила в 2010 г. Национальный исследовательский технологический университет «МИСиС». E-mail: hobb@cognitive.ru

Плискин Евгений Львович. Старший научный сотрудник ИСА РАН, к. т. н. Окончил в 1982 г. Московский физико-технический институт. Количество печатных работ: 13. Область научных интересов: автоматизированные информационные системы. E-mail: pliskin@cognitive.ru