ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ ОРГАНИЗАЦИИ

Влацкая И.В., канд. техн. наук, доцент, Чернышев М.С.
Оренбургский государственный университет

С появлением бизнес-процессов возникает потребность в управлении механизмами с помощью упорядоченной документации. Рост предприятия увеличивает количество документации. В то же время, если не заниматься документами своевременно, то они начнут накапливаться и есть вероятность потерять важный документ или не исполнить вовремя поручение. Для того чтобы избежать подобных проблем применяют электронный документооборот.

Документооборот – это движение документов с момента их создания или получения до завершения исполнения, отправки адресату или передачи в архив. [1]

Электронный документооборот – это единый механизм движения документов, созданных с помощью компьютерных средств, как правило, подписанных электронной цифровой подписью, а также способ обработки этих документов с помощь различных электронных носителей. [2]

Задачи, решаемые системами электронного документооборота:

1 систематизацию и регламентацию работы с документами;
2 подготовка документов по шаблонам;
3 ведение номенклатуры дел организации;
4 автоматизацию учёта документов, в том числе:
   a. классификацию документов по различным критериям;
   b. регистрацию документов по заданным шаблонам и алгоритмам;
   c. учёт сроков хранения;
   d. помещение документов в дела и разбивка дел на тома;
5 автоматизацию поиска документов;
6 электронную рассылку документов;
7 автоматизацию процедур коллективной работы с документом:
   a. разработка проекта документа;
   b. согласование документа;
   c. экспертиза документа;
   d. исполнение документа;
8 обеспечение защиты от несанкционированного доступа и искажения или удаления информации.

Перед каждой организацией стоит свой набор задач и, соответственно, нет необходимости в излишнем функционале.

Системы электронного документооборота принято классифицировать по следующим типам в зависимости от особенностей:

1) Универсальные системы электронного документооборота:

- небольшой функционал, относительно остальных видов систем;

- неадаптированность под конкретику организации;
- доступность и простота в установке;
- недорогие по стоимости, относительно других видов систем электронного документооборота;
- техническая поддержка в период действия лицензии;
- чаще всего реализует общий документооборот без поддержки электронной подписи.

2) Индивидуальные системы электронного документооборота

- максимальная персонификация системы электронного документооборота;
- дополнительные траты на переобучение сотрудников и закупку оборудования;
- высокая стоимость;
- затраты времени на разработку, развертывание и внедрение больше, чем у остальных видов систем.

3) Комбинированные системы электронного документооборота

- полностью подходит для обеспечения потребностей организации;
- затраты на разработку, установку и введение в эксплуатацию снижаются;
- базовые модули позволяют быстро освоить систему и обучить персонал;
- может взаимодействовать с другими программными продуктами;
- заказчик получает полное право на программный продукт.

Основные требования, которые выдвигают организации к системам электронного документооборота являются: серверная и клиентская операционная системы, СУБД, возможность интеграции со сторонними продуктами, стоимость и наличие сертификата ФСЭК России. Так же выдвигаются требования к функционалу, который реализует система: делопроизводство, общий документооборот, управление договорной документацией, электронный архив, управление проектами, работа с документами СМК, электронная подпись.

Рассмотрим пример системы электронного документооборота реализующий обмен юридически значимой и общей документацией внутри предприятия. В данном случае необходимо наличие цифровой подписи. Согласно ФЗ №63 выделяют три типа подписи: простая, усиленная неквалифицированная, усиленная квалифицированная. В данном случае подписи имеют разную юридическую силу в зависимости от места применения и особенностей обработки. К примеру усиленная квалифицированная подпись в любой ситуации будет иметь юридическую силу, за исключением случаев в которых удастся доказать компрометацию подписи до момента ее использования. В случае с усиленной неквалифицированной подписью, она имеет юридическую силу в рамках органи-

зации, в случае документооборота с контрагентами необходимо заключать соглашение рассматривающее порядок формирования обработки подписи и организацию хранения подписанной документации. Существенным отличием квалифицированной и неквалифицированной подписей является то, что усиленную подпись необходимо приобретать в специальных удостоверяющих центрах, сертифицированных ФСБ России. Неквалифицированную же подпись можно сгенерировать силами IT отдела, или так же приобрести в определенных организациях, но в данном случае наличие сертификата ФСБ России у организации не обязательно.

На данный момент усиленную неквалифицированную подпись применяют во многих сферах деятельности. Последние года данный вид подписи активно применяется в сфере государственных заказов, на этапе подачи заявок на участие в тендере. Обратим внимание, что итоговые документы по заключению договоров по государственным заказам подписываются только с применением усиленной квалифицированной подписи. Нормальной практикой является приобретение небольшого количества ключей усиленной квалифицированной подписи для руководителей, их заместителей и бухгалтерии, а на всю остальную организацию - усиленную неквалифицированную. Так же данный вид подписи применяется для обращений граждан в государственные органы через портал государственные услуги.

Так же существует проблема организации хранения подписанной документации. Срок действия сертификатов подписей ограничен, а в некоторых случаях согласно ФЗ №125 «Об архивном деле», срок хранения документов может достигать 75 лет, но в большинстве случаев не превышает 10, то существует необходимость хранения временных меток подписи, а также основной информации по сертификатам подписей. Для решения данной проблемы в базе данных необходимо хранить дату подписи документа, а также добавлять данную метку к самой подписи, а для ключей использовать PKI, где так же будут храниться даты действия и отзыва сертификатов ключей. Другим путем решения проблемы является перенос документов для длительного хранения на бумажные носители и заверение их печатями и подписями ответственных должностных лиц.

Очень важным является выбор алгоритма электронной подписи. Разные алгоритмы имеют разную стойкость в зависимости от длины ключей, разную основу и разные хэш-алгоритмы. Более молодыми являются алгоритмы на основе эллиптических кривых. Они имеют большую вычислительную стойкость и, как следствие, меньшую рекомендуемую длину ключа. Не маловажным параметром является используемая хэш-функция, к примеру алгоритм SHA1 и SHA512 имеют разную крипто стойкость и вероятность коллизии. Так же на

примере SHA1 можно сказать о возможности практического взлома, но на данный момент это займет пять миллиардов лет. NIST прогнозирует возможность реализации практического взлома в ближайшие 5-10 лет, из-за этого NIST планирует полностью отказаться от данного алгоритма хэширования.

Таблица 1 - сравнение алгоритмов электронной подписи

Название	Дата создания	Основа	Рекомендуемый алгоритм хэширования	Рекомендуемая длина ключей
DSA	1991	Вычислительная сложность взятия логарифма в конечных полях	SHA	2048 бит
EGSA	1985	Вычисление дискретных логарифмов в конечном поле	SHA	1024 бит
RSA	1989	Факторизация больших чисел	SHA/MD5	2048 бит
ГОСТ Р 34.10-2012	2012	Операции в группе точек эллиптической кривой, определенной над конечным простым полем.	ГОСТ Р 34.11.2012	512 бит

Из таблицы можно сделать однозначный выбор в пользу алгоритма ГОСТ, Он новее всех остальных, имеет большую крипто стойкость при меньшей рекомендуемой длине ключей, что существенно упростит задачу создания пары ключей.

Стандарт ГОСТ Р 34.10-2012 разработан центром защиты информации и специальной связи ФСБ России с участием Открытого акционерного общества «Информационные технологии и коммуникационные системы». Утвержден 7 августа 2012 года и заменил собой стандарт ГОСТ Р 34.10-2001.

Данный стандарт содержит описание процессов формирования и проверки электронной подписи, реализуемой с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем.

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции. Алгоритмы вычисления хэш-функции установлены в ГОСТ Р 34.11-2012. [3]

Схема формирования и проверки подписи представлена на рисунке 1.

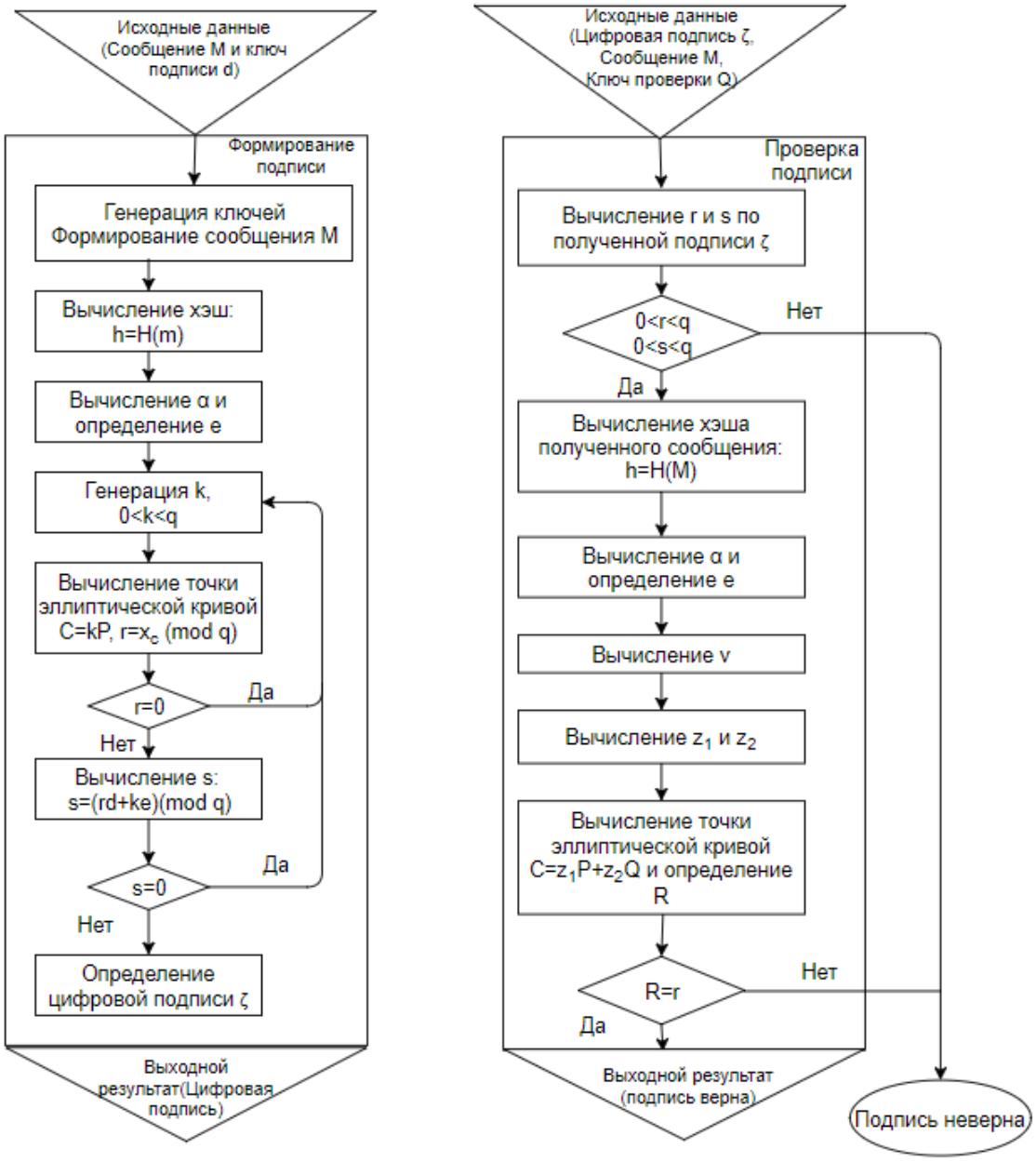

Рисунок 2 – Процесс формирования и проверки подписи (взято из ГОСТ Р 34.11-2012)

Для любой системы существует ряд угроз информационной безопасности. Данные угрозы представлены в банке данных угроз сформированным ФСТЭК России.

УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию. [4]

Данная угроза заключается в том, что у программы и ее компонентов существуют учетные записи по умолчанию, которые применяются для начально настройки системы. Например, у базы данных при ее создании могли использоваться стандартные поля admin/admin. Единственным вариантом защиты от

данной угрозы является изменение этих заданных по умолчанию данных или же использовать при начальной настройке надежные варианты, а не простые и удобные.

УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией. [4]

Данная угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена. В данном случае не предусматривается использование каких-то специальных средств. Угроза заключается в возможности просмотра с монитора пользователя или чтение отпечатанных документов. Стоит отметить что данная угроза применима ко всей документации, как юридически значимой, так и нет. Защита в данном случае является физическое разделение рабочего пространства работников, а также контроль за печатаемой документацией на сетевых принтерах.

УБИ.074: Угроза несанкционированного доступа к аутентификационной информации. [4]

Угроза заключается в возможности извлечения паролей из оперативной памяти или паролей, хранящихся в файлах в открытом виде. Защитой является шифрование участков операционной памяти в которых хранится пароль, с использованием криптопотоков, а также отказ от хранения паролей в открытом виде. Особое внимание стоит обратить на разграничение прав доступа, сетевую защиту и физическую защиту рабочих станций, ведь без доступа к ним реализация данной угрозы невозможно.

УБИ.084: Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети. [4]

Данная угроза реализуется с помощью специальных программных средств, способных эксплуатировать слабости технологий, использованных при построении системы хранения данных. Например, в случае использования ftp-сервера или его модификаций, необходимо применять надежные наборы логина и пароля, запретить анонимный вход, разрешить доступ к административной части только с определенных IP адресов.

УБИ.086: Угроза несанкционированного изменения аутентификационной информации. [4]

В случае взлома рабочей почты, злоумышленник может изменить аутентификационную информацию для системы. Оптимальным методом защиты от подобной угрозы является смена этой информации только по запросу и после подтверждения администратором личности, звонок по рабочему телефону или

личном присутствии. Обратим внимание, что в случае проникновения злоумышленника в саму организацию и доступу к рабочему телефону данный метод не может гарантировать стопроцентную защиту.

УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети. [4]

Так называемая атака человек посередине. Решается путем шифрования трафика. Более того реализация данной угрозы без физического внедрения в сеть практически не реально.

Рассмотрим принцип работы предполагаемой системы. В системе присутствуют три типа пользователей: администратор, руководитель, сотрудник. Администратор осуществляет управление пользователями, отделами и ключами. Руководитель может создать документ, отправить документ в другой отдел и осуществлять поиск, создавать юридически значимый документ, получить юридически значимый документ, отправить и извлечь документ (обычный и юридически значимый) из архива, осуществлять поиск документов, отправить документ в другой отдел или внутри отдела. Перед отправкой юридически значимого документа осуществляется его подпись. После получения юридически значимого документа можно проверить его достоверность, так же руководитель имеет права на управление отделом, который находится в его подчинении. Сотрудник может создать документ, отправить документ в архив, получить из архива, отправить документ в другой отдел или внутри отдела и осуществлять поиск.

Список литературы

1 *Романов, Д.А. Правда об электронном документообороте / Д.А. Романов, Т.Н. Ильина, А.Ю. Логинова – Москва: ДМК Пресс, 2008. – 224 с. – ISBN 5-94074-171-1.*

2 *Бухгалтерия, учет и отчетность: Электронный документооборот, электронная отчетность. [Электронный ресурс]. – Режим доступа: http://www.klerk.ru/rubricator/elektronnyj-dokumentooborot-elektronnaja-otchetnost/.*

3 *"ГОСТ Р 34.10-2012. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи" (утв. и введен в действие Приказом Росстандарта от 07.08.2012 N 215-ст).*

4 *Банк данных угроз безопасности информации: ФСТЭК России. [Электронный ресурс]. – Режим доступа: http://bdu.fstec.ru/threat (дата обращения 20.12.2017).*