Механизмы обеспечения защиты информации в электронных архивах

Андреев Владимир Сергеевич,
президент компании «ДоксВижн» (компания «ДоксВижн» - член «Гильдии Управляющих Документацией»)

В последнее время переход на безбумажный документооборот становится актуальным для большинства отечественных компаний. Само по себе внедрение электронного документооборота сулит не только ускорение всех процессов работы с документами, но и радикальное увеличение подконтрольности процессов и возможности получения информации для их оптимизации. Еще больший эффект может быть получен при применении электронного варианта межорганизационного документооборота: в этом случае ускорение бизнес-процессов может быть еще выше. При этом важнейшим фактором успешного внедрения системы электронного документооборота (СЭД) является обеспечение доверия пользователей к достоверности данных, хранящихся в системе и передаваемых между отдельными организациями, а также к надежности системы безопасности хранения данных. Именно поэтому подсистема безопасности в современной СЭД и, в частности, в электронных архивах документов, которые являются центральной частью современной СЭД, играет ключевое значение. Какие же аспекты необходимо учесть при внедрении в организации СЭД и электронных архивов? Среди аспектов использования механизмов безопасности в архиве электронных документов можно выделить:

- обеспечение идентификации пользователя, выполняющего те, или иные действия в системе;
- разграничение прав доступа к документам, хранящимся в системе;
- обеспечение возможности верхнего уровня управления уровнем доступа и контроля доступности документов в специальных случаях (например, для секретных документов, и документов ДСП);
- обеспечение идентификации исполнителя операции;
- обеспечение неизменности документа и информации о действиях пользователя в ходе процесса обработки документов
- обеспечение доступа к необходимому контексту обработки документа в рамках бизнес-процесса в приложениях СЭД;
- идентификация подлинности и неизменности документа при передаче за границы системы;
- защита секретных данных от администратора;
- создание технологической базы в соответствии с требованиями законодательства с целью организации юридически значимого документооборота.

Весь этот комплекс задач реализуется посредством механизмов безопасности, которые мы рассмотрим далее.

Для **идентификации пользователя** используется так называемая система аутентификации, т.е. проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение его подлинности. После аутентификации все действия в системе производятся от имени соответствующей учетной записи. Эта задача далеко не специфична для управления архивом документов, однако, перед его внедрением, необходимо убедится в следующих нюансах реализации данной задачи. Прежде всего,

необходимо, чтобы система обеспечивала так называемую «интегрированную секретность», т.е. чтобы аутентификация в системе происходила один раз при входе пользователя и не требовалась бы каждый раз при обращении к данным архива. При этом желательно, чтобы отдельная аутентификация в архиве вообще не требовалась, а действия производились от имени пользователя операционной системы, как это происходит, например, при работе с корпоративной электронной почтой. Таким образом, необходима тесная интеграция базы данных учетных записей архива и системного каталога операционной системы, например Active Directory.

Механизмы **разграничения правд доступа к документам** достаточно хорошо известны и, по сути, идентичны средствам разграничения доступа к объектам файловой системы. Для этого, в основном, используются механизмы так называемой дискреционной безопасности, или избирательного управления доступом. При этом управление доступом субъектов (пользователей групп) к документам осуществляется на основе списков управления доступом или матрицы доступа. Какие данные, хранящиеся в архиве могут защищаться правами доступа? Опыт показал, что при реализации конечных приложений мы сталкиваемся с необходимостью разграничения прав доступа практически на все объекты архива , а именно на содержимое документа, папки (база данных), метаданные (учетная карточка), отдельные версии документов, документы определенного типа, типы документов для конкретной папки, поисковый фильтр, виртуальная папка и т.д.

Также на практике мы сталкиваемся с необходимостью разграничения прав доступа на отдельные поля метаданных документа, однако на практике реализация данного разграничения прав через механизмы дискреционной безопасности сильно понижает производительность системы и реализуется другим способом, например через механизмы контекстной безопасности.

Однако подчас стандартных средств обеспечения безопасности оказывается недостаточно, и требуются дополнительные механизмы так называемой **мандатной безопасности**: то есть разграничение доступа субъектов к документам, основанное на назначении метки конфиденциальности и выдаче официальных разрешений (допусков) субъектам на обращение к документам соответствующего уровня конфиденциальности. В этом случае механизм работы подсистемы безопасности гораздо проще - система сравнивает уровень доступа документа и уровень допуска пользователя и, в случае, если последний равен или выше уровня допуска пользователя, то доступ предоставляется, если нет – доступ запрещается.

Управление средствами мандатной безопасности обычно реализуется специально выделенными специалистами, отвечающими за безопасность особо значимых и секретных документов; мандатный уровень реализуются поверх обычного, дискреционного, т.е. даже если пользователю даны все права на обработку документа, но уровень допуска не позволяет получить доступ к документу, то работать с документом он не сможет.

Еще один механизм разграничения доступа, который особенно востребован при обработке документов в рамках различных бизнес-процессов - **ролевая или контекстная безопасность**. При использовании этого механизма возможность доступа к документам, отдельным их фрагментам и операциям, в зависимости от текущего контекста обработки, например стадии жизненного цикла документа, или содержимого документа (наличия данного сотрудника в поле «Исполнитель» и т.д.). Контекст может быть и более сложным, например содержимое объекта, связанного с документом логической связью (исполнитель задания по документу), привязка к значениям справочников (данный пользователь является активным заместителем сотрудника указанного в поле «исполнитель» документа),

произвольными внешними данными (время рабочей смены сотрудника) и т.п. Данные механизмы позволяют, помимо разграничения доступа, обеспечить пользователям наиболее удобный интерфейс доступа к документам в рамках бизнес-процессов, с учетом контекста их обработки. Надо отметить, что единого понимания механизмов контекстной безопасности в настоящее время не выработано и каждая система может поддерживать специфические и, как правило, частичные реализации данного механизма.

Помимо ограничения доступа пользователей к данным документа и операциям с ним необходимо обеспечить гарантию подлинности информации. Это касается как содержимого документов и гарантии их неизменности (как известно электронные документы гораздо проще подделать), так и гарантии фактов выполнения тех, или иных действий с документами конкретными пользователями (заверяемые в бумажном документообороте личной подписью ответственного лица и оттиском печати). Также важно гарантировать надежное хранение конфиденциальных документов и исключить копирование их содержимого кем бы то ни было, в частности, администраторами системы. Одним из инструментов решения данных задач являются средства криптографической защиты, такие как шифрование и электронная цифровая подпись. При разработке системы корпоративного документооборота DocsVision, по мере получения опыта разнообразных внедрений системы мы столкнулись с тем, что контексты использования этих технологий весьма разнообразны, и при их использовании необходимо учитывать различные нюансы и специфические особенности их применения. Рассмотрим специфику использования данных технологий в контексте работы с документами. Какие же данные бывает нужно шифровать и подписывать?

Прежде всего файлы документов, хранящихся в системе: необходимо обеспечить возможность шифрования файлов документов для ограниченного круга читателей (которым может быть в принципе доступно содержимое документов). Необходимо отметить следующее: шифрование является последней степенью защиты содержимого документа и имеет смысл только для наиболее секретных документов (в том, например, случае если вам необходимо закрыть содержимое документа от администратора). Ограничение использования шифрования связано с тем, что зашифрованный документ не может быть использован стандартными средствами полнотекстового индексирования и, соответственно, выпадает из возможности полнотекстового поиска. В общем случае он будет доступен только через классификационный и атрибутивной поиск. И наконец, при использовании шифрования существует потенциальная возможность утраты содержимого документа в случае утери возможности доступа ко всем секретным ключам читателей. Именно в связи с перечисленными трудностями использование шифрования, как правило, весьма ограничено.

ЭЦП применяется гораздо активнее, наиболее типичным сценарием его применения является наложение электронной подписи на файл хранящегося в системе документа. Нужно отметить, что при работе с документами в системе контекст использования механизмов ЭЦП гораздо шире, чем при ее использовании при обмене документами между организациями. В последнем случае она используется исключительно как аналог подписи на бумажном (неизменном) документе. Помимо этого ЭЦП может использоваться, в частности, для подтверждения согласия с документом на какой-либо стадии его разработки, или, например, в случае необходимости подтверждения факта чтения документа сотрудником в какой-либо момент его жизненного цикла. Например, ЭЦП может использоваться при согласовании документа по кругу с внесением правок в текст документа. В этом случае документ считается согласованным в тот момент, когда последние по времени ЭЦП всех участников согласования документа оказываются валидными. После этого документ может быть передан на утверждение или визирование.

Так же важно чтобы имелась возможность не просто накладывать и проверять ЭЦП на файле документа, но и удостоверять конкретное действие по отношению к документу, например наложение согласующей, визирующей или утверждающей подписи, с учетом ее семантики. При этом важно, что действие отнесено именно к конкретной версии файла документа. В этом случае ЭЦП применяется не собственно к файлу, а к массиву данных, включающему файл и сигнатуру действия пользователя. Действия могут быть самым разнообразными, например – согласован, воздержался от согласования, утвержден, установить срок действия, и пр. В зависимости от типа документа и бизнес-процесса его обработки, могут потребоваться различные варианты наложение подписи на те или иные действия пользователя.

При этом некоторые варианты действия, например наложение утверждающей подписи, может вызывать изменение статуса документа (в данном случае эквивалентно наложению ручной подписи), после чего файл документа уже нельзя модифицировать или создавать новые его версии. Еще одним вариантом использования ЭЦП является подпись не тела документа, а отдельных атрибутов регистрационной карточки документа, которая будет подтверждать авторство и подлинность заполнения регистрационной информации или других объектов системы, например, полей задания на документ (автор, текст задания, дата создания и пр.)

Еще один аспект использования ЭЦП касается возможностей обмена электронными документами, с контрагентами компании. Наиболее просто это решалось бы при наличии полноценной инфраструктуры ЭЦП, соответствующей всем требованиям квалифицированной подписи ФЗ N63. Однако в отдельных случаях может быть использованы и другие варианты ЭЦП – простая и усиленная, требующие гораздо более дешевой инфраструктуры PKI внутри компании.