**Как переложить правила режимного бумажного документооборота в электронные системы**

Виктор Ивановский

Действия сотрудников подразделений внутренней (или информационной) безопасности описаны в Федеральном законе № 98–ФЗ "О коммерческой тайне" от 29 июля 2004 г., где в общих словах определено, какие сведения подпадают под "коммерческую тайну" и какими способами владелец информации может ее защищать (ст. 10 "Охрана конфиденциальности информации"; ст. 11 "Охрана конфиденциальности информации в рамках трудовых отношений").

Классический подход к оценке безопасности информационной системы сводится к определению приоритетов трех критериев – доступности, конфиденциальности и целостности. Если в базе данных хранятся сведения общего доступа, на первое место выходит первый параметр – "доступность". Остальные два будут иметь меньший приоритет, с точки зрения разработчика. Когда же появляются сведения, составляющие коммерческую тайну (в соответствии с упомянутым законом № 98–ФЗ и внутренними распорядительными документами), "доступность" отходит на второй план и уступает место "конфиденциальности".

Вопрос, который сразу же возникает у любого специалиста при переходе компании от бумажного документооборота к электронному, – каким образом мы будем защищать сведения, составляющие коммерческую тайну?

От теории к практике В традиционной канцелярии способы защиты сводятся к организационным мерам – простановке грифов и проверке прав каждого сотрудника на допуск к тем или иным сведениям. Утечка сведений может произойти только при физическом доступе к конкретному документу. При этом ответственность за соблюдение режима конфиденциальности ложится на лица, на хранении у которых находятся документы. Совсем по-другому обстоит дело, когда в организации планируется переход на систему ЭДО. Бумажные экземпляры документов заменяются на электронные, которые хранятся либо в виде отдельных файлов на общедоступном сетевом ресурсе, либо в составе единой базы данных (БД). Фактически объектом защиты становятся не отдельные разрозненные документы, а единая информационная система.

Задачи и пути решения Перед персоналом, занимающимся внедрением или разработкой решения системы ЭДО, как правило, ставятся следующие задачи:

- максимально защитить конфиденциальные сведения;

- минимизировать затраты на внедрение;

- по возможности задействовать существующие в компании информационные системы. Какие имеются способы для их решения?

Сразу обозначим границу – речь не будет идти о секретных сведениях, нормы работы с которыми регламентируются соответствующими документами. Мы будем рассматривать случаи, когда в организациях используются:

- типовые ограничения "для служебного пользования";

- другие ограничения, определенные внутри компании, но не подпадающие под "государственные" грифы секретности. Первый способ – самый простой – пригоден для реализации в небольших компаниях с небольшим объемом документов. В этих условиях достаточно задавать разрешения на работу с каждым конкретным документом при его создании. В данном случае ответственность за конфиденциальность ложится на исполнителя и напрямую зависит от того, как он задаст список доступа к файлу.

Способы реализации – задание прав доступа к файлам на уровне файловой системы либо с помощью Microsoft Right Management Service. Минусом данного решения является жесткая привязка к Active Directory, что ограничивает возможности по расширению системы за рамки компании.

Второй способ – использование корпоративных почтовых систем в связке с аппаратнопрограммными комплексами, осуществляющими шифрование и подпись документов. По сути, он представляется плавным переходом от одиночных файлов к БД. Защиту передачи файлов обеспечивает шифрование, идентификацию отправителя и целостность файла – проставленная ЭЦП. При этом мы уходим от привязки к Active Directory, но идеология защиты остается практически на том же уровне, что и в первом случае. С конкретным документом работает все тот же исполнитель. Если же осуществляется выход за рамки домена, появляется вероятность ошибки при назначении получателей зашифрованных файлов. Лишний адресат в строке получателей, и как результат – утечка сведений.

Тем не менее данный подход считается одним из самых популярных. Модули для работы с почтовыми программами входят в состав многих СКЗИ, временные затраты на их встраивание и обслуживание минимальны, а действия, которые необходимо выполнять конечным пользователям, интуитивно понятны.

Третий способ – организация полноценной БД. Здесь возможны следующие варианты:

- проектирование на базе одной платформы СУБД как для общих документов, так и для категорированных;

- реализация концепции раздельного доступа на базе одной платформы.

В объединении с аппаратнопрограммными комплексами СКЗИ данный подход считается наиболее защищенным и гибким для применения как в рамках одной организации, так и в масштабе нескольких компаний.

Заключение Для каждого конкретного случая решение индивидуально, но является развитием одного из вышеописанных подходов. Следует обратить внимание на два ключевых момента. 1. Затраты на приобретение, внедрение и сопровождение системы защиты ЭДО не должны превышать потенциальные потери от утечки данных. Ключ к оптимальному бюджету – экспертная оценка рисков компании в части ИБ.

2. Перед внедрением необходимо провести оценку объемов конфиденциальной информации, которые будут проходить через информационную систему. В одних случаях достаточно будет обойтись разграничениями на уровне прав доступа к файлам, в других – будет необходима организация БД.

Эффективность разработанных мер по защите конфиденциальных сведений будет напрямую зависеть от подхода компании к проведению подготовительных мероприятий.

**Список литературы**

Information Security №1, февраль-март 2009