Безопасность электронного документооборота

Владимир НИКОНОВ,
преподаватель учебного центра «Информзащита»

Задача обеспечения безопасности документооборота существовала всегда, и за прошедшие века были найдены решения, обеспечившие полное доверие к документам на бумаге. Сам лист бумаги позволяет убедиться в целостности документа, поэтому в части стран законодательные акты и судебные решения хранятся в виде бумажных свитков, чтобы не было возможности позднейшей вставки. Вопросы доверия к документу на бумаге решаются с помощью штампов, печатей, личных подписей или печаток, а в особых случаях применяются водяные знаки или специальная фактура бумажной поверхности. Кроме того, можно ограничить доступ к содержанию документа, применяя такой способ, как шифрование.

Использование электронных документов, да и само понятие электронного документа появилось относительно недавно. Первоначально файлы были заготовками для редактирования документа. Потом оказалось удобным передавать файл вместе с бумажным документом. Появление первых сетей, а затем и доступа к сети интернет полностью изменило положение, предоставив новые возможности для передачи данных в электронном виде. Использование электронных документов в сравнении с бумажными дает большие преимущества, сокращая расходы на их создание, пересылку и хранение, обеспечивает быстрое нахождение документов, а также предоставляет возможность удаленного доступа. Поэтому использование документов в электронном виде стало очень привлекательным. Сначала крупные учреждения, а затем и все остальные перешли на использование электронных документов. За короткое время оказался возможным полный переход к электронному документообороту, и некоторые страны совсем отказались от бумажных документов. Электронный документооборот особо привлекателен для Российской Федерации, правительство страны приняло решение о полном переходе на использование электронного документооборота и, соответственно, об отказе от бумажного документооборота.

Для полного перехода на использование электронных документов необходимо решить вопросы доверия к ним и обеспечить уровень безопасности, не уступающий бумажному документообороту. Решаются эти вопросы с помощью применения совокупности мер.

В соответствии с положениями Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» для защиты информации используются правовые, организационные и технические меры, направленные на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Правовые меры принимает правительство Российской Федерации, осуществляя государственное регулирование отношений в сфере защиты информации путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации.

Выбор и принятие необходимых организационных и технических мер решается непосредственно самим обладателем информации.

Если электронные документы содержат сведения конфиденциального характера (указ президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» № 188 от 06.03.1997 г., указы «О внесении изменения в перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 6 марта 1997 года № 188» № 1111 от 23.08.2005 г. и № 357 от 13.07.2015 г.), например, персональные данные, обработка которых регулируется отдельными законами (Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ),то при выборе мер необходимо обеспечить соблюдение требований законодательства Российской Федерации. Федеральными органами, такими как Федеральная служба безопасности и Федеральная служба по техническому и экспортному контролю Российской Федерации, могут быть установлены дополнительные требования по защите информации.

Выбор способов и средств защиты зависит от поставленных задач по обеспечению безопасности:

- ограничение доступа;
- разграничение полномочий;
- обеспечение доверия;
- защита содержания.

Самый распространенный способ ограничения доступа к ресурсам – это создание учетных записей с помощью встроенных средств операционной системы или какой-либо информационной системы. Отличаются только протоколы, применяемые при передаче данных идентификации пользователя, начиная от кодирования и вплоть до использования значений хеш-функций и шифрования, выбор протокола определяет уровень безопасности доступа. Независимо от протокола учетные записи могут обеспечить лишь грубое деление пользователей на доверенных и недоверенных, если же мы хотим предоставлять пользователям разные полномочия, то для этого нужны другие решения.

Начнем с простой задачи разграничения полномочий по редактированию электронных документов. Нередко в подразделениях крупных организаций используются общие электронные документы, подготовленные в головном подразделении. Эти документы обычно содержат таблицы с данными, используемыми сотрудниками подчиненных подразделений. Искажение данных может привести к нарушению сводной отчетности организации. Для разграничения полномочий по работе с данными в электронных документах можно задействовать встроенные возможности редакторов, определив группы пользователей, которым будет предоставлено право на чтение или на внесение изменений в электронный документ или только в определенные листы и области. Такой способ разграничения полномочий предоставляет больше возможностей, чем простое «пустить – не пустить», но в целом возможности редакторов ограничены и помимо ограничения редактирования других задач решать они не могут.

Намного большими возможностями по разграничению полномочий пользователей при работе с электронными документами обладают специализированные программные средства, например такие, как служба управления правами ActiveDirectory. С ее помощью можно разграничить права на чтение, редактирование, копирование, печать и пересылку электронных документов. Возможно ограничение срока предоставления доступа пользователей к электронному документу. С помощью этой службы организации могут применять единую корпоративную политику по использованию и распространению конфиденциальных сведений. Заданная для электронного документа политика остается с ним независимо от его перемещения, отправки или пересылки. Для защиты содержания электронных документов и заданных политик используется шифрование с помощью встроенных средств операционной системы Microsoft.

Существующие способы разграничения доступа позволяют защитить электронные документы от неправомерного доступа, уничтожения, модифицирования, копирования и распространения в рамках одной системы, но не могут обеспечить решение вопроса доверия при электронном взаимодействии пользователей разных систем.

Использование полноценного электронного документооборота предполагает обеспечение доверия к самим электронным документам независимо от того, где и кем они созданы. Наиболее успешно вопрос доверия решается с помощью так называемой электронной подписи.

Законодательной основой для применения электронной подписи является Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ, в котором даны определения двух основных видов электронной подписи, которые носят название простой и усиленной электронной подписи.

Простая электронная подпись позволяет определить создателя подписи путем добавления к электронному документу подтверждающего значения, такого как код, строка, личная подпись или отпечаток пальца, полученные с помощью считывателя. Такие способы широко распространены, не требуют больших затрат, просты в использовании, чем, собственно, и привлекательны для пользователей. Уровень безопасности, который обеспечивает простая электронная подпись, невысок, но может быть вполне достаточен, например, для обеспечения доверия во внутреннем документообороте. Многие платежные системы для обеспечения доверия при электронном взаимодействии с клиентами используют простую электронную подпись.

Более высокий уровень безопасности обеспечивает усиленная электронная подпись, которая представляет собой набор данных вместе с зашифрованной частью, позволяющей однозначно установить создателя электронной подписи и проверить целостность электронного документа. Шифрование выполняется с использованием личного ключа пользователя и предполагает применение средств криптографической защиты информации, что требует определенных затрат на их приобретение, установку и настройку, а также на предварительное обучение пользователей работе с такими средствами. Существуют и простые решения, когда средства криптографической защиты информации устанавливаются на удаленном сервере и туда предоставляется доступ доверенным пользователям. Такого рода решение используется Федеральной налоговой службой, где в своем личном кабинете каждый налогоплательщик может отправить электронный документ на удаленный сервер и воспользоваться возможностью создания там своей электронной подписи. При проверке электронной подписи выполняется расшифровывание зашифрованной части подписи с помощью известного открытого ключа пользователя, который хранится вместе с учетной записью пользователя. Если же пользователи взаимодействуют, не используя общее хранилище учетных данных, то для обеспечения доверия к открытому ключу применяется документ, подтверждающий владение пользователя открытым ключом, который носит название сертификата открытого ключа или ключа проверки электронной подписи. Создают сертификаты удостоверяющие центры, которым

должны доверять все участвующие в электронном взаимодействии пользователи. Доверие к сертификату обеспечивает электронная подпись, созданная удостоверяющим центром.

Для полного перехода Российской Федерации на использование электронного документооборота создана система аккредитованных удостоверяющих центров. Эти центры получают электронный сертификат своего ключа проверки электронной подписи у головного удостоверяющего центра, роль которого выполняет уполномоченный федеральный орган. Головной удостоверяющий центр объединяет аккредитованные удостоверяющие центры и всех тех, кто получает там сертификаты. Поэтому при проверке электронной подписи электронного документа, из какой бы части страны этот документ ни поступил, оказывается возможным построить цепочку доверия до головного удостоверяющего центра. В итоге мы получаем возможность построения единого электронного документооборота для всех граждан и учреждений Российской Федерации.

Очень важная задача при электронном взаимодействии – это соблюдение конфиденциальности информации ограниченного доступа с помощью защиты содержания электронных документов. Есть разные решения этой задачи, выбор зависит от способа взаимодействия пользователей.

При сетевом взаимодействии пользователей можно ограничить доступ к передаваемым данным, используя набор протоколов IPSecurity. Для защиты данных и ограничения доступа используется шифрование на общем ключе, при этом могут применяться разные криптографические алгоритмы и программные средства, в том числе и разработанные в России.

При взаимодействии пользователей с помощью сети интернет используются протоколы TLS/SSL. Для защиты передаваемых данных используется шифрование на общем ключе. Данный способ защиты получил широкое распространение, и, когда при использовании какого-либо ресурса вы видите в заголовке https, – это и есть пример применения криптографических протоколовTLS/SSL. Для согласования ключа шифрования используется сертификат с определенным назначением, полученный владельцем интернет-ресурса в удостоверяющем центре.

Если пользователи взаимодействуют посредством почтовых сообщений, то для их защиты создан стандарт протоколов S/MIME. Защита передаваемых почтовых сообщений обеспечивается в этом случае совместным использованием электронной подписи и шифрования. Здесь все участники взаимодействия должны получить свой сертификат в удостоверяющем центре с необходимыми указаниями о назначении ключей.

Существующие информационные и платежные системы используют совокупность решений для защиты передаваемых электронных данных и обеспечения доверия к ним, но есть и немало схем, где используется только одно из вышеперечисленных решений.

При удаленном взаимодействии пользователей разных систем наиболее эффективными являются решения с использованием сертификатов, обеспечивающие доверие ко всем взаимодействующим сторонам и позволяющие удаленно согласовать ключи шифрования для защиты передаваемых электронных данных, а также использовать в рамках электронного документооборота усиленную электронную подпись. Этим достигается наиболее высокий уровень защищенности передаваемых электронных документов и степени доверия к ним.

Имеющиеся в нашем распоряжении средства позволяют при любом электронном взаимодействии обеспечить необходимый уровень безопасности электронного документооборота.