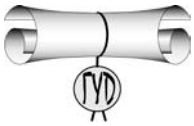

Проблемы обеспечения защиты и юридической силы электронного документа при хранении

Сабанов Алексей Геннадьевич, заместитель генерального директора ЗАО «Аладдин Р.Д.», к.т.н.

Введение

До сих пор понятие защищенного электронного документооборота (ЗЭД) расплывчато и неполно. В нормативных документах это понятие не раскрывается. На сайтах некоторых разработчиков систем электронного документооборота (СЭД) до сих пор можно найти ряд определений, из которых следует, что для того, чтобы защитить СЭД, достаточно использование электронно-цифровой подписи (ЭЦП). Как правильно использовать ЭЦП, какая инфраструктура при этом нужна и какие защищенные сервисы необходимо развернуть на ее основе, зачастую также не раскрывается. На сайтах интеграторов (компаний, внедряющих эти решения), как правило, приводятся конкретные реализации систем ЗЭД определенных поставщиков; тех, с которыми у интеграторов уже сложились определенные бизнес - отношения и есть обученные для внедрения специалисты.

Понятие ЗЭД определить достаточно трудно, особенно в условиях динамично меняющегося российского правового поля, недостатка стандартов и бурно развивающихся технологий. В этих условиях постараемся затронуть некоторые наиболее спорные и актуальные вопросы защиты СЭД, тем самым раскрывая и уточняя само понятие ЗЭД и его компонентов.

Почему задача защиты документооборота становится актуальной только сейчас

Если формулировать задачу предельно коротко, то просто пришло время. Можно выделить несколько основных причин, по которым именно сейчас вопросы развития ЗЭД становятся объектом внимания:

- при непосредственном участии первых лиц государства интенсивно развиваются государственные услуги, оказываемые в электронном виде, обмен электронными документами быстро набирает критическую массу, при которой неизбежно

встают вопросы защиты конфиденциальной информации, в частности, персональных данных;

- услуги, предоставляемые в электронном виде, должны базироваться на ЭЭД, поскольку формированию электронного документа в ответ на запрос от физического или юридического лица, как правило, предшествует огромная работа по обмену документами многих ведомств, который далеко не всегда надо делать общедоступным;
- приходит массовое понимание необходимости внедрения СЭД в государственных организациях, работающих с гражданами и юридическими лицами, и применения средств защиты для обеспечения целостности и конфиденциальности информации, содержащейся в электронных документах, а также подтверждения авторства электронных документов;
- принят Федеральный закон №63-ФЗ «Об электронной подписи», который дает возможность более широко подойти к защите электронных документов, в частности, использовать различные технологии для использования электронной подписи, а следовательно, и защиты СЭД в зависимости от их принадлежности и других условий;
- при массовом переходе к «облачным» вычислениям вопросы информационной безопасности таких вычислений и защиты ЭДО становятся еще более актуальными;
- появляется реальная необходимость обеспечения и понимание механизмов придания электронным документам юридической силы наравне с бумажными документами.

Изменение парадигмы защиты систем ЭДО

Если еще недавно защищались сами электронные документы или информационный ресурсы, содержащие документы, то теперь изменяется основной вектор атак и соответственно изменяется объект защиты. Кроме традиционных атак на информационный ресурсы все чаще и чаще объектом становится **взаимодействие** «человек - электронный документ», «человек – информационный ресурс». Главный тезис: защищать надо не только непосредственно документы, но главным объектом защиты считать сами системы передачи, обработки и хранения электронных документов при доступе легальных пользователей систем к работе с электронными документами. Понятно, что взаимодействие – это процесс, и как любой процесс он тянется во времени. Задача защиты взаимодействия, также как и сам процесс, распределяется на этапы. Одним из

важнейших этапов является процедура доступа пользователя к системе, к инструментам обработки и непосредственно к документам. Например, система управления доступом должна предусматривать минимизацию прав доступа каждого пользователя из соображений достаточности для выполнения непосредственных служебных функций. При этом очень важным фактором является обеспечение защищенного доступа с применением в качестве механизмов двухсторонней двухфакторной аутентификации таких развитых сервисов безопасности, как ЭЦП. Для этого необходимо построить инфраструктуру открытых ключей, систему управления закрытыми ключами, использовать защищенные носители, но это позволит применение технологий, обеспечивающих защиту взаимодействия пользователя с информационными ресурсами и содержащимися в них документами.

Что такое защищенный электронный документооборот?

Определим ЗЭДО как электронный документооборот, обеспечивающий конфиденциальность, целостность и доступность информации в системе ЗЭДО для легальных пользователей. Основной идеей предлагаемого подхода является то, что к задаче защиты системы электронного документооборота надо подходить классически с точки зрения защиты информационной системы. А именно, кроме известных уже среди разработчиков СЭД задач по защите электронных документов, таких как:

- аутентификация пользователей и разделение доступа;
- подтверждение авторства электронного документа;
- контроль целостности электронного документа;
- конфиденциальность электронного документа;
- обеспечение юридической значимости электронного документа

для организации ЗЭДО необходимо использовать механизмы, обеспечивающие

- контроль целостности используемого программного обеспечения;
- регистрацию событий в информационной системе ЗЭДО;
- криптографическую защиту;
- межсетевое экранирование;
- защиту каналов с помощью виртуальных частных сетей;
- антивирусную защиту;
- аудит информационной безопасности,

которые хорошо известны широкому кругу специалистов по защите информации.

Коротко рассмотрим некоторые аспекты защиты системы ЭДО, вызывающие дискуссии и вопросы в печати, на конференциях и семинарах.

Аутентификации пользователей

Несмотря на то, что про аутентификацию пишут и говорят много в течение последних 5-8 лет, к вопросам практического применения тех или иных технологий аутентификации приходится обращаться все чаще и чаще. Например, в целях достижения наиболее быстрого результата многие участники организации ЗЭД пытаются применять вместо аутентификационных идентификационные технологии. Типичным случаем является использование биометрических способов идентификации личности. При внешней привлекательности решения (не надо носить с собой смарт - карту и помнить ПИН-код) эта технология на практике слишком дорога и не предоставляет необходимого уровня надежности (ошибки первого и второго рода). В принципе, процесс идентификации в ряде случаев не позволяет достичь тождественной однозначности. Простой и понятный всем пример: Вы предъявили паспорт. Это – идентификация личности по документу. Однако фотография может быть подменена (таких случаев множество) или кого-то удачно загримировали под Вас. А вот если бы во время проверки паспорта Вам задали ряд вопросов, на которые можете ответить только Вы, и Вы ответили правильно на все вопросы – это уже полноценная аутентификация, т.е. подтверждение подлинности идентификации. Аутентификация - это подтверждение подлинности идентификатора, производимое, как правило, с помощью криптографических преобразований. В итоге мы получаем логическую цепочку: без надежной идентификации нельзя, самой надежной идентификацией является аутентификация, следовательно, без аутентификации не обойтись. Мало того, строгая аутентификация позволяет не только разделить, но и персонифицировать доступ, т.е. сделать всех пользователей, работающих, например, с персональными данными, лично ответственными за все их действия с этими данными. Как уже упоминалось выше, при этом надо сделать доступ минимально-достаточным для выполнения своих рабочих обязанностей. Современным подходом для организации персонифицированного доступа является применение решений на базе PKI, при этом механизмом аутентификации фактически является процедура электронной подписи.

Учитывая вышесказанное, можно сказать, что для организации ЗЭД необходимы:

- Строгая аутентификация пользователей для организации доступа к защищаемым и информационно-значимым ресурсам;

- Ограничение доступа к конфиденциальной информации и персональным данным;
- Блокирование несанкционированного доступа;
- Обеспечение доступности публичной информации.

Обеспечение юридической силы электронных документов

Споры о том, какими способами можно придать электронному документу юридическую силу, а ЗЭДО – юридическую значимость, будут длиться еще долго, скорее всего, до выхода закона, где это будет прямо указано. Однако никто уже не спорит, что для обеспечения юридической значимости ЗЭДО необходимы три составляющих: соответствующая нормативно-правовая база, организационные меры и техническая составляющая.

Обеспечение юридической силы электронному документу (это понятие, кстати, тоже законодательно не определено) не поддерживается текущим состоянием законов. Для бумажного документооборота Постановлением Правительства №477 от 15.06.2009г. определен минимальный набор из 24 реквизитов для придания бумажному документу юридической силы. Для электронного документа набор реквизитов будет меняться в зависимости от степени важности документа (от правовых последствий), однако сейчас законодательно ни минимальный, ни полный набор таких реквизитов не определен. Понятно, что такими реквизитами в электронном мире будут доверенные (то есть надежные, проверенные, поддерживаемые в соответствии с регламентами) сервисы, такие, как сервис электронной подписи, сервис штампов времени, сервис заверения полномочий подписанта, сервис аутентификации и т.д.

В соответствии с этим должны применяться и организационные меры по обслуживанию (созданию, хранению, передаче, обработке и т.д.) электронных документов, имеющих юридическую силу.

Отдельным вопросом необходимо рассматривать проблемы организации архива электронных документов, обладающих необходимыми реквизитами для юридической силы. Особенно остро в настоящее время специалистами обсуждаются проблемы проверки наличия полномочий подписанта на момент электронной подписи. Основные вопросы, вызывающие дискуссии, представлены в докладе.

Теперь коснемся технической составляющей, точнее, ее инфраструктурной части, вызывающей споры специалистов. Основываясь на результатах работы [3], заметим, что для обеспечения юридической силы электронных документов необходимо, чтобы были построены и развиты:

- Инфраструктура электронных баз данных документов (реестры, регистры, кадастры), принадлежащих разным ведомствам;
- Инфраструктура квалифицированной электронной подписи, включающая аккредитованные удостоверяющие центры, входящие в единую систему на базе развитой инфраструктуры открытых ключей – PKI, архитектура национальной системы PKI пока окончательно не утверждена, но все понимают, что существующие ведомственные «островки доверия» необходимо связать в единую систему;
- Инфраструктура доверенных сервисов, таких, как доверенная третья сторона, инфраструктура доверенного времени для проставления меток времени, прилагаемых к электронному документу, на основе доверенного источника времени; инфраструктура удостоверения места издания документа (сделки, контракта, договора, соглашения) двумя или более сторонами на основе доверенной третьей стороны и инфраструктура валидации (проверки действенности предъявленных к проверке цифровых сертификатов);
- Инфраструктура электронных реестров участников информационного взаимодействия, для подтверждения их правового статуса, правомочий, полномочий, и права подписи.

Задача управления закрытыми ключами

Согласно п.1 ст.10 Федерального закона №63-ФЗ участники электронного взаимодействия обязаны обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия. Другими словами, задача хранения закрытого ключа лежит на его владельце. Может ли неподготовленный пользователь самостоятельно обеспечить безопасность своего закрытого ключа?

Безопасность закрытого ключа пользователя должна быть обеспечена на каждом из этапов его жизненного цикла: на этапе генерация ключевой пары (открытый и закрытый ключи), во время хранения закрытого ключа, при использовании закрытого ключа (выполнение криптографических операций, требующих использования закрытого ключа пользователя, например – формирование электронной подписи) и при уничтожении

закрытого ключа. Генерация ключевой пары должна выполняться в среде, исключающей возможность влияния злоумышленника на сам процесс генерации, так и возможность получения какой-либо информации о закрытом ключе, которая может впоследствии быть использована при попытке его восстановления.

При хранении закрытого ключа должны быть обеспечены его конфиденциальность и целостность – ключ должен быть надёжно защищён от несанкционированного доступа, а также модификации. Лучшими устройствами для генерации и хранения закрытых ключей являются аппаратные устройства класса eToken, которые также предназначены для выполнения криптографических операций, требующих использования закрытого ключа.

При использовании закрытого ключа важно исключить возможности его перехвата, а также несанкционированного использования (помимо воли и желания владельца ключа).

И, наконец, на этапе уничтожения закрытого ключа необходимо обеспечить гарантированное уничтожение информации и полностью исключить возможность его повторного использования (например, путём восстановления ранее удаленного хранилища).

Организация защищенного электронного документа в «облаках»

При переходе к облачным вычислениям вопросы защиты информации становятся весьма актуальными, тем более, что в настоящее время эта область знаний пока не исследована до приемлемого для практики уровня. При всех достоинствах облачных сервисов (в первую очередь, отсутствие необходимости содержать развитую инфраструктуру из аппаратных и программных компонентов на местах, необходимости закупки и содержания дорогих компьютеров и ПО, отказоустойчивость, экономичность и эффективность, простота использования, гибкость и масштабируемость), вычисления в облаках в настоящее время являются зоной повышенного риска с точки зрения безопасности. Как известно, при организации облачных вычислений отсутствует понятие «защищенного периметра». При этом весьма трудной задачей становится построение системы «доверенных» сервисов, без которых невозможно решение многих актуальных задач информационной безопасности, таких, например, как обеспечение юридической силы электронного документа и электронного взаимодействия в облаках в целом. При отсутствии нормативной базы и стандартов ИБ для облачных вычислений переводит использование облачных сервисов в разряд самых рискованных.

К обычным критериям ИБ, сформулированным как выполнение задач обеспечения конфиденциальности, доступности и целостности информации добавить применительно к облакам вряд ли кто сможет. Другое дело, что выполнить эти критерии в облаках весьма непросто. Потенциальным пользователям облачных сервисов можно только посоветовать не хранить в облаках не обезличенную (незашифрованную) информацию (конфиденциальность), обеспечивать гарантированную строгую взаимную аутентификацию «пользователь-ресурс» (доступность) и использовать средства обеспечения целостности информации, например, с помощью применения усиленных квалифицированных электронных подписей.

Новая архитектура, новые подходы к расчетам и хранению данных в распределенных и удаленных вычислительных центрах требуют применения новых технологий защиты.

Есть отдельные (возможно, неплохие) решения, но в целом обеспечить безопасность облачных вычислений сегодня трудно. Однако не все так плохо. Поскольку Указом Президента РФ от 8 февраля 2012 г. № 146 определено, что федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности данных в информационных системах, созданных с использованием суперкомпьютерных и грид-технологий, являются ФСБ России и ФСТЭК России, за безопасность назначены правильные ответственные. Соответственно, можно надеяться, что в недалеком будущем появятся нормативные документы, в которых будут правильно оценены риски и выданы рекомендации по защите интересов государства, бизнеса и граждан.

Заключение

Безусловно, строительство электронного правительства и информационного общества должно дать мощный толчок развитию систем ЗЭДО. Например, развитие таких массовых систем, как система государственных закупок, невозможно без ЗЭДО. По сути, сами торги должны являться своего рода вершиной айсберга, основу которого должен составлять защищенный обмен документами (сбор заявок от потребителей, бюджетирование, обоснование стоимости и т.д.). Не менее важна роль ЗЭДО и при оказании государственных услуг с применением электронных документов, электронного взаимодействия в целом. При этом весьма актуальными являются вопросы межведомственного обмена защищенными документами, который ложится в основу подготовки выданного по заявке гражданина или организации электронного документа, имеющего правовые последствия.