ЭКСПЕРТНЫЙ СОВЕТ

КАТАЛИЗАТОР ПРОЦЕССОВ ДОКУМЕНТООБОРОТА

Александр Безбородов, фирма «1С»

Работа с информацией автоматически предполагает обеспечение ее достоверности и защиту от несанкционированного доступа. Одним из таких средств можно считать электронную цифровую подпись (ЭЦП). В системах электронного документооборота ЭЦП защитит от фальсификации и от раскрытия содержимого документов, которые всем видеть не положено.

Юридическая основа

Использование электронной цифровой подписи и порядок ее использования регламентируется законодательно. Так, Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» предусматривает несколько видов электронной подписи:

- простую;
- неквалифицированную;
- квалифицированную.

Простая электронная подпись подтверждает факт своего формирования определенным лицом посредством использования кодов, паролей или иных средств.

Неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Квалифицированная электронная подпись соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной под-

писи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным Законом № 63-ФЗ, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

Все эти виды электронной подписи поддерживаются в системе «1С:Документооборот» и могут использоваться одним лицом. Допустим, руководитель компании может использовать одну подпись для согласования договорных отношений, другую — для подписания договоров, третью — для подписания ответов на обращения частных лиц и т.д. У всех этих подписей могут быть разные статусы, разный жизненный цикл.

> **Основные цели применения ЭЦП — обеспечение безопасности и достоверности информации в системе документооборота. Обычно механизм ЭЦП решает две задачи: шифрование данных и формирование подписи. В системах электронного документооборота обычно шифруются файлы с персональными данными, планы реструктуризации зарплат и сокращения сотрудников, протоколы конфиденциальных переговоров и пр. документы. Шифрование документов защитит их от просмотра лицами, наделенными по роду деятельности полными правами доступа к информации в системе электронного документооборота, например, от сотрудников информационно-технологических подразделений.**

Формирование электронной подписи предусматривается при подписании, согласовании и утверждении электронных документов, при отправке документов по почте в другую организацию или учреждение. При этом важно понимать, что ЭЦП не устранит утечку информации от сотрудников, которые имеют к ней доступ по роду работы. Но ЭЦП защитит от фальсификации и от раскрытия документы, которые видеть всем не положено.

Регламент

Электронная подпись включает установку и проверку. До начала использования ЭЦП должен быть выработан регламент. Это может быть сделано, например, в рамках инструкции по документообороту. Кроме того, правила применения ЭЦП должны быть отражены также в должностных инструкциях, в которых указывается:

- какой подписью нужно пользоваться в том или ином случае;
- когда надо устанавливать подпись, а когда — нет;
- кто и когда выполняет проверку подписей;
- что делать, если проверка подписи не прошла.

ЭКСПЕРТНЫЙ СОВЕТ

Необходимо учесть, что подписей может быть много, и они могут иметь разный порядок использования. Для этого в дополнение к каждой подписи можно приписать краткий комментарий, поясняющий ее назначение. Причем система электронного документооборота сама должна следить за соблюдением регламентов, помогать пользователям и обеспечивать правильное использование ЭЦП.

Итак, регламент разработан. Теперь, чтобы использовать ЭЦП, необходимо выполнить шесть основных шагов.

1. Развернуть инфраструктуру ЭЦП или заключить договор с удостоверяющим центром только для юридически значимой ЭЦП.
2. Получить от удостоверяющего центра сертификат электронной цифровой подписи, которая будет использоваться непосредственно в программе при выполнении, например, команд «подписать», «зашифровать».
3. Реализовать обмен открытыми сертификатами между пользователями.

Открытый сертификат — небольшая часть ЭЦП, которая передается от одного пользователя к другому, чтобы тот мог проверить, что это действительно подпись лица, подписавшего тот или иной документ. Открытая часть сертификата не несет в себе никаких секретных сведений (поэтому и называется «открытой») и может безопасно передаваться, например, сотрудникам, чтобы они могли удостовериться, что да, действительно, этот документ подписан директором или начальником юридического отдела.

В системе электронного документооборота полезно создать папку файлов «Открытые сертификаты» и складывать в нее открытые сертификаты всех ответственных лиц. Эти сертификаты каждый сотрудник должен перенести на свой локальный компьютер и дальше использовать их в своей работе для проверки ЭЦП, которая поступает к нему вместе с документами и файлами.

4. Настроить шаблоны процессов согласования — указать в них необходимость установки ЭЦП.
5. Научить сотрудников пользоваться ЭЦП.
6. Назначить ответственного за соблюдение регламента работы с ЭЦП. Задача ответственного — следить за тем, чтобы ЭЦП применялась вообще и применялась правильно. Он должен знать закон «Об электронной подписи», ГОСТы, квалифицированно отвечать на вопросы пользователей. Это необходимое условие того, чтобы ЭЦП действительно использовалась всеми, кто в соответствии со своими должностными инструкциями, должен с ней работать.

ЭКСПЕРТНЫЙ СОВЕТ

Необходимо также и очень важно приказом по организации довести до сведения всех сотрудников, что подписанные ЭЦП электронные документы, находящиеся в системе электронного документооборота, имеют такую же силу, как и бумажные.

Выбор криптопровайдера

Криптопровайдер — это технология и программное обеспечение для использования в организации ЭЦП. Выбор криптопровайдера осуществляется в зависимости от задач, которые решаются в системе электронного документооборота.

Так, при юридически значимом документообороте (например, согласование и подписание договора с другой организацией) файл с текстом документа находится в системах документооборота обеих организаций и подписывается электронной подписью каждой стороны. В этом случае надо использовать криптопровайдер, поддерживающий ГОСТ Р 34.10-2001, например, КриптоПро, СигналКом, ViPNet. Причем обе организации должны использовать одни и те же алгоритмы подписи и хеширования.

Для ЭЦП юридически значимого документооборота потребуется приобрести криптографическое программное обеспечение (ПО), соответствующее ГОСТ Р 34.10-2001 и заключить договор с удостоверяющим центром для получения сертификатов. Криптографическое программное обеспечение надо будет установить на компьютеры пользователей. Приобретается криптографическое программное обеспечение у организаций, специализирующихся на защите данных, имеющих сертификаты на соответствие ГОСТу, законодательству. Эти организации и обеспечивают квалифицированный уровень обслуживания ЭЦП.

Если в электронном документообороте есть несколько участников, тогда все они должны использовать одного криптопровайдера, одну криптотехнологию и обращаться в один и тот же удостоверяющий центр. Этот удостоверяющий центр будет выдавать сертификаты на ЭЦП всем участникам электронного документооборота, проверять их достоверность, сообщать, что срок сертификата истек, и выполнять другую работу по обслуживанию. Понятно, что эти услуги потребуют от организации некоторых финансовых затрат.

При реализации внутреннего документооборота ЭЦП используется только внутри фирмы, например, для подписания файлов приказов, находящихся в системе электронного документообороте или шифрования файлов. В этом случае можно использовать криптопровайдер, не поддерживающий ГОСТ Р 34.10-2001. Это может быть, к примеру, бесплатный Microsoft Enhanced Cryptographic Provider v1.0, который входит в Microsoft Windows.Он довольно просто устанавливается и настраивается. С его помощью можно реализовать регламент использования ЭЦП на хорошем уровне.

ЭКСПЕРТНЫЙ СОВЕТ

Если организации не нужен юридически значимый документооборот за ее пределами, то достаточно с помощью Windows Server 2008(или 2003) развернуть Certificate Authority. Он не будет соответствовать ГОСТам, но обеспечит шифрование документов и хороший уровень поддержки ЭЦП. Финансовые затраты — покупка программного обеспечения (Windows Server 2008), но, скорее всего, оно в организации уже имеется, и оплата труда специалиста, который будет его поддерживать.

Практика вносит коррективы

Предположим, директор компании согласовывает и утверждает документы, используя ЭЦП. Он уезжает в командировку, и там, включая свой компьютер, обнаруживает, что срок действия сертификата ЭЦП истек. Передача же сертификата по электронной почте — дело небезопасное, почту могут вскрыть и прочесть. Что делать в такой ситуации? Ждать окончания командировки, чтобы вернуться в офис и там решить возникшую проблему? Либо нужно было заранее знать какой-то секретный канал связи с администратором, по которому тот вышлет ему новый сертификат?

Поскольку не все удостоверяющие центры предоставляют программное обеспечение для удаленного защищенного обновления сертификатов, то выбирая «свой» удостоверяющий центр, не следует забывать о возможном возникновении такого рода проблем.

Как правило, используют ЭЦП и проверяют ее небольшое число сотрудников. Например, в компании 1,5 тыс. сотрудников, но реально используют ее не более 10 менеджеров. Именно им и только им устанавливается соответствующее программное обеспечение. За счет этого экономятся средства на покупку криптографического ПО. А остальные сотрудники, работающие в системе электронного документооборота, если возникнет необходимость проверить ЭЦП, будут проверять ее на сервере (при этом на сервере также потребуется установить криптографическое ПО).

В этом случае проводятся соответствующие настройки, программное обеспечение проверки ЭЦП устанавливается на сервере, и программа будет автоматически сообщать результат: «да, эта подпись верна», «нет, эта подпись не верна».

Важно отметить также, что при подписании документа подписывается не только он сам, но и все приложенные к нему файлы. В карточке документа отображается, во-первых, подписан ли сам внутренний документ, и, во-вторых, подписан ли файл, приложенный к нему.

Внешний документооборот

Электронная цифровая подпись используется и в системе внешнего документооборота для организации электронного документооборота с контрагентами компании.

В этом случае компании договариваются, что все документы (входящие и исходящие) будут иметь электронную подпись. В момент отправки, если исходящий документ не имеет ЭЦП,

ЭКСПЕРТНЫЙ СОВЕТ

то система электронного документооборота требует установки для него ЭЦП. Когда документ поступает в компанию, то секретарь, регистрируя его как входящий электронный документ, присваивает ему идентификационный номер.

Когда документ поступает с ЭЦП, то система сама проверит ее и в случае ошибочной подписи сообщит об этом адресату.

Входящий документ с ошибочной ЭЦП будет помечен как «ошибочный». В систему электронного документооборота он вовлечен не будет. Ответственный за разбор документов сразу увидит его и сможет оперативно отреагировать.

Таким образом, перед тем, как начинать работу с ЭЦП, необходимо определить регламент ее использования, кому она нужна в организации, кто будет отвечать за работу с ней. И когда использование ЭЦП станет повседневной практикой, скорость прохождения документов за счет сокращения времени их обработки значительно возрастет. А это означает, что ЭЦП стала в компании настоящим катализатором процессов документооборота.