# Ваш цифровой автограф

**В прошлом номере журнала мы в общих чертах осветили процесс передачи электронной отчетности в налоговую инспекцию. Как уже было отмечено, первый шаг в работе с отчетами бухгалтер делает, покупая Электронную цифровую подпись (ЭЦП). В этот раз мы подробно расскажем о том, что такое ЭЦП и на что следует обратить внимание при ее приобретении у компании — оператора по передаче электронной отчетности.**

Авторы статьи:
**А.А. Пауков,**
генеральный директор компании «ГАРАНТ Электронный Экспресс», к. э. н.,
**М.В. Быданцев,**
руководитель Удостоверяющего центра ГАРАНТ, компания «ГАРАНТ Электронный Экспресс»

Принятие Федерального закона «Об электронной цифровой подписи»[1] предоставило специалистам возможность в ряде случаев заменить бумажные документы их электронными аналогами. ЭЦП, созданная в соответствии с принятыми государством стандартами, нужна для того, чтобы электронный документ сохранял юридическую значимость. Проще говоря, это реквизит электронного документа, предназначенный для его защиты от подделки. Использование ЭЦП позволяет подтвердить авторство такого документа, а также определить, изменялся ли он после подписания.

Безусловно, тут возникает ряд закономерных вопросов. Что нужно сделать, чтобы получить ЭЦП и использовать ее при подписании документов? Что представляет из себя эта самая электронная подпись? Давайте по порядку.

## Удостоверяющий центр — наше все!

Итак, вам необходимо получить ЭЦП, позволяющую передавать отчетность в инспекцию. Для этого вам следует обратиться в специализированную организацию — Удостоверяющий центр (УЦ), аккредитованный в сети доверенных УЦ ФНС России (перечень таких УЦ публикуется на сайте http://www.gnivc.ru/)[2]. Далее существуют два сценария развития событий (в зависимости от организации работы конкретного УЦ). Первый — вы заключаете с УЦ договор на оказание услуг по выдаче ЭЦП, а также оплачиваете счет данной организации. Второй — вы знакомитесь с существующим регламентом УЦ и, оплатив счет, подписываете заявление о присоединении к нему (заключать отдельный договор в этом случае не придется). При любом сценарии вам нужно будет еще и оплатить отдельный счет УЦ на приобретение лицензии на специальную программу — Средство криптозащиты информации (СКЗИ).

Следующий шаг, который вам нужно сделать, — это установить на ваш компьютер СКЗИ. Данную программу вам может поставить специалист УЦ. Или же вы сами можете ее установить из дистрибутива (например, компакт-диска), предоставленного Удостоверяющим центром (тут все зависит от вашей договоренности с УЦ). О том, зачем нужна данная программа, мы расскажем чуть позже.

## Формируем закрытый ключ

Идем дальше. По факту оплаты счета УЦ выдаст вам персональный код для удаленного доступа. Зайдите на сайт вашего Удостоверяющего центра и введите этот код в специальное окошко. Поздравляем вас! Теперь вы получили возможность сгенерировать так называемый закрытый ключ (а проще говоря, создать вашу электронную цифровую подпись). Далее, следуя инструкциям, приведенным на сайте, вы создаете свою ЭЦП, визуально представляющую из себя определенную уникальную последовательность цифр. По окончании этого процесса сохраните вашу подпись (закрытый ключ) на надежный носитель (можно использовать обычную флешку, а лучше — специальную флешку с защищенной областью памяти (в народе называемую «токен»)). На сайте УЦ предусмотрена функция, позволяющая вам сделать это. Так вот, именно для того, чтобы вы могли создать защищенное соединение и сгенерировать на своем рабочем месте закрытый ключ без опасения утечки информации, и нужна СКЗИ, которую вы уже установили на компьютере ранее.

[1] Федеральный закон от 10.01.2002 № 1-ФЗ

[2] УЦ, как правило, является подразделением компании, организующей передачу отчетности и разрабатывающей специальное программное обеспечение, — так называемого Спецоператора связи

Обратите особое внимание на условия, в которых хранится закрытый ключ, достаточно ли надежно он защищен от посторонних глаз. Ведь если злоумышленник завладеет вашим закрытым ключом, он фактически получит возможность использовать вашу ЭЦП. Как вы понимаете, это может привести к весьма нежелательным последствиям.

## Не забудьте про Сертификат!

Следующий шаг — попросите, чтобы УЦ оформил вам Сертификат ключа подписи (СКП). Он нужен для того, чтобы налоговая инспекция смогла понять, от кого именно ей пришла отчетность (т. е. смогла бы проверить вашу подпись). В Сертификате ключа подписи обязательно должны быть указаны:

- информация о владельце, например, ФИО, должность, e-mail и т. п.;
- открытый ключ электронной цифровой подписи;
- информация о выдавшей ЭЦП организации — Удостоверяющем центре;
- области применения подписи, где документ с ЭЦП будет иметь юридическое значение (в вашем случае подпись применима при передаче отчетности в налоговую инспекцию).

Учтите, что владельцем СКП может являться только физическое (а не юридическое!) лицо, которое владеет закрытым ключом, позволяющим подписывать электронные документы. Сертификат передается вам в электронном виде. Возможно его оформление и на бумаге[3].

Также Удостоверяющий центр включит ваш СКП в реестр Сертификатов ключей подписи, размещенный на сайте УЦ. Получив отчетность от вашей организации, инспектор найдет в данном интернет-реестре ваш Сертификат и с помощью указанного в нем открытого ключа проверит, что ваша ЭЦП создана именно вашим закрытым ключом. Именно в этом и заключается принцип работы данной ключевой пары.

## Визируем отчетность

Однако мы заглянули немного вперед, не осветив вопрос визирования электронного документа с помощью ЭЦП. Тут надо действовать следующим образом. Сначала сформируйте в специальной программе отчетность для передачи в налоговую инспекцию. Затем вставьте флешку с закрытым ключом в компьютер. Программа с помощью определенной функции считает с данного носителя ваш закрытый ключ и произведет шифровку отчетности. В результате у вас образуется документ с электронной цифровой подписью. Теперь отчетность можно смело отправлять в ИФНС.

Конечно, это лишь общий алгоритм действий. Ведь процесс взаимодействия с Удостоверяющим центром имеет немало тонкостей и особенностей. Грамотно сформировать отчетность для передачи в ИНФС тоже не так-то просто. Подробнее об этом читайте в следующем номере «Актуальной бухгалтерии». АБ

> Обратите особое внимание на условия, в которых хранится ваш закрытый ключ

[3] ст. 6 Федерального закона от 10.01.2002 № 1-ФЗ

**Ю.Г. Маслов,**
коммерческий директор
компании «КРИПТО-ПРО»

Понятие «электронная цифровая подпись» уже давно не является новеллой с точки зрения юриспруденции. Для проверки отсутствия искажений в электронных документах ЭЦП используют в России еще с 90-х годов прошлого века. В основном данное средство применялось в банковской сфере для обеспечения взаимодействия банков с клиентами и для межбанковских расчетов по телекоммуникационным каналам связи.

В январе 2001 года вышел Закон «Об электронной цифровой подписи», который определил правовые условия равнозначности ЭЦП собственноручной подписи и замещения печати организации. С этого момента в России началось бурное развитие систем юридически значимого электронного документооборота, основанного на безбумажных технологиях.

Такие системы гарантируют, что электронные документы, подписанные ЭЦП, можно использовать в конфликтных ситуациях (спорах) при их разрешении в судебном порядке. Они будут признаны судом как полноценные документы, имеющие юридическую силу. Поэтому про такие системы и говорят, что в них реализован юридически значимый документооборот.

При построении подобной системы ее организатор должен привести свои правила использования ЭЦП в соответствие с нормами действующего законодательства РФ.

В настоящее время сложилась судебная практика по делам, в которых в качестве полноценных доказательств принимаются электронные документы, удостоверенные ЭЦП. Такая практика существует по уголовным, административным и гражданским делам.

При предъявлении электронных документов в качестве доказательства необходимо также предъявить и заключение экспертов, подтвердивших подлинность ЭЦП в документах. Это единственное существенное отличие от предъявления документов на бумажном носителе.

Экспертизу должен проводить тот Удостоверяющий центр, который изготовил соответствующие Сертификаты ключей подписи.