**Разъяснение порядка получения и использования электронной подписи, ответственность за нарушение правил создания (замены) и выдачи ключа простой электронной подписи и правил использования.**

В современном мире особую актуальность приобретает использование электронной подписи. Основными преимуществами использования электронной подписи является скорость, надежность, уход от традиционного бумажного документооборота, немаловажно, что обладатель электронной подписи может беспрепятственно получать государственные услуги.

Электронная подпись - это цифровой аналог собственноручной подписи, с помощью которого можно подписывать электронные документы. Такая подпись гарантирует, что документ исходит от конкретного лица.

Существуют разные виды электронной подписи, выделяют простые и усиленные электронные подписи.

**Простая электронная подпись** - наименее защищенный вид подписи. Простая подпись приравнивается к собственноручной, только если это предусмотрено нормативным правовым актом, нормативным актом Банка России или соглашением лиц, которые собираются обмениваться электронными документами, в том числе правилами платежных систем (ч. 2 ст. 6 Закона об электронной подписи).

**Простую электронную подпись** чаще всего используют граждане для подтверждения банковских операций и получения ряда госуслуг. Организации нередко используют ее во внутреннем электронном документообороте.

**Простую подпись** получить несложно. Как правило, это бесплатно и не занимает много времени. Например, вам могут предложить заполнить регистрационную форму на сайте, а затем ввести код, направленный в СМС-сообщении.

**Усиленные электронные подписи** подразделяются на квалифицированные и неквалифицированные. Их получают в результате криптографического преобразования информации с использованием ключа электронной подписи (ч. 1, п. 1 ч. 3, ч. 4 ст. 5 Закона об электронной подписи).

**Усиленная электронная подпись** используется, в частности:

- для сдачи отчетности в электронном виде (например, в налоговую, пенсионный фонд);

- подачи документов в суд;

- участия в электронных торгах;

- получения госуслуг;

- организации документооборота внутри организации, а также с ее контрагентами (например, для подписания договоров с ними).

В большинстве указанных случаев закон требует использовать усиленную квалифицированную подпись.

Чтобы получить **усиленную подпись**, нужно обратиться в удостоверяющий центр.

Удостоверяющие центры бывают аккредитованными и неаккредитованными (ст. ст. 13, 15 Закона об электронной подписи). Выдавать квалифицированные сертификаты имеют право только аккредитованные удостоверяющие центры. Также к удостоверяющим центрам относятся ФНС России, Федеральное казначейство (для государственных органов и органов местного самоуправления, а также организаций, определенных Правительством РФ), Банк России (для кредитных организаций, операторов платежных систем и некоторых других лиц).

**Перечень аккредитованных удостоверяющих центров** опубликован на сайте Минцифры России https://clck.ru/FStza. В нем указывается дата аккредитации. Необходимо обращать внимание на то, что дата такой аккредитации должна быть после 1 июля 2020 г. (п. 2 Письма Минцифры России от 10.08.2021 N ОП-П15-085-33604).

Прежде чем создать и выдать сертификат ключа проверки подписи, удостоверяющий центр идентифицирует заявителя (п. 1 ч. 1 ст. 13 Закона об электронной подписи):

В дальнейшем такой центр обеспечивает конфиденциальность ключей электронной подписи. При получении соответствующего обращения он может ее проверить (п. 9 ч. 1, п. 4 ч. 2 ст. 13 Закона об электронной подписи).

Как правило, на сайтах таких центров есть форма заявления и перечень требуемых документов. Чтобы заказать подпись, достаточно заполнить заявление и приложить к нему документы по списку. Когда электронная подпись будет готова, вам выдадут ключ электронной подписи, ключ проверки электронной подписи и сертификат ключа проверки электронной подписи.

**Ключ электронной подписи** - это уникальная последовательность символов, с помощью которой создается электронная подпись (п. 5 ст. 2 Закона об электронной подписи). Его также называют закрытым, потому что доступ к нему имеет только тот, кто подписывает документы с помощью электронной подписи. Важно хранить этот ключ в секрете.

Одновременно с этим ключом выдается **ключ проверки электронной подписи**. Он однозначно связан с ключом электронной подписи и нужен для того, чтобы получатель документа мог проверить подлинность электронной подписи (п. 6 ст. 2 Закона об электронной подписи). Этот ключ называют открытым, поскольку получатели файлов, подписанных электронной подписью, имеют доступ к нему.

За нарушение правил создания (замены) и выдачи ключа простой электронной подписи и правил использования ГИС ЕСИА предусмотрена административная ответственность. В частности, если орган либо организация, имеющие право создания (замены) и выдачи ключа простой электронной подписи, при использовании ГИС ЕСИА нарушили конфиденциальность такого ключа, штраф составит (ч. 1 ст. 13.33.1 КоАП РФ):

для должностных лиц - от 7 тыс. до 10 тыс. руб.;

для юрлиц - от 50 тыс. до 200 тыс. руб.

Управление правовой статистики

прокуратуры Челябинской области

Управл