произвольной форме о недостоверности сведений. Это можно сделать как при непосредственном посещении налоговой инспекции, так и по почте или через интернет.

3. Если на Ваше имя зарегистрировано юридическое лицо или ИП, следует незамедлительно внести в реестр ЕГРЮЛ или реестр ЕГРИП информацию о недостоверности данных о Вас, как о руководителе. Для этого в налоговую инспекцию следует направить заявление о недостоверности сведений о юридическом лице или ИП по форме № Р34001 (рекомендуем направить такое заявление непосредственно в инспекцию по месту регистрации юридического лица или ИП). Это можно сделать как при непосредственном посещении инспекции, так и по почте или через интернет.

4. Если Вы потеряли пароль доступа к закрытому ключу (PIN-код) или сам ключевой носитель, или он сломан, то необходимо приостановить бизнес-процессы электронного документооборота до перевыпуска электронной подписи.

5. Если действия посторонних лиц с Вашей электронной подписью причинили ущерб, от Вашего имени совершена незаконная сделка в электронной форме, подписаны значимые документы в электронной форме, то необходимо обратиться с заявлением в полицию или прокуратуру и зафиксировать факт такого события, приложив копии документов, выданных Удостоверяющим центром при получении электронной подписи (при наличии). Также можно обратиться в суд и аннулировать договор или признать документы недействительными.

Электронная подпись - ключ к Вашему имуществу, деньгам и репутации!

Удостоверяющий центр
ФНС России

www.nalog.gov.ru

МЕЖРАЙОННАЯ ИФНС РОССИИ
№4 ПО ТВЕРСКОЙ ОБЛАСТИ

ЗАЩИТИ СВОЮ ЭЛЕКТРОННУЮ ПОДПИСЬ!

Вы получили квалифицированный сертификат электронной подписи? Будьте внимательны и осторожны!

Электронная подпись – надежный инструмент для работы, но при неосторожном обращении она открывает возможности для злоумышленников.

Получение квалифицированного сертификата электронной подписи по значимости даже важнее получения паспорта! Когда Вы используете паспорт для совершения юридически значимых действий, Вас идентифицируют, сравнивая Ваше лицо с фотографией в паспорте. Электронная подпись (авторство электронного документа) обычно проверяется дистанционно, то есть предполагается, что никто кроме Вас не может поставить Вашу электронную подпись на электронный документ.

Усиленная квалифицированная электронная подпись (УКЭП) признается равнозначной собственноручной «живой» подписи. Поэтому, если кто-то использует Вашу электронную подпись вместо Вас, юридически это расценят как Ваши действия. Использование чужой ЭЦП по значимости сравнимо с использованием чужого паспорта.

ЧТО ПРОИЗОЙДЕТ, ЕСЛИ ВАША ЭЛЕКТРОННАЯ ПОДПИСЬ ПОПАДЕТ В РУКИ ЗЛОУМЫШЛЕННИКОВ?

- На Ваше имя могут оформить микрокредиты;
- Ваш автомобиль могут продать без Вашего ведома;
- Вас могут сделать номинальным руководителем фирмы-однодневки;
- Если Вы владелец организации, ее могут переоформить на другое лицо, вывести деньги компании на другой счет, незаконно возместить НДС;
- Вместо Вас могут подписать любые документы;
- Вас могут привлечь к ответственности за нарушение законодательства Российской Федерации в области электронной подписи.

МЕРЫ ПРЕДОСТОРОЖНОСТИ

1. **Не передавайте ключевой носитель третьим лицам**, даже тем, кому Вы доверяете!
Если подписывать документы с помощью электронной подписи должен Ваш сотрудник, чтобы освободить себя, как руководителя, от рутинного подписания бумаг, обеспечьте его собственным ключевым носителем с закрытым ключом электронной подписи и сертификатом на его имя, а также выдайте доверенность на подписание документов.

2. **Обеспечьте надежное хранение носителя с электронной подписью (ключевой носитель)**, которое исключает доступ к нему посторонних лиц (например, храните его в сейфе). Не оставляйте ключевой носитель подключенным к компьютеру без присмотра.

3. **При потере или краже ключевого носителя** незамедлительно обратитесь с заявлением на отзыв сертификата в Удостоверяющий центр, который его выдал.

4. **Замените «заводской» пароль (PIN-код)** ключевого носителя на свой собственный при получении электронной подписи, как Вы это делаете с банковской картой. Обеспечьте надежное хранение пароля, исключите доступ к паролю любых лиц.

5. **Внимательно читайте договор и другие документы** в рамках сделки с обслуживающей организацией на предоставление услуг. Обращайте внимание в тексте соглашения на словосочетание «электронная подпись», на условия выдачи сертификата, как он хранится и аннулируется, кто обеспечивает его сохранность, а также для чего требуется выпуск сертификата и можно ли от него отказаться.

6. **Не соглашайтесь на предложения выдать электронную подпись без личной явки при первичном ее получении.** Во-первых, это незаконно. Во-вторых, закрытый ключ могут скопировать и использовать его в дальнейшем без Вашего ведома для формирования электронной подписи на электронном документе.

7. **Регулярно проверяйте информацию о выпуске на Ваше имя сертификатов электронных подписей** на Едином портале государственных и муниципальных услуг (Госуслуги). Информация о выпущенной на Ваше имя электронной подписи, ее серийном номере и сроке действия, Удостоверяющем центре, который ее выпустил, размещена на сайте «Госуслуги» в Вашем личном кабинете в разделе "Настройки и безопасность" => "Электронная подпись".

ЧТО ДЕЛАТЬ, ЕСЛИ ПРОИЗОШЛО МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ ПОДПИСИ, ВЫДАННОЙ НА ВАШЕ ИМЯ?

1. Незамедлительно обратитесь в Удостоверяющий центр, который выдал этот сертификат электронной подписи на Ваше имя, и напишите заявление на его аннулирование! Это не позволит злоумышленникам в дальнейшем совершать мошеннические действия с использованием этого сертификата.

2. Если злоумышленники за Вас сдали отчетность, как можно скорее подайте в налоговую инспекцию заявление в