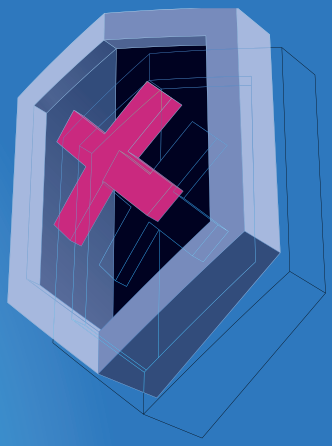
ИНТЕРНЕТ-ВЕРСИЯ



ЭЛЕКТРОННАЯ ПОДПИСЬ
ПРОСТО О СЛОЖНОМ

ВВЕДЕНИЕ

Неотъемлемой частью юридически значимого электронного документооборота является электронная подпись[1]. Безопасность электронной подписи зависит от:

- свойств закрытого ключа[2];
- функциональных возможностей ключевого носителя[3];
- ответственного хранения.

Рекомендуется использовать защищенные носители ключевой информации (далее — ключевые носители), которые, в свою очередь, делятся на пассивные (с защитой данных только по PIN-коду) и активные (со встроенными на аппаратном уровне функциями средства криптографической защиты информации, далее — СКЗИ[4]).

Соблюдение настоящих методологических рекомендаций по использованию ключевых носителей поможет защитить участников электронного документооборота от рисков:

- получения несанкционированного доступа третьих лиц к закрытому ключу для создания его копии;
- подписания электронных документов третьими лицами от имени владельца электронной подписи;
- хищения ключевого носителя или его уничтожение.

СВОЙСТВА ЗАКРЫТОГО КЛЮЧА

Экспортируемые и неэкспортируемые закрытые ключи

Свойство экспортируемости или неэкспортируемости закрытого ключа присваивается на этапе формирования закрытого ключа и записи его на ключевой носитель. Указанное свойство может быть реализовано в средствах электронной подписи и управляться его настройками, которые следует установить до формирования закрытого ключа.

Для экспортируемых закрытых ключей доступно их копирование, что несет риски нарушения конфиденциальности закрытого ключа.

Для копирования закрытого ключа нарушителю потребуется получить физический доступ к ключевому носителю и узнать пароль (PIN-код).

Возможность копирования закрытого ключа создаёт риск возникновения неучтенных копий, усложняет контроль за его хранением, использованием и уничтожением. Также указанное усложняет определение возможного нарушителя, особенно когда нарушитель начнет использовать копию не сразу.

Неэкспортируемые закрытые ключи обладают большей защищенностью, так как записанный на ключевой носитель закрытый ключ не подлежит копированию при помощи стандартных СКЗИ. Получение доступа к такому ключу требует применения специальных средств и техники.

1 Электронная подпись — это аналог собственноручной подписи для подписания электронных документов.

2 Закрытый (секретный) ключ электронной подписи — это уникальный набор символов (байт), сформированный средством электронной подписи. Используется для формирования самой электронной подписи на электронном документе и хранится в зашифрованном виде на ключевом носителе. Доступ к закрытому ключу защищен паролем (PIN-кодом) и его нужно хранить в секрете.

3 Ключевой носитель — это устройство для хранения закрытого ключа. Ключевой носитель внешне напоминает «флешку» для компьютера, но отличается по своим свойствам: память у него защищена паролем (PIN-кодом). Может иметь встроенное средство криптографической защиты информации. В этом случае он является программно-аппаратным ключевым носителем и позволяет максимально безопасно формировать электронную подпись на электронном документе.

4 Средство криптографической защиты информации (СКЗИ) — термин используется в соответствии с частью 2 раздела I Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ РФ от 09.02.2005 № 66 (Зарегистрировано в Минюсте России 03.03.2005 N 6382).

Извлекаемые и неизвлекаемые закрытые ключи

Свойство неизвлекаемости закрытого ключа достигается способом его создания[5] и хранения[6], и напрямую зависит от вида ключевого носителя. Для обеспечения свойства неизвлекаемости закрытого ключа используются только активные ключевые носители, содержащие в себе аппаратно реализованные функции СКЗИ, при использовании которых создается и используется неизвлекаемый закрытый ключ.

Для некоторых ключевых носителей существует возможность записи закрытого ключа на активные ключевые носители сторонними СКЗИ (установленными локально на компьютерное устройство[7] или непосредственно в информационной системе удостоверяющего центра) и, в таком случае, такой носитель применяется как пассивный ключевой носитель, который может обеспечить только свойство неэкспортируемости закрытого ключа.

К извлекаемым закрытым ключам относятся все виды закрытых ключей, за исключением неизвлекаемых, включая экспортируемые и неэкспортируемые.

ВИДЫ КЛЮЧЕВЫХ НОСИТЕЛЕЙ

Пассивный ключевой носитель

Виды реализации: носитель с USB интерфейсом, носитель с бесконтактным интерфейсом (NFC интерфейс), смарт-карта.

Для доступа к защищенному содержимому данного ключевого носителя необходимо ввести пароль (PIN-код). Закрытый ключ хранится в ключевом контейнере[8] на ключевом носителе. Пароль (PIN-код), которым защищён от доступа закрытый ключ на таком носителе, при получении следует изменить, обеспечить его надежное хранение и исключить доступ к паролю любых лиц.

При подписании электронного документа с использованием пассивного носителя и средства электронной подписи вычисляется уникальный набор символов — хэш документа[9], однозначно связанных с содержанием электронного документа. Далее закрытый ключ копируется в память компьютерного устройства, где с его помощью средство электронной подписи выполняет криптографические операции[10] формирования электронной подписи — подписание электронного документа. По завершении процедуры подписания закрытый ключ удаляется из памяти компьютерного устройства. Процедура подписания электронного документа происходит незаметно для пользователя в течение нескольких секунд.

На ключевом носителе установлено ограничение попыток неправильного ввода пароля (PIN-кода) и при превышении такого лимита ключевой носитель блокируется. Несмотря на это пассивный ключевой носитель обладает средним уровнем защищенности от атак злоумышленников — в момент подписания документа образуется короткий промежуток времени, когда закрытый ключ находится в памяти компьютерного устройства, где существует возможность его перехвата злоумышленником с высоким уровнем технических знаний и/или с использованием специальных технических средств. Для исключения такого вида атак существует активный ключевой носитель.

Активный ключевой носитель (криптографический ключевой носитель)

Виды реализации: носитель с USB интерфейсом, носитель с бесконтактным интерфейсом (NFC интерфейс), смарт-карта.

Активный ключевой носитель содержит в себе функции СКЗИ. Закрытый ключ на таком ключевом носителе хранится в защищенном ключевом контейнере и в специальном внутреннем формате.

У такого носителя существует ряд технических преимуществ перед пассивным ключевым носителем:

5 Генерация закрытого ключа — создание закрытого ключа с использованием средства электронной подписи.

6 Хранение и использование закрытого ключа происходит только в специальной и защищенной микропроцессором области памяти ключевого носителя, доступ к которой осуществляется с помощью нередактируемого перечня команд микропроцессора, среди которых отсутствуют команды, позволяющие получить доступ к содержанию закрытого ключа

7 Компьютерное устройство — мобильный телефон, смартфон, компьютер, планшет.

8 Ключевой контейнер — способ хранения закрытого ключа на ключевом носителе. Доступ к ключевому контейнеру защищается установкой пароля. Защита ключевого контейнера индивидуальна для каждого типа ключевого носителя.

9 Хэш документа (хэш значение документа) — уникальный набор символов, полученный в результате вычисления однонаправленной функции, который неразрывно связан с содержанием электронного документа: в случае изменения электронного документа, даже незначительного, например, добавления в текст пробела, хэш значение электронного документа изменится.

10 Криптографические операции формирования электронной подписи — преобразование ранее вычисленного хеш-значения электронного документа таким образом, что его обратное преобразование возможно только с помощью сертификата ключа проверки электронной подписи.

- создание закрытого ключа происходит на самом носителе с использованием аппаратных криптографических функций ключевого носителя;
- при подписании электронного документа закрытый ключ не копируется в память или реестр компьютерного устройства — подписание электронного документа происходит на самом ключевом носителе;
- закрытый ключ ни в какой момент времени не покидает ключевой носитель.

Вычисление значения хэш документа может происходить на компьютерном устройстве, а итоговое формирование электронной подписи только на самом активном ключевом носителе.

Компрометация закрытого ключа на таком носителе возможна только в случае его хищения вместе с паролем (PIN-кодом).

Активный ключевой носитель (криптографический ключевой носитель) обладает высоким уровнем защищенности от атак злоумышленников. Риск атаки «подмена хэша»[11] злоумышленником присутствует, но такие случаи крайне редки.

МЕРЫ ПРЕДОСТОРОЖНОСТИ ПРИ РАБОТЕ С КЛЮЧЕВЫМИ НОСИТЕЛЯМИ

Технические меры предосторожности

При выборе вида ключевого носителя для хранения закрытого ключа электронной подписи следует учитывать, что электронная подпись считается равнозначной собственноручной подписи в случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». Рекомендуется использовать ключевые носители с наивысшей степенью защиты закрытого ключа.

Рекомендуется сменить пароль доступа к ключевому носителю (PIN-код), установленный его изготовителем, на уникальный — известный только владельцу электронной подписи. Рекомендуемая длина пароля — не менее 6 символов с использованием специальных символов, прописных и строчных латинских букв. Рекомендуется периодическая смена пароля.

Не рекомендуется при выборе пароля основываться на типовых шаблонах и идущих подряд на клавиатуре или алфавите символов (qwerty, abcde, 12345 и другие) на каком-либо идентификаторе, паспортных данных, кличек питомцев и подобных ассоциаций.

Не рекомендуется активировать функцию «запомнить пароль» в средствах электронной подписи и настройках программного обеспечения, которое необходимо для использования ключевого носителя.

ОРГАНИЗАЦИОННЫЕ МЕРЫ ПРЕДОСТОРОЖНОСТИ

Не рекомендуется в рамках организации процедур безопасной работы с ключевым носителем:

- передавать ключевой носитель третьим лицам
- записывать пароль доступа к ключевому носителю (PIN-код) на бумаге или непосредственно на ключевом носителе, запоминать пароли в реестровой памяти систем электронных устройств и хранить парольную информацию в общедоступных местах
- оставлять ключевой носитель без присмотра в доступных или общественных местах
- оставлять без присмотра ключевой носитель в компьютерном устройстве, на котором осуществляется подписание электронных документов (usb-порты в системном блоке компьютера, ноутбука, планшета или других электронных устройствах).

Рекомендуется в рамках организации процедур безопасной работы с ключевым носителем:

- при необходимости, обеспечивать сотрудников организации, не имеющих права действовать без доверенности, их персональными закрытыми ключами и сертификатами электронной подписи, с наделением их правом подписи распорядительными документами организации путем оформления доверенности
- хранить ключевой носитель в недоступном для третьих лиц месте
- при потере или краже ключевого носителя незамедлительно обратиться в удостоверяющий центр, выпустивший сертификат электронной подписи, и прекратить действие такого сертификата электронной подписи, и, не дожидаясь завершения процедуры аннулирования, уведомить контрагентов о том, что утраченный сертификат с соответствующим серийным номером, считается уже недействительным.

11 Атака «подмена хэша» — тип атаки злоумышленником, когда последний вычисляет хэш-значение поддельного документа и перехватив в памяти компьютера хэш-значение подписываемого документа, заменяет его своим .

ПОЛУЧЕНИЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ (КВАЛИФИЦИРОВАННЫЙ СЕРТИФИКАТ)

КТО МОЖЕТ ОБРАТИТЬСЯ ЗА ПОЛУЧЕНИЕМ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА В УДОСТОВЕРЯЮЩИЙ ЦЕНТР ФНС РОССИИ?

ЮРИДИЧЕСКОЕ ЛИЦО

(ЛИЦО, ИМЕЮЩЕЕ ПРАВО ДЕЙСТВОВАТЬ ОТ ИМЕНИ ЮРИДИЧЕСКОГО ЛИЦА БЕЗ ДОВЕРЕННОСТИ)

ИНДИВИДУАЛЬНЫЙ ПРЕДПРИНИМАТЕЛЬ

НОТАРИУС

КУДА В ЯРОСЛАВСКОЙ ОБЛАСТИ МОЖНО ОБРАТИТЬСЯ ЗА ПОЛУЧЕНИЕМ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА?

точки выдачи КЭП

Межрайонная ИФНС России № 5 по Ярославской области (код НО 7604):
150000, г. Ярославль, ул. Свободы, д. 46, (4852) 30-25-36;

Межрайонная ИФНС России № 9 по Ярославской области (код НО 7606):
150040, г. Ярославль, проспект Октября, д. 56, (4852) 73-25-90;

Межрайонная ИФНС России №3 по Ярославской области (код НО 7610):
152901, г. Рыбинск, ул. Крестовая, д. 54, (4855) 21-49-04;
152615, г. Углич, ул. Ярославская, д. 5а, (48532) 5-02-10;

Межрайонная ИФНС России №7 по Ярославской области (код НО 7627):
150006, г. Ярославль, ул. Корабельная, д. 1, стр. 9,(4852) 46-43-42;
152025, г. Переславль-Залесский, ул. 50 лет Комсомола, д.16А,(48535) 3-26-17;
152155, г. Ростов, ул. Спартаковская, д. 142, (48536) 7-45-87;

УФНС России по Ярославской области (код НО 7600):
150003, г.Ярославль, ул. Кооперативная, д. 11, (4852) 59-67-10

ЧТО НЕОБХОДИМО ДЛЯ ПОЛУЧЕНИЯ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ ФНС РОССИИ?

- ✓ Основной документ, удостоверяющий личность
- ✓ СНИЛС (номер страхового свидетельства государственного пенсионного страхования) заявителя
- ✓ Документ, подтверждающий право заявителя действовать от имени юридического лица без доверенности либо подтверждающий право заявителя действовать от имени госоргана или органа местного самоуправления
- ✓ USB-НОСИТЕЛЬ КЛЮЧЕВОЙ ИНФОРМАЦИИ (токен) для записи квалифицированного сертификата и ключа электронной подписи, сертифицированный ФСТЭК России или ФСБ России
- ✓ Сертификат соответствия на ключевой носитель, выданный ФСБ России или ФСТЭК России, или его скан-копия
- ✓ В случае использования ключевого носителя с встроенным СКЗИ – формуляр на СКЗИ

ГДЕ ИСПОЛЬЗУЕМ КВАЛИФИЦИРОВАННЫЙ СЕРТИФИКАТ?

- Для юридически значимого электронного документооборота
- На всех электронных площадках и в сервисах
- При предоставлении налоговых деклараций (расчетов):
  - Через операторов электронного документооборота
  - Через сервис «Представление налоговой и бухгалтерской отчетности в электронной форме» на сайте www.nalog.gov.ru

ФЕДЕРАЛЬНАЯ НАЛОГОВАЯ СЛУЖБА

ТЕЛЕФОН «ГОРЯЧЕЙ ЛИНИИ»
8 (800) 222-22-22

Документы, необходимые для получения квалифицированного сертификата электронной подписи:

Физическому лицу (Гражданину РФ):
→ Российский паспорт (оригинал или заверенная копия);
→ Заявление на выдачу сертификата (только оригинал);
→ Страховое свидетельство Пенсионного Фонда (СНИЛС) (оригинал или заверенная копия);
→ Свидетельство ИНН.

Юридическому лицу (в качестве владельца указана организация и генеральный директор организации):
→ Российский паспорт генерального директора (оригинал или заверенная копия);
→ Заявление на выдачу сертификата генерального директора (только оригинал);
→ Страховое свидетельство Пенсионного Фонда (СНИЛС) генерального директора (оригинал или заверенная копия);
→ Свидетельство ИНН генерального директора.

Юридическому лицу (в качестве владельца указана организация и уполномоченное лицо)*:
→ Российский паспорт уполномоченного лица (оригинал или заверенная копия);
→ Заявление на выдачу сертификата уполномоченного лица (только оригинал);
→ Страховое свидетельство Пенсионного Фонда (СНИЛС) уполномоченного лица (оригинал или заверенная копия);
→ Свидетельство ИНН уполномоченного лица;
→ Доверенность на право подписи (оригинал или заверенная копия);
→ Доверенность на получение сертификата (оригинал или заверенная копия).

---

* Применение электронной подписи регулируется федеральным законом "Об электронной подписи" от 06.04.2011 N 63-ФЗ

Способы идентификации личности

Удостоверяющий центр обязан провести идентификацию вашей личности – в вашем присутствии либо дистанционно. Дистанционно – при наличии у вас действующей квалифицированной электронной подписи, биометрического паспорта гражданина, подтвержденной учетной записи на Едином портале государственных и муниципальных услуг (Госуслуги) или учетной записи в Единой биометрической системе России (ЕБС).

Как получить и использовать квалифицированную электронную подпись?

Для получения сертификата электронной подписи вам необходимо обратиться в удостоверяющий центр – специализированную организацию, аккредитованную Министерством цифрового развития, связи и массовых коммуникаций, заполнить заявление и предоставить **необходимые документы.**

Проведя **идентификацию** вашей личности, удостоверяющий центр создаст **ключевую пару,** запишет закрытый ключ на **ключевой носитель,** и выдаст вам сертификат ключа проверки электронной подписи, который подтверждает, что вы являетесь владельцем сертификата и электронной подписи.

Если вы используете программно-аппаратный ключевой носитель, вы можете самостоятельно создать ключевую пару, и предоставить ее в удостоверяющий центр и получить в нем ваш сертификат ключа проверки электронной подписи.

Для подписания электронных документов электронной подписью необходимо использовать специализированную программу – **средство электронной подписи.**

ИНТЕРНЕТ-ВЕРСИЯ

→ **Электронная подпись** – это аналог собственноручной подписи для подписания электронных документов.

→ **Ключевая пара** – это набор из открытого и закрытого ключей электронной подписи, однозначно привязанных к друг другу.

→ **Открытый ключ** (ключ проверки электронной подписи) это уникальный набор символов (байт), сформированный средством электронной подписи и однозначно привязанный к закрытому (секретному) ключу. Открытый ключ необходим для того, чтобы любой желающий мог проверить электронную подпись на электронном документе. Он передается получателю электронного документа в составе файла электронной подписи и может быть известен всем.

→ **Закрытый** (секретный) **ключ** электронной подписи – это уникальный набор символов (байт), сформированный средством электронной подписи. Используется для формирования самой электронной подписи на электронном документе и хранится в зашифрованном виде на ключевом носителе. Доступ к закрытому ключу защищен PIN-кодом и его нужно хранить в секрете.

→ **Сертификат ключа проверки электронной подписи** (сертификат электронной подписи, квалифицированный сертификат электронной подписи) – это электронный и бумажный документ, который подтверждает связь электронной подписи с ее владельцем (человеком или организацией). Сертификат содержит сведения о его владельце, открытый ключ, информацию о сроке действия сертификата, информацию о выдавшем электронную подпись удостоверяющем центре, серийный номер сертификата и иные сведения.

→ **Ключевой носитель** – это устройство для хранения закрытого ключа. Ключевой носитель внешне напоминает "флешку" для компьютера, но отличается по своим свойствам: память у него защищена паролем (PIN-кодом). Может иметь встроенное средство электронной подписи. В этом случае он является программно-аппаратным ключевым носителем и позволяет максимально безопасно формировать электронную подпись на электронном документе.

→ **Средство электронной подписи** – это программно-аппаратное или только программное средство, предназначенное для создания ключевой пары, формирования и проверки электронной подписи на электронном документе. Его еще называют "криптопровайдером" или СКЗИ (средством криптографической защиты информации). Устанавливается на компьютерное устройство (мобильный телефон, смартфон, компьютер, планшет) или на ключевой носитель.

Формирование электронной подписи

При подписании электронного документа формируется уникальный набор символов (хэш-код), однозначно привязанный к содержанию электронного документа и созданный средством электронной подписи путем обработки этого электронного документа с помощью криптографического преобразования (хэш-функции). Такой уникальный набор символов неразрывно связан с электронным документом: если в текст добавят незаметно для вас, например, пробел, электронный документ уже не будет соответствовать этому уникальному набору символов.

Средство электронной подписи шифрует уникальный набор символов (хэш-код) используя ваш закрытый ключ. Зашифрованный уникальный набор символов и есть электронная подпись на электронном документе. Она может быть как встроенной в электронный документ, так и отсоединенной от него и преобразованной в отдельный файл.

Направляя адресату подписанный электронный документ, необходимо направлять также ваш сертификат ключа проверки электронной подписи, который содержит открытый ключ, чтобы адресат (получатель) мог проверить авторство и неизменность документа.

Проверка электронной подписи

Для проверки электронной подписи получатель документа использует средство электронной подписи, которое:
→ расшифровывает уникальный набор символов (хэш-код), содержащийся в электронной подписи электронного документа;
→ формирует уникальный набор символов путем обработки проверяемого электронного документа с помощью различных криптографических алгоритмов;
→ сравнивает указанные выше уникальные наборы символов (хэш-коды). Их соответствие друг другу является подтверждением того, что в проверяемый электронный документ не вносились изменения после его подписания электронной подписью;
→ проверяет соответствие электронной подписи в электронном документе и направленном вместе с ним сертификате ключа проверки электронной подписи, подтверждая авторство электронного документа;
→ Если хотя бы одна из проверок завершится с ошибкой, средство электронной подписи сообщит, что электронная подпись на электронном документе недействительна и авторство электронного документа не подтверждено.

ФЕДЕРАЛЬНАЯ НАЛОГОВАЯ СЛУЖБА

Вы получили квалифицированный сертификат электронной подписи?

Будьте внимательны и осторожны!

Электронная подпись – это аналог собственноручной подписи, ключ к вашему имуществу, деньгам и репутации!

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. Поэтому если кто-то использует вашу электронную подпись вместо вас, юридически это расценят как ваши действия.

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:

→ **Не передавайте ключевой носитель третьим лицам, даже тем, кому вы доверяете!**
Если вы руководитель организации и ваш сотрудник должен подписывать документы с помощью электронной подписи, обеспечьте его собственным ключевым носителем с закрытым ключом электронной подписи и сертификатом на его имя, а также выдайте доверенность на подписание документов.

→ **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.

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

→ **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.

→ **Внимательно читайте документы при оформлении различных сервисов в организациях, оказывающих услуги для бизнеса и банках.**
Если вы видите в тексте соглашения словосочетание "электронная подпись", уделите этому разделу особое внимание. Возможно, на вас оформят сертификат электронной подписи, закрытый ключ от которой будет храниться в недоступном для вас месте. Если к этому ключу будет доступ у третьих лиц, не исключено, что за вас и без вашего ведома могут подписать какие-либо документы в электронной форме.

→ **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 так же, как в предыдущем сценарии, использовать его без вашего ведома для формирования электронной подписи на электронном документе.

→ **Регулярно проверяйте информацию о выпуске на ваше имя сертификатов электронных подписей на Едином портале государственных и муниципальных услуг (Госуслуги).**
Информация о выпущенных на ваше имя электронных подписях и удостоверяющих центрах, которые их выпустили, размещены 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?

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.

→ **Если злоумышленники за вас сдали отчетность, как можно скорее подайте в налоговую инспекцию заявление в произвольной форме о недостоверности сведений.**
Это можно сделать как при непосредственном посещении налоговой инспекции, так и по почте или через интернет.

→ **Если на ваше имя зарегистрировано юридическое лицо или ИП, следует незамедлительно проинформировать налоговый орган о наличии такого факта.**
В случае непричастности вы можете внести в ЕГРЮЛ сведения о недостоверности можно представить в регистрирующий орган заявление, по форме № Р34002, либо направить в предусмотренном порядке заявление по форме № Р34001 (рекомендуем направлять такие заявления непосредственно в инспекцию по месту регистрации юридического лица). В случае несогласия с внесением сведений в ЕГРИП можно подать в налоговый орган жалобу в порядке, установленным Федеральным законом от 08.08.2001 № 129-ФЗ. Это можно сделать как при непосредственном посещении инспекции, так и по почте или через интернет.

→ **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.

→ **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. Возьмите с собой копии документов, выданных удостоверяющим центром при получении электронной подписи (при наличии). Также вы можете обратиться в суд и аннулировать договор или признать документы недействительными.

ФЕДЕРАЛЬНАЯ НАЛОГОВАЯ СЛУЖБА

МАТЕРИАЛ ПОДГОТОВЛЕН ПРИ УЧАСТИИ КОМПАНИЙ:

ЭЛЕКТРОННЫЕ ДОКУМЕНТЫ ЭФФЕКТИВНАЯ ЭКОНОМИКА

1С

СКБ Контур

МАГНИТ

ЭВОТОР

Компания Актив

Электронная подпись «в придачу»

Организации, которые оказывают предпринимателям различные услуги, будь то регистрация контрольно-кассовой техники или помощь в оформлении расчетного счета, в борьбе за клиента стараются сделать обслуживание максимально комфортным. При этом в погоне за простотой и удобством часто упускают важные детали, например, могут не обратить внимание клиента на то, что на его имя выпускают сертификат электронной подписи.

В таких случаях заявление на выпуск сертификата присутствует в общей массе документов, которые подписываются при заключении договора на получение услуг. Но так как документов много, формулировки – нечеткие, а представитель обслуживающей организации не дает никаких дополнительных устных пояснений, клиент не обращает внимание на то, что получает дополнительную услугу – выпуск сертификата.

Закрытый ключ электронной подписи могут выдать на носителе с пакетом документов об оказании услуги, а могут хранить его в «облачном» хранилище организации. Сертификат могут аннулировать сразу после оказания услуги, а могут продолжить использовать его для совершения юридически значимых действий от вашего имени. Все зависит от добросовестности организации.

Как избежать получения сертификата электронной подписи «в придачу»:

→ прочитайте внимательно договор и другие документы, обратите внимание, есть ли там слова «электронная подпись»;
→ обратите внимание на условия выдачи сертификата, как он хранится и аннулируется, кто обеспечивает его сохранность;
→ спросите у представителя обслуживающей организации: для чего требуется выпуск сертификата и можно ли от него отказаться.

Если вам стало известно о выдаче сертификата электронной подписи на ваше имя без вашего ведома или о факте компрометации, то НЕМЕДЛЕННО аннулируйте его, обратившись в удостоверяющий центр, в котором выпущен этот сертификат электронной подписи.

ИНТЕРНЕТ-ВЕРСИЯ

Проверить, не выпущен ли на ваше имя сертификат электронной подписи, можно в личном кабинете на Едином портале государственных и муниципальных услуг https://lk.gosuslugi.ru/settings/signature