УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ
НАЛОГОВОЙ СЛУЖБЫ ПО ТОМСКОЙ ОБЛАСТИ

Безопасность использования электронной подписи

Начальник отдела информационной безопасности
УФНС России по Томской области
Миклашевич Андрей Александрович

Безопасность использования электронной подписи

1. Что защищаем
2. От чего защищаем
3. Как защищаем

Что защищаем

Основной документ, регулирующий использование электронной подписи - Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи» (далее Закон).

Говорить «**ЭЦП**» – это не очень правильно!
Правильно говорить «**ЭП**» – электронная подпись!

Что защищаем

Статья 2. Основные понятия, используемые в Законе

электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

Далее по электронной подписью понимаем квалифицированную усиленную электронную подпись.

Подписываемая информация – файл Подписанный_документ.pdf

Электронная подпись – файл Подписанный_документ.p7s
Или
Электронная подпись – файл Подписанный_документ.sig

Что защищаем

Статья 2. Основные понятия, используемые в Законе

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

Ключ электронной подписи – это то, что в точках выдачи УЦ ФНС России записывается на токен!

Что защищаем

Статья 2. Основные понятия, используемые в Законе.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Файл с расширением CER.
Например - КлючПроверки.cer

Что защищаем

Статья 2. Основные понятия, используемые в Законе.

квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган), ***и являющийся в связи с этим официальным документом;***

Файл с расширением pdf
Например - СертификатКлючаПроверки.pdf

Что защищаем

Статья 2. Основные понятия, используемые в Законе.

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

Для квалифицированной электронной подписи используются **только сертифицированные ФСБ России** средства электронной подписи.
КриптоПро CSP
КриптоАРМ ГОСТ и т.п.

Что защищаем

Что из вышеперечисленного подлежит защите?

Информация, которая подписана ЭП.
Подписываемая информация – файл Подписанный_документ.pdf

Единственный способ её защиты – шифрование.

Средства электронной подписи – их надо защищать исходя из требований производителя и требований кибербезопасности.

Ключ электронной подписи (носитель ключа электронной подписи). Важнейший объект защиты.

От чего защищаем

Статья 6 Закона. Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью

1. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, **равнозначным документу на бумажном носителе, подписанному собственноручной подписью**, и может применяться в **любых правоотношениях** в соответствии с законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

От чего защищаем

Статья 10 Закона. Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей

1. При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

1) **обеспечивать конфиденциальность ключей электронных подписей**, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

Владелец сертификата ключа электронной подписи несет юридическую ответственность за все действия, совершенные с использованием его электронной подписи.

От чего защищаем

От чего (кого) защищать ключ электронной подписи:

1. От потери носителя, содержащего ключ электронной подписи.

2. От попадания носителя, содержащего ключ электронной подписи, в ненадежные руки.

3. От кибератаки.

Как защищаем

Перечень требований по безопасности применения электронной подписи установлен следующими документами:

Приказ ФАПСИ от 13.06.2001 №152;
Приказ ФСБ от 09.02.2005 №66;
Приказ ФСБ России от 27.12.2011 №796;
Эксплуатационной документации к средствам электронной подписи.

Далее представляю некую идеальную картину по защите ЭП.

Как защищаем

От потери носителя, содержащего ключ электронной подписи.

Владельцу подписи:

1. Быть внимательным и аккуратным, не забывать токен где-либо.
2. На работе хранить токен в сейфе, доступ к которому ограничен.
3. Принять все возможные меры по защите токена от кражи (физическая защита).
4. Подписывать все документы самостоятельно и никому не передавать токен.

Как защищаем

Если начали терзать смутные сомнения, немедленно обратиться в УЦ, выдавший ключ электронной подписи.

Статья 10 Закона.
При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

2) уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о **нарушении конфиденциальности ключа электронной подписи** в течение не более чем **одного рабочего дня** со дня получения информации о таком нарушении;

3) не использовать ключ электронной подписи при наличии оснований полагать, что **конфиденциальность данного ключа нарушена**;

Как защищаем

От попадания носителя, содержащего ключ электронной подписи, в ненадежные руки.

Не всегда владелец подписи может подписывать все документы самостоятельно.

Чего делать не нужно:

1. Отдать токен кому-либо, пусть он подписывает.
2. Делать копию ключа электронной подписи на другой токен(ы).
3. Делать копию ключа электронной подписи на флешку.
4. Экспортировать ключ электронной подписи в реестр Windows.

Лучшее решение:

Сделать машиночитаемую доверенность.

Доверенность

Физическое лицо (наемный работник) не наделено полномочиями, но ему необходимо действовать от имени юридического лица (индивидуального предпринимателя).

От имени юридического лица (ИП) действует представитель (Физическое лицо, другое юридическое лицо или ИП).

Пункт 2 части 1 Статьи 17.2 Закона.
Пункт 2 Статьи 17.3 Закона.
Статья 17.5 Закона.

Положения указанных статей вступили в силу с 01.09.2024 года!

Доверенности.

Юридическое лицо (ИП) самостоятельно предоставляет НБО в ФНС России.

ФНС России

Доверенности.

Два случая:

1. Лицо, уполномоченное действовать от имени ЮЛ без доверенности (ИП) наделяет сотрудника какими-либо полномочиями, выдавая доверенность.
2. Юридическое лицо (ИП) через уполномоченную организацию предоставляет НБО в ФНС России.

ФНС России

Доверенности.

Два случая:

1. Лицо, уполномоченное действовать от имени ЮЛ без доверенности (ИП), наделяет сотрудника какими-либо полномочиями, выдавая нотариальную доверенность.

2. ЮЛ (ИП) через уполномоченную организацию предоставляет НБО в ФНС России, выдавая нотариальную доверенность.

ФНС России

Доверенности.

Очень желательно донести до работника, который получил ключ электронной подписи физического лица, что требования по безопасности использования электронной подписи также распространяются и на него.

Доверенности.

Изготовить машиночитаемую доверенность можно, в том числе, на сайте ФНС России по ссылке https://m4d.nalog.gov.ru/emchd/create.

Приказ ФНС России от 19.09.2023 №ЕД-7-26/648@ "Об утверждении формата доверенности, подтверждающей полномочия уполномоченного представителя налогоплательщика (плательщика сбора, плательщика страховых взносов, налогового агента) в отношениях, регулируемых законодательством о налогах и сборах, в электронной форме и порядка ее направления по телекоммуникационным каналам связи«

ВАЖНО! Доверенность должна быть направлена в налоговый орган и принята налоговым органом до начала сдачи налоговой отчетности.

Как защищаем

От кибератаки:

1. Не оставлять токен подключенным к USB порту компьютера. Подключать токен только когда он нужен, и отключать, когда перестал быть нужным.

2. Не сохранять ПИН код токена в памяти компьютера.

3. Не подключать компьютер, на котором установлены средства электронной подписи и используется ключ электронной подписи напрямую к сети Интернет.

4. Использовать программное обеспечение комплексной защиты компьютера (межсетевой экран+антивирус+средства обнаружения вторжения и т.п.).

5. Если нужен удаленный доступ к компьютеру для работы с ключом электронной подписи, то использовать криптографические средства защиты траффика (строить VPN).

Как получить электронную подпись

Процедура выдачи ЭП регулируется следующими документами:

1. Статья 18 Закона. Выдача квалифицированного сертификата

2. Порядок реализации Федеральной налоговой службой функций аккредитованного удостоверяющего центра и исполнения его обязанностей, утвержденный приказом Федеральной налоговой службы от 30.12.2020 № ВД-7-24/982@

Где получить электронную подпись

В точках выдачи по адресам:

г.Томск, пр.Комсомольский, 11а
г. Асино, Асиновский район, Томская область, ул. Стадионная, 35
с. Кожевниково, Томская область, ул. Кирова, 30
г. Стрежевой, Томской области, 4 мкр, д.455
г. Колпашево, Томская область, ул. Победы, 9
с. Кривошеино, Томская область, ул. Гагарина, 53
с. Каргасок, Томская область, ул. Октябрьская, 3

Что иметь для получения электронной подписи

Для выпуска электронной подписи необходимо иметь с собой:
Основной документ, удостоверяющий личность (паспорт).

А также копии, оригиналы или сведения из следующих документов:
Страховой номер индивидуального лицевого счета (СНИЛС);
Идентификационный номер налогоплательщика (ИНН).

Для записи ключа электронной подписи - сертифицированный ФСТЭК России или ФСБ России носитель (USB токен).

Как проверить электронную подпись

1. Обратиться в аккредитованный удостоверяющий центр.
Статья 13 Закона. Удостоверяющий центр

9) осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

2. Воспользоваться имеющимся средством электронной подписи

3. Воспользоваться сервисом на сайте госуслуг по ссылке
https://e-trust.gosuslugi.ru/#/portal/sig-check

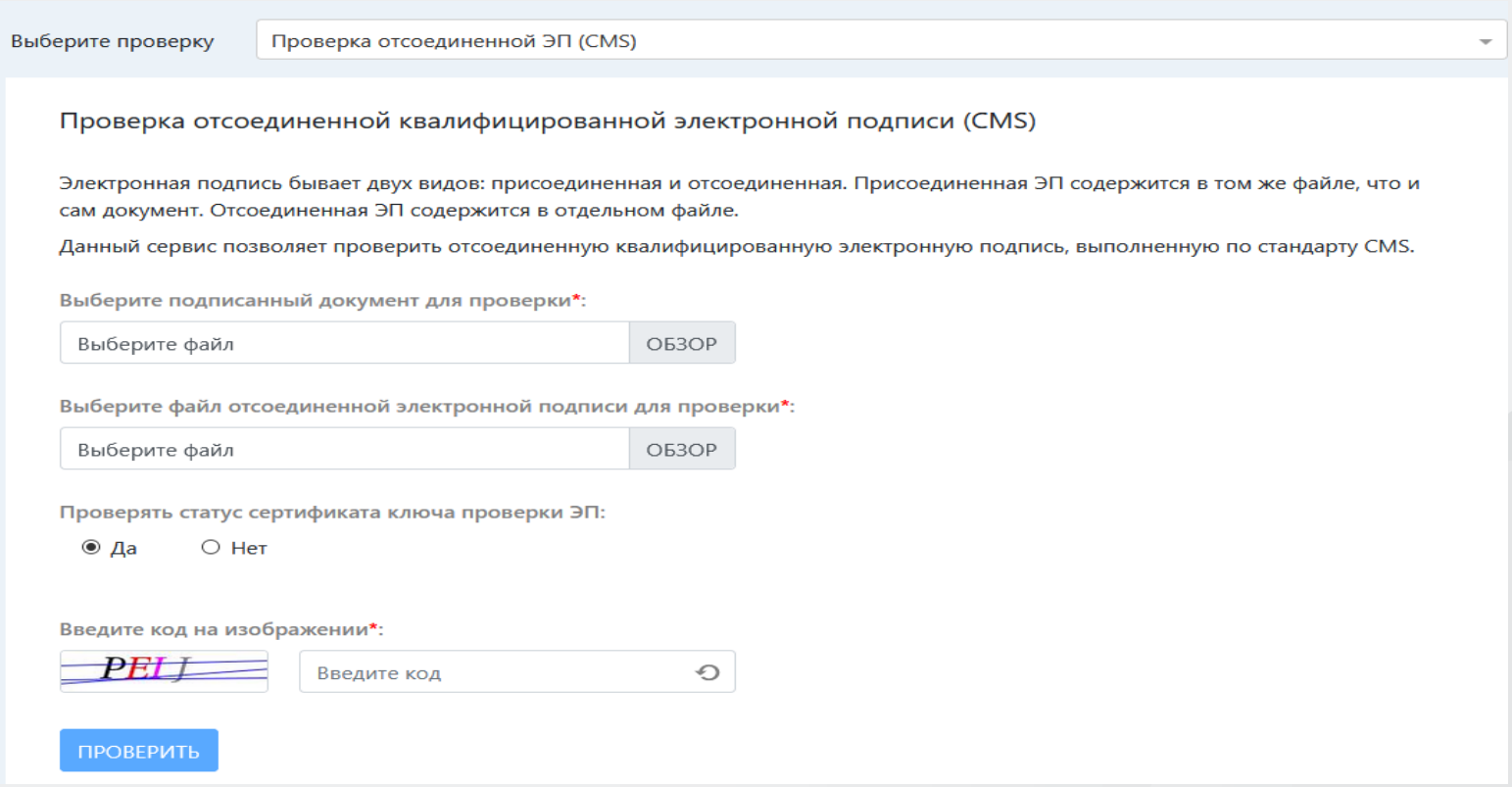
Что нужно для проверки электронной подписи

Подписанная информация – файл Подписанный_документ.pdf

Электронная подпись – файл Подписанный_документ.p7s
Или
Электронная подпись – файл Подписанный_документ.sig

Что нужно для проверки электронной подписи

Загрузить файлы в сервис проверки



Благодарю за внимание !