Семинарское занятие

ТЕМА 1.3.2:
ЭЛЕКТРОННАЯ ПОДПИСЬ: ТЕОРИЯ И ПРАКТИКА ИСПОЛЬЗОВАНИЯ

ГОТОВ К СЕМИНАРУ?

Электронная подпись: теория и практика использования

- **Электронная подпись -** это цифровой аналог собственноручной подписи, с помощью которого можно подписывать электронные документы. Такая подпись гарантирует, что документ исходит от конкретного лица, а для ряда электронных подписей - также то, что в него не вносились изменения с того момента, как он был подписан.
- С технической точки зрения электронная подпись представляет собой определенную информацию в электронной форме, которая присоединяется к подписываемой информации (п. 1 ст. 2 Закона об электронной подписи). На документе электронная подпись может выглядеть как набор символов, штамп с подписью и печатью или же вовсе быть невидимой.

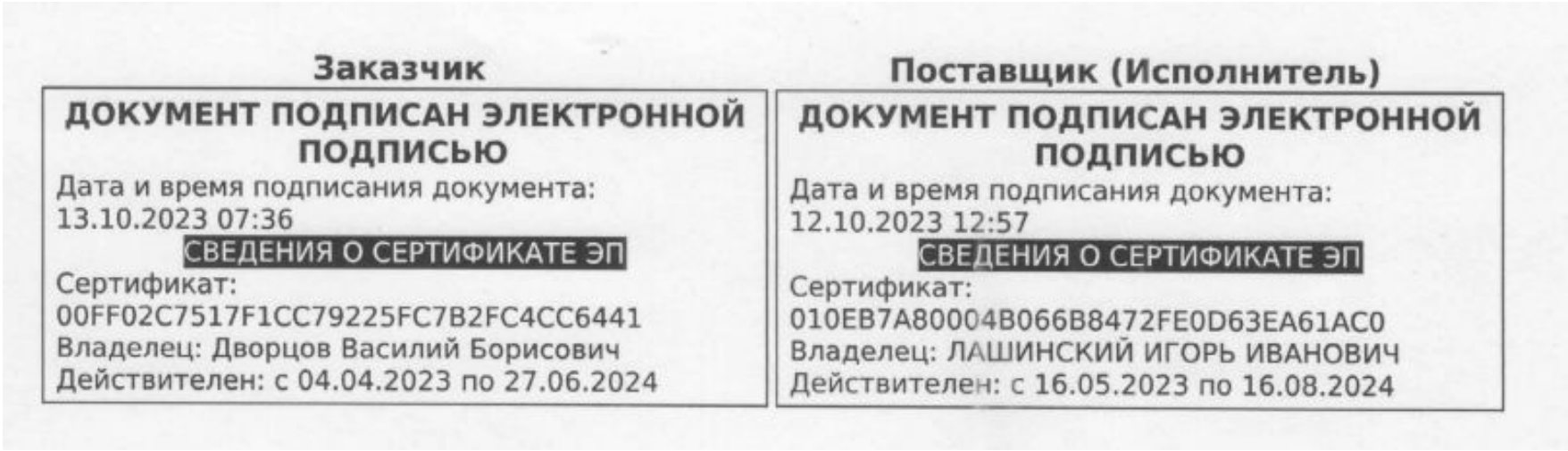

Заместитель директора
генерал-лейтенант внутренней службы А.В. Хабаров

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 288900583006136958066928874656377058980
Владелец: Хабаров Александр Владимирович
Действителен с 07.10.2022 по 31.12.2023

(Документ создан в электронной форме в Федеральной службе исполнения наказаний)

Электронная подпись: теория и практика использования



Заказчик

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Дата и время подписания документа:
13.10.2023 07:36

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат:
00FF02C7517F1CC79225FC7B2FC4CC6441
Владелец: Дворцов Василий Борисович
Действителен: с 04.04.2023 по 27.06.2024

Поставщик (Исполнитель)

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Дата и время подписания документа:
12.10.2023 12:57

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат:
010EB7A80004B066B8472FE0D63EA61AC0
Владелец: ЛАШИНСКИЙ ИГОРЬ ИВАНОВИЧ
Действителен: с 16.05.2023 по 16.08.2024

Электронная подпись: теория и практика использования

- Иногда электронной подписью называют материальный носитель, который выдается владельцам усиленных электронных подписей. Чаще всего это USB-флешка.

- Законом определено понятие метки доверенного времени. Метка представляет собой информацию в электронной форме о том, когда (дата, время) документ был подписан электронной подписью.
- Метку создает и проверяет доверенная третья сторона, удостоверяющий центр или оператор информационной системы в порядке, установленном Минцифры России (п. 19 ст. 2 Закона об электронной подписи

Электронная подпись: теория и практика использования

- **Выделяют простые и усиленные электронные подписи.**
- Простая электронная подпись - наименее защищенный вид подписи. Для подтверждения того, что такая подпись сформирована конкретным лицом, используются коды, пароли или аналогичные средства (ч. 2 ст. 5 Закона об электронной подписи). Например, это могут быть логин и пароль для входа на сайт или код, направленный в СМС-сообщении.
- 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).
- **В отличие от усиленной простая ЭП не гарантирует, что после подписания электронного документа в него не вносились изменения.**

Электронная подпись: теория и практика использования

- Простую электронную подпись чаще всего используют граждане для подтверждения банковских операций и получения ряда госуслуг. Организации нередко используют ее во внутреннем электронном документообороте. В частности, идентификация лица производится с помощью корпоративной электронной почты.

-).

Электронная подпись: теория и практика использования

- **Усиленные электронные подписи подразделяются на:**
  - Квалифицированные;
  - 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). То есть эти **подписи работают по принципу шифрования информации.**
- **Неквалифицированная подпись** надежнее простой, однако, как и простая, она **приравнивается к собственноручной, только если это предусмотрено нормативным правовым актом или соглашением**. Ее вправе выдавать любой удостоверяющий центр.

Электронная подпись: теория и практика использования

- **Квалифицированная подпись** - самый надежный вид подписи.
- **Она автоматически приравнивается к собственноручной.** Такая подпись обязательно должна иметь квалифицированный сертификат, выданный аккредитованным удостоверяющим центром.
- **Юрлица и ИП могут применять квалифицированную ЭП (КЭП), квалифицированный сертификат которой выдает удостоверяющий центр** (п. 1 ч. 1, п. 1 ч. 2, п. 4 ч. 3 ст. 17.2, п. 1 ст. 17.3, ст. 17.4 Закона об электронной подписи, Информация ФНС России, п. 1 Перечня, утвержденного Постановлением Правительства РФ от 10.07.2020 N 1018):
  - ФНС России;
  - Федерального казначейства - для государственных органов и органов местного самоуправления, а также государственных и муниципальных учреждений, ……;
  - Банка России - для участников финансового рынка.

Электронная подпись: теория и практика использования

- **В удостоверяющих центрах подпись получают бесплатно.**
- Квалифицированный **сертификат физлица, а также лица, планирующего действовать от имени юрлица по доверенности, можно получить в коммерческих аккредитованных удостоверяющих центрах .**
  - **ИЗМЕНЕНИЕ ПРАВИЛ АККРЕДИТАЦИИ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ**
- До 31 августа 2024 г. электронные документы можно подписывать КЭП, которую выдал удостоверяющий центр аккредитованный после 1 июля 2020 , в следующих случаях :
  - если от имени юрлица **действует лицо, не уполномоченное действовать без доверенно**сти, с сертификатом выданным **не позднее 31 августа 2023 г.** При этом в данном сертификате указано в качестве владельца также физлицо, являющееся таким представителем юрлица. Представлять электронную доверенность в машиночитаемом виде не требуется;
  - когда в правоотношениях участвует представитель ИП, с сертификатом выданным не позднее 31 августа 2023 г. Представлять электронную доверенность в машиночитаемом виде не требуется.

Электронная подпись: теория и практика использования

Усиленная электронная подпись используется, в частности:

- ✔ для сдачи отчетности в электронном виде (например, в налоговую, СФР);
- ✔ 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.

Неквалифицированная подпись в основном применяется во внутреннем документообороте организации, а также во взаимоотношениях с контрагентами.

Электронная подпись: теория и практика использования

Использование конкретного вида электронной подписи при подписании договора может быть предусмотрено (п. 1 ст. 160 ГК РФ):

1) соглашением сторон.

В соглашении вы можете определить, электронная подпись какого вида будет использоваться.

В некоторых случаях включить (ч. 2 ст. 6, ч. 2 ст. 9 Закона об электронной подписи):

правила определения лица, подписывающего электронный документ, по его простой электронной подписи;

обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность;

2) законом или иными правовыми актами.

Например, только усиленной квалифицированной электронной подписью можно подписать контракт для обеспечения государственных и муниципальных нужд, если он заключается по итогам электронной процедуры (п. 1 ч. 3, п. 1 ч. 4, ч. 5 ст. 51, п. 3 ч. 1 ст. 4 Закона N 44-ФЗ).

Электронная подпись: теория и практика использования

Удостоверяющий центр - администратор, который выдает и обслуживает усиленные электронные подписи. Гарант, который обеспечивает безопасность и надежность использования электронных подписей.

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

- при его присутствии;
- без его присутствия с использованием КЭП (при наличии действующего квалифицированного сертификата).

В дальнейшем 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).

Удостоверяющие центры бывают аккредитованными и неаккредитованными (ст. ст. 13, 15 Закона об электронной подписи). Выдавать квалифицированные сертификаты имеют право только аккредитованные удостоверяющие центры. К ним относятся удостоверяющие центры, получившие аккредитацию, а также удостоверяющие центры ФНС России, Казначейства России, Банка России (ч. 1 ст. 15 Закона об электронной подписи).

Электронная подпись: теория и практика использования

Порядок реализации Федеральным казначейством функций аккредитованного удостоверяющего центра и исполнения его обязанностей утвержден приказом Казначейства России от 15.06.2021 N 21н.

Федеральное казначейство осуществляет функции аккредитованного удостоверяющего центра непосредственно и через территориальные органы Федерального казначейства (далее - ТОФК).

Письмо Казначейства России от 25.08.2023 N 95-09-11/15-377 "О вопросах создания и выдачи сертификатов"

Электронная подпись: теория и практика использования

- **Ключ электронной подписи** - это уникальная последовательность символов, с помощью которой создается электронная подпись (п. 5 ст. 2 Закона об электронной подписи). 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.

Электронная подпись: теория и практика использования

- **Сертификат ключа проверки электронной подписи** - это документ, который подтверждает, что открытый ключ (ключ проверки электронной подписи) принадлежит лицу, которому выдан сертификат.
- Такой сертификат выдает удостоверяющий центр в форме электронного документа или в бумажном виде. **Пользоваться электронной подписью можно только в течение срока действия сертификата**, который устанавливает удостоверяющий центр (п. 2 ст. 2, ч. 4 ст. 14, п. 2 ч. 1 ст. 13 Закона об электронной подписи).
- Сертификат ключа проверки строго **необходим для усиленной квалифицированной подписи.** Для неквалифицированной он может не создаваться при соблюдении определенных требований (ч. 5 ст. 5 Закона об электронной подписи). Для простой подписи сертификат не создается.

Электронная подпись: теория и практика использования

- **Квалифицированный сертификат ключа проверки электронной подписи** - это документ, который создается для усиленной квалифицированной подписи и подтверждает, что такой ключ принадлежит его владельцу (п. 1 ч. 4 ст. 5 Закона об электронной подписи).
- От неквалифицированного он отличается следующим :
- 1) его может выдать только аккредитованный удостоверяющий центр или Минцифры России;
- 2) закон устанавливает форму и содержание такого сертификата.
- Владелец квалифицированного сертификата может получить информацию о сертификатах, выданных на его имя, через портал госуслуг.

Электронная подпись: теория и практика использования

Владелец сертификата ключа проверки электронной подписи - это лицо, которому выдана электронная подпись и которое имеет право использовать ее.

Им может быть (п. 2 ч. 2, ч. 3 ст. 14 Закона об электронной подписи):

1) Юрлицо. По общему правилу в качестве владельца сертификата наряду с юрлицом указывается физлицо, действующее от его имени без доверенности (как правило, руководитель). КЭП без обозначения такого физлица может применяться, если ее проверяют и создают без участия человека, например, когда юрлица взаимодействуют с использованием информационных систем (п. 4 Письма Минцифры России от 10.08.2021 N ОП-П15-085-33604);
2) гражданин (физлицо или ИП).

Статья: Сколько электронных подписей можно записать на одном токене ("Главная книга", 2022, N 3)

УКЭП должна храниться на специальном защищенном носителе - токене. Подойдут Рутокен ЭЦП 2.0, Рутокен S, JaCarta ГОСТ, ESMART Token ГОСТ или другие, соответствующие требованиям ФНС <1>. Обычная флешка для этого не годится.

Удостоверяющий центр (УЦ) вручает токен с записанной ЭП **лично ее владельцу**, и тот не должен передавать его кому бы то ни было.

Ппередача ключа ЭП другому лицу может повлечь нарушение конфиденциальности ключа подписи <2>.

В случае использования ЭП без согласия владельца тот обязан прекратить использование ЭП и немедленно обратиться в УЦ, выдавший сертификат, для прекращения его действия <3>.

Хранить на одном токене электронные подписи разных владельцев нельзя.

<1> подп. "в" п. 22 Порядка, утв. Приказом ФНС от 30.12.2020 N ВД-7-24/982@.

<2> пп. 1, 3 ч. 1 ст. 10 Закона от 06.04.2011 N 63-ФЗ; п. 6.5 Регламента, утв. Приказом ФНС от 05.07.2021 N ЕД-7-24/636@.

<3> ч. 6 ст. 17 Закона от 06.04.2011 N 63-ФЗ; Письмо ФНС от 20.08.2020 N ЕА-3-26/5960@.

ЭЛЕКТРОННАЯ ПОДПИСЬ И МАШИНОЧИТАЕМАЯ ДОВЕРЕННОСТЬ: ЧТО ИЗМЕНЯЕТСЯ С 1 СЕНТЯБРЯ 2023 ГОДА

- **По общему правилу подписывать электронные документы от имени организации возможно** (в частности, налоговую отчетность) тольк**о при наличии машиночитаемой доверенности** (МЧД).
- **Есть исключение, позволяющее отсрочить переход к ней на 1 год.**
- **МЧД - это электронный документ, который подтверждает полномочия лица действовать от имени организации.**
- **Доверенность оформляется в соответствии с требованиями ГК РФ. Ее представляют в том числе в электронной форме в машиночитаемом виде.**

ЭЛЕКТРОННАЯ ПОДПИСЬ И МАШИНОЧИТАЕМАЯ ДОВЕРЕННОСТЬ: ЧТО ИЗМЕНЯЕТСЯ С 1 СЕНТЯБРЯ 2023 ГОДА

- **Руководителю организации МЧД не нужна. Он подписывает документы электронной подписью юрлица, сертификат которой выдает налоговая служба.**
- **Остальные сотрудники** подписывают документы личными квалифицированными электронными подписями и **представляют МЧД в пакете электронных документов или иным способом.**
- **МЧД должна быть подписана электронной подписью организации** (отдельные правила действуют при передоверии, а также нотариальном удостоверении доверенности).

ЭЛЕКТРОННАЯ ПОДПИСЬ И МАШИНОЧИТАЕМАЯ ДОВЕРЕННОСТЬ: ЧТО ИЗМЕНЯЕТСЯ С 1 СЕНТЯБРЯ 2023 ГОДА

Для кого продлевается срок перехода к МЧД

Сотрудники, которые указаны в качестве владельцев сертификата подписи компании, могут продолжить их использовать и после 1 сентября 2023 года, МЧД при этом не нужна.

С 1 сентября 2023 года такие сертификаты выдавать не будут. Ранее выданные сертификаты будут действовать до окончания срока, но не позднее 31 августа 2024.

ЭЛЕКТРОННАЯ ПОДПИСЬ И МАШИНОЧИТАЕМАЯ ДОВЕРЕННОСТЬ: ЧТО ИЗМЕНЯЕТСЯ С 1 СЕНТЯБРЯ 2023 ГОДА

Особенности:

- при изменении с 1 сентября 2023 года состава сотрудников, которые будут подписывать электронные документы от имени организации, наделить новых сотрудников полномочиями можно будет только с помощью МЧД.

ЭЛЕКТРОННАЯ ПОДПИСЬ И МАШИНОЧИТАЕМАЯ ДОВЕРЕННОСТЬ: ЧТО ИЗМЕНЯЕТСЯ С 1 СЕНТЯБРЯ 2023 ГОДА

Как оформить МЧД

Решение этого вопроса зависит от того, для чего нужна электронная доверенность.

МЧД для сдачи налоговой отчетности можно оформить на сайте ФНС (https://service.nalog.ru/dovel/#/).

Сервис по созданию доверенностей, необходимых для электронного взаимодействия компаний друг с другом (https://m4d.nalog.gov.ru/create-xml-b2b-002/).

У СФР свои требования к доверенности и программное обеспечение для ее создания (https://lk.fss.ru/mchd.html).

Отдельный сервис по созданию МЧД для оформления документов от имени организации есть на Госуслугах (https://partners.gosuslugi.ru/catalog/attorney).

ЭЛЕКТРОННАЯ ПОДПИСЬ И МАШИНОЧИТАЕМАЯ ДОВЕРЕННОСТЬ: ЧТО ИЗМЕНЯЕТСЯ С 1 СЕНТЯБРЯ 2023 ГОДА

С 2 октября 2023 года в ГИС ЕИС ЗАКУПКИ стало доступным формирование и применение МАШИНОЧИТАЕМЫХ ДОВЕРЕННОСТЕЙ (далее – МЧД).

Начиная с этой даты заказчики и поставщики при подписании документов электронной подписью могут применять МЧД **как право**.

При этом функционалом ГИС ЕИС ЗАКУПКИ предусмотрены следующие особенности:

- формирование МЧД, содержащих полномочия на подписание сведений в ГИС ЕИС ЗАКУПКИ и на электронных площадках;
- выдача МЧД как с правом передоверия, так и без;
- представление МЧД при правоотношениях сторон с использованием личных кабинетов.

При этом в соответствии с положениями статьи 4 Федерального закона от 30.12.2021 № 443-ФЗ до 31.08.2024 допускается подписание документов

ЭЛЕКТРОННАЯ ПОДПИСЬ И МАШИНОЧИТАЕМАЯ ДОВЕРЕННОСТЬ: ЧТО ИЗМЕНЯЕТСЯ С 1 СЕНТЯБРЯ 2023 ГОДА

При этом в соответствии с положениями статьи 4 Федерального закона от 30.12.2021 № 44-ФЗ до 31.08.2024 допускается подписание документов квалифицированной электронной подписью юридического лица и индивидуального предпринимателя без представления МЧД участниками правоотношений.

В ГИС ЕИС ЗАКУПКИ будет доступно подписание документов электронной подписью без применения МЧД до указанного срока – 31.08.2024.

Казначейство рассказало, как применять электронные доверенности в ЕИС

- С 1 сентября 2024 года для всех участников закупок такая форма доверенности станет обязательной.
- До этого времени подписывать документы можно КЭП без МЧД.
- Со 2 октября заказчики и поставщики могут выдавать машиночитаемую доверенность в ЕИС.
- **Доверенности, которые нужны для закупок, формируются и размещаются исключительно в ЕИС.** Из других информационных систем МЧД поступать не будут.

Казначейство рассказало, как применять электронные доверенности в ЕИС

- **Чтобы выдать МЧД по 44-ФЗ, нужно выполнить три шага.**
- **Шаг 1.** Настройте права доступа сотрудникам, которым понадобится МЧД.
- В личном кабинете в разделе «Администрирование» перейдите к пункту «Пользователи организации». Выберите сотрудника и нажмите на кнопку «Регистрационные данные». В разделе «Права доступа» выберите нужные сотруднику права и нажмите «Сохранить». Возле права доступа, для которого нужна МЧД, появится специальная иконка. Например, разместить извещение о закупке без МЧД не получится.

Казначейство рассказало, как применять электронные доверенности в ЕИС

- **Шаг 2.** Заполните доверенность.
- В разделе «Уведомление» выберите пункт «Выдать доверенность». На экране появится доверенность. Часть сведений заполнится в документе автоматически, остальные данные нужно дозаполнить вручную.
- **Шаг 3.** Подпишите доверенность. На экранной форме доверенности поставьте галочку «Я подтверждаю, что согласен на подписание указанной информации своей электронной подписью и размещение ее в реестре доверенностей ЕИС». Нажмите на две кнопки: «Подписать» и «Разместить».

Казначейство рассказало, как применять электронные доверенности в ЕИС

- Машиночитаемая доверенность поступит в ЕИС в составе всех электронных документов через личный кабинет пользователя. Возле документа, который подписали с помощью МЧД, появится соответствующая иконка. Если нажать на иконку, увидите доверенность с реквизитами и сведениями о доверителе, представителе и лицах – передоверителях.

Казначейство рассказало, как применять электронные доверенности в ЕИС

- На примере этапа подписания контракта специалисты Казначейства рассказали, как заказчик и поставщик будут использовать МЧД на площадке и в системе.
- После размещения итогового протокола заказчик формирует и направляет проект контракта без подписи. Машиночитаемая доверенность понадобится сначала победителю закупки.
- Если контракт подписывает руководитель организации, доверенность не понадобится, если подпись ставит другое лицо – нужна МЧД. Смотрите на схеме, как от оператора площадки МЧД поступит заказчику. **Если контракт подпишет иное лицо, которое в доверенности не уполномочено на такие действия, заказчик признает победителя уклонившимся от заключения контракта** (ст. 51 Закона № 44-ФЗ).

Казначейство рассказало, как применять электронные доверенности в ЕИС

- При работе с МЧД учитывайте четыре правила:

1) Если в ЕИС расширить сотруднику список полномочий, нужно выдать новые МЧД на эти полномочия.
2) Если МЧД выдана в порядке передоверия, а у доверителя отменили или отозвали доверенность, все выданные доверенности автоматически станут недействительными.
3) Если истек срок действия МЧД, нужно выдать новую доверенность. **Срок МЧД автоматически не пролонгируется.**
4) ПОКА НЕ ОТМЕНЯТ ДОВЕРЕННОСТЬ, ОНА ДЕЙСТВУЕТ, даже в случае смерти, увольнения, банкротства, ликвидации доверителя

1. *Электронная подпись в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» — это:*

- 1) 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;
- 2) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата.

2. *Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» регулирует отношения в области использования электронных подписей* {*несколько верных ответов*):

- 1) при оказании государственных и муниципальных услуг;
- 2) совершении гражданско-правовых сделок;
- 3) исполнении государственных и муниципальных функций;
- 4) совершении иных юридически значимых действий.

3. *Ключ электронной подписи — это*:

- 1) уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее — проверка электронной подписи);
- 2) уникальная последовательность символов, предназначенная для создания электронной подписи.

4. ***Ключ проверки электронной подписи — это:***

- 1) уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее — проверка электронной подписи);
- 2) уникальная последовательность символов, предназначенная для создания электронной подписи.

5. *Удостоверяющий центр — это*:

- 1) юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;
- 2) осуществляющий обмен информацией в электронной форме государственный орган, орган местного самоуправления или организация;
- 3) лицо, которому в установленном законом порядке выдан сертификат ключа проверки электронной подписи.

6. *Сертификат ключа проверки электронной подписи — это:*

- 1) уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее — проверка электронной подписи);
- 2) электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

7. *Видами электронных подписей в соответствии с Федеральным законом № 63-ФЗ являются (несколько верных ответов):*

- 1) простая электронная подпись;
- 2) простая неквалифицированная электронная подпись;
- 3) усиленная неквалифицированная электронная подпись;
- 4) усиленная квалифицированная электронная подпись.

8. *Простой электронной подписью в соответствии с Федеральным законом № 63-ФЗ является*:

- 1) электронная подпись, для которой ключ проверки электронной подписи указан в квалифицированном сертификате;
- 2) электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом;
- 3) электронная подпись, которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи.

9. ***Неквалифицированной электронной подписью в соответствии с Федеральным законом № 63-ФЗ является электронная подпись, которая (несколько верных ответов)***:

- 1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- 2) позволяет определить лицо, подписавшее электронный документ;
- 3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- 4) создается с использованием средств электронной подписи.

10. ***Квалифицированной электронной подписью в соответствии с Федеральным законом № 63-ФЗ является:***

- 1) электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом;
- 2) электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи, а также ключ проверки электронной подписи указан в квалифицированном сертификате;
- 3) электронная подпись, которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи.

11. *В чем отличие рукописной подписи от электронной (несколько верных ответов)*:

- 1) электронную подпись можно подделать, а рукописную подпись нельзя;
- 2) с помощью электронной подписи можно определить реальное время подписания документа в отличие от рукописной подписи;
- 3) в рукописной подписи содержатся метка времени, а в электронной подписи не содержится;
- 4) рукописную подпись можно удостоверить в отличие от электронной подписи;
- 5) дополнительное свойство электронной подписи — контроль целостности подписанного документа.

12. *При отправке по электронной почте подписанного ЭЦП документа будет отправлен*:

- 1) сам файл и подпись файла;
- 2) только файл;
- 3) только подпись.

13. ***При подписании файла электронной цифровой подписью:***

- 1) создается новая версия файла, в которую добавляется подпись;
- 2) все версии файла преобразуются с помощью крипто-алгоритмов ЭЦП;
- 3) к файлу добавляется подпись, при этом сам файл не меняется.

14. Разрешается ли редактирование файла, подписанного ЭЦП:

- 1) нет;
- 2) да;
- 3) разрешается только пользователю с полными правами.

15. *Может ли документ одновременно быть зашифрованным и подписанным ЭЦП*:

- 1) да;
- 2) нет.

16. *При подписании документа ЭЦП используется*:

- 1) открытый ключ;
- 2) секретный ключ;
- 3) сертификат ключа.

21. ***Какую роль выполняет электронная цифровая подпись:***

- 1) роль дополнительной информации о передаваемых данных;
- 2) это данные о времени передачи информации;
- 3) роль обычной подписи в электронных документах;
- 4) роль обратного адреса отправителя.

24. ***Первый ФЗ «Об электронной цифровой подписи» в Российской Федерации был принят:***

- 1) в 2000 г.;
- 2) в 2002 г.;
- 3) в 2006 г.