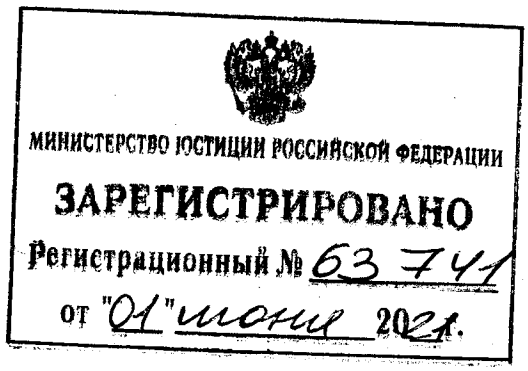
# ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

# ПРИКАЗ

1 мая 2021 года **Москва** **№** 171

Об утверждении организационно-технических требований в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц




В соответствии с частью 6.1 статьи 15 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»[1] и пунктом 1 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960[2],

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые организационно-технические требования в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти,

[1] Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2019, № 52, ст. 7794.
[2] Собрание законодательства Российской Федерации, 2003, № 33, ст. 3254; 2007, № 1, ст. 205.

уполномоченного на осуществление государственной регистрации юридических лиц.

2. Настоящий приказ вступает в силу с 1 марта 2022 г. и действует до 1 марта 2028 г.

Директор А.Бортников

Утверждены
приказом ФСБ России
от 1 мая 2021 г.
№ 171

# Организационно-технические требования в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц

1. Настоящий документ определяет организационно-технические требования в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц (далее – Требования и доверенные лица соответственно), наделяемым в соответствии с частью 6.1 статьи 15 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее – Закон об электронной подписи) полномочиями на прием заявлений о получении квалифицированного сертификата ключа проверки электронной подписи (далее – квалифицированный сертификат) юридического лица и выполнение требований статьи 18 Закона об электронной подписи от имени удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц[1] (далее – УЦ), на создание ключа электронной подписи (далее – ЭП) (при условии исключения возможности доступа работников таких доверенных лиц к ключам ЭП заявителей), а также на хранение ключей усиленных квалифицированных ЭП (далее – квалифицированная ЭП) для дистанционного использования и на создание при помощи указанных ключей квалифицированных ЭП для электронных документов.

---

[1] Абзац второй пункта 1 Положения о Федеральной налоговой службе, утвержденного постановлением Правительства Российской Федерации от 30 сентября 2004 г. № 506 (Собрание законодательства Российской Федерации, 2004, № 40, ст. 3961; 2021, № 5, ст. 852).

2. При реализации полномочий, которыми УЦ наделил доверенное лицо в соответствии с частью 6.1 статьи 15 Закона об электронной подписи, доверенное лицо должно:

2.1. Осуществлять контроль за нахождением и действиями лиц и (или) транспортных средств в зданиях и помещениях, предназначенных для размещения технических средств, обеспечивающих выполнение доверенным лицом своих функций (далее – контролируемая зона).

2.2. Ограничивать доступ в контролируемую зону, обеспечивать конфиденциальность проводимых в ней работ, сохранность помещений, оборудования и документов путем:

оборудования помещений в контролируемой зоне системой контроля доступа, использующей электронные идентификаторы;

предотвращения доступа в контролируемую зону лиц, не имеющих права доступа в нее;

осуществления контроля пребывания и действий лиц, допускаемых в контролируемую зону, и не относящихся к работникам доверенного лица;

осуществления контроля нахождения в контролируемой зоне транспортных средств;

обеспечения возможности экстренной эвакуации в случае возникновения пожара и других чрезвычайных ситуаций работников доверенного лица, технических средств, обеспечивающих выполнение доверенным лицом своих функций, иного оборудования и документов доверенного лица с учетом обеспечения конфиденциальности информации ограниченного доступа, обладателями которой являются доверенное лицо и его работники;

установления правил нахождения лиц в контролируемой зоне, порядка контроля их выполнения, мер по предупреждению нарушений указанных правил и ликвидации последствий таких нарушений.

2.3. Организовать и вести учет машинных носителей информации (средств обработки (хранения) информации, съемных машинных носителей информации), используемых средствами криптографической защиты информации (далее – СКЗИ), включая средства ЭП.

2.4. Обеспечивать защиту машинных носителей информации от несанкционированного доступа к ним и хранящейся на них информации, а также от их несанкционированного использования.

2.5. Обеспечивать защиту подключения к информационно-телекоммуникационным сетям общего пользования, в том числе к информационно-телекоммуникационной сети «Интернет», технических средств, обеспечивающих выполнение доверенным лицом своих функций, за исключением оборудования, обеспечивающего информационное взаимодействие с УЦ, реализацию схемы доставки заявления о получении квалифицированного сертификата юридического лица в УЦ в соответствии с пунктами 6 и 7 дополнительных требований к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, утвержденных постановлением Правительства Российской Федерации от 31 декабря 2020 г. № 2409[1] (далее – дополнительные требования).

2.6. Применять для выполнения возложенных на доверенное лицо функций информационные системы, аттестованные на соответствие Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17[2] (с изменениями,

---

[1] Действуют до 6 января 2027 г. Собрание законодательства Российской Федерации, 2021, № 2, ст. 455.

[2] Зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608.

внесенными приказами ФСТЭК России от 15 февраля 2017 г. № 27[1], от 28 мая 2019 г. № 106[2]).

2.7. Применять некриптографические средства защиты информации в системах защиты информации информационных систем, указанных в подпункте 2.5 пункта 2 Требований, сертифицированные по требованиям безопасности информации, устанавливаемым ФСТЭК России в соответствии с подпунктом 9.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085[3], или ФСБ России в соответствии с подпунктом 21 пункта 9 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960[4], и обеспечивающие:

защиту от угроз в виде целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения инженерно-технической и криптографической безопасности используемых доверенным лицом средств защиты информации, или с целью создания условий для этого (далее – атака), направленных на веб-сервера, в том числе путем контроля и фильтрации информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера;

защиту от вредоносного программного обеспечения, в том числе обнаружение компьютерных программ или иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования защищаемой информации или нарушения штатного функционирования средств защиты информации, а также реагирование на обнаружение этих программ и информации;

---

[1] Зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933.
[2] Зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924.
[3] Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2018, № 20, ст. 2818.
[4] Собрание законодательства Российской Федерации, 2003, № 33, ст. 3254; 2007, № 1, ст. 205.

обнаружение (предотвращение) вторжений, направленных на преднамеренный несанкционированный доступ к обрабатываемой информации, специальное воздействие на средства защиты информации и (или) информацию в целях ее получения, уничтожения, искажения и блокирования доступа к информации, а также для реагирования на эти действия (предотвращение этих действий);

доверенную загрузку средств вычислительной техники, в том числе путем контроля локального доступа и целостности программного обеспечения средств вычислительной техники.

2.8. Соблюдать требования эксплуатационной документации на используемые СКЗИ, включая средства ЭП.

2.9. Утвердить локальный акт, включающий:

а) комплекс мер по ограничению доступа в контролируемую зону, обеспечению конфиденциальности проводимых в ней работ, сохранности помещений, оборудования и документов доверенного лица с указанием работников, ответственных за осуществление соответствующих мер;

б) правила идентификации и аутентификации работников доверенного лица, исполняющих обязанности в соответствии с пунктом 9 Требований, и инициируемых ими процессов на средствах вычислительной техники, криптографических ключей, обрабатываемой информации, программного кода;

в) правила управления доступом;

г) правила управления программной средой, регулирующие контроль программной среды, установку компонентов программного обеспечения, их запуск, обращение к ним, проведение обновлений;

д) правила защиты машинных носителей информации;

е) правила регистрации событий и просмотра журналов событий работниками доверенного лица;

ж) правила осуществления антивирусной защиты;

з) правила обнаружения вторжений и реагирования на них (их предотвращения);

и) правила контроля целостности программного обеспечения, включая установление периодичности регламентного контроля целостности программных и аппаратных компонентов средств ЭП, СКЗИ;

к) правила обеспечения доступа работников доверенного лица к техническим средствам, регулирующие:

резервирование технических средств, каналов передачи информации, программного обеспечения с указанием периодичности резервного копирования информации в объеме, необходимом для восстановления возможности выполнения доверенным лицом своих функций;

контроль безопасного функционирования средств ЭП, СКЗИ, включая действия при обнаружении сбоев и (или) возникновении неисправностей и сроки восстановления;

л) правила защиты информации от утечки по техническим каналам, регулирующие в том числе размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;

м) правила действий в нештатных ситуациях (при пожаре и иной чрезвычайной ситуации);

н) порядок проверки (аудита) состояния информационной безопасности в доверенном лице и выполнения Требований и сроков ее (его) проведения.

3. Для идентификации заявителя с использованием квалифицированной ЭП при наличии действующего квалифицированного сертификата, а также при идентификации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными

владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»[1] (далее – единая система идентификации и аутентификации) и единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (далее – единая биометрическая система) в порядке, установленном Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2], доверенным лицом должны применяться информационные системы, для которых обеспечивается защита от атак, реализуемых с использованием возможностей, указанных в пункте 13 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10 июля 2014 г. № 378[3] (далее – Состав и содержание организационных и технических мер).

---

[1] Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (Собрание законодательства Российской Федерации, 2011, № 49, ст. 7284; 2021, № 1, ст. 114).

[2] Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2021, № 11, ст. 1708.

[3] Зарегистрирован Минюстом России 18 августа 2014 г., регистрационный № 33620.

4. Для организации приема заявления о получении квалифицированного сертификата юридического лица доверенным лицом реализуется в соответствии с пунктом 7 дополнительных требований схема доставки в УЦ заявления о выдаче квалифицированного сертификата, включающая перечень необходимых средств защиты информации, обеспечивающих конфиденциальность, целостность и достоверность персональных данных, содержащихся в таком заявлении.

5. При приеме заявления о получении квалифицированного сертификата юридического лица доверенное лицо должно:

подтвердить соответствие средства ЭП, находящегося во владении заявителя и используемого им для создания ЭП, проверки ЭП, создания ключа ЭП и ключа проверки ЭП, Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796[1] (с изменениями, внесенными приказом ФСБ России от 4 декабря 2020 г. № 555[2])[3] (далее – Требования к средствам ЭП);

подтвердить факт владения заявителем ключом ЭП, соответствующим ключу проверки ЭП, указанному им для получения квалифицированного сертификата юридического лица, в соответствии с правилами подтверждения владения ключом ЭП, предусмотренными пунктом 1 части 5 статьи 8 Закона об электронной подписи;

учесть сведения о заявителе в информационной системе доверенного лица (в случае отсутствия подтверждения владения заявителем ключом ЭП, который соответствует ключу проверки ЭП, указанному заявителем для получения квалифицированного сертификата) и при его новом обращении за получением квалифицированного сертификата направить запросы в аккредитованные удостоверяющие центры с целью выявления уникальности ключа проверки ЭП, указанного заявителем для получения сертификата;

---

[1] Зарегистрирован Минюстом России 9 февраля 2012 г., регистрационный № 23191.
[2] Зарегистрирован Минюстом России 30 декабря 2020 г., регистрационный № 61972.
[3] Действуют до 1 января 2027 г.

отказать заявителю в создании квалифицированного сертификата в случае неподтверждения уникальности ключа проверки ЭП, указанного заявителем для получения сертификата, по результатам проверки, проведенной в соответствии с абзацем четвертым настоящего пункта.

6. При реализации полномочий на прием заявлений о получении квалифицированного сертификата юридического лица, содержащих достоверную и актуальную информацию, доверенное лицо должно:

соблюдать сроки эксплуатации средств ЭП, находящихся во владении доверенного лица, указанные в документах о подтверждении соответствия этих средств Требованиям к средствам ЭП;

информировать заявителя в письменной форме о необходимости соблюдения им условий эксплуатации имеющихся у него средств ЭП и СКЗИ, применяемых для аутентификации владельцев квалифицированных сертификатов, по поручению которых создается и проверяется квалифицированная ЭП, защиты информации, передаваемой по каналу взаимодействия между владельцем квалифицированного сертификата и УЦ, осуществляющим создание и проверку квалифицированной ЭП по поручению такого владельца, требований по доказательству невозможности отказа владельца квалифицированного сертификата от поручения на создание квалифицированной ЭП (далее – СКЗИ для дистанционного использования ключей ЭП), в соответствии с эксплуатационной документацией на данные средства;

применять информационные системы, обеспечивающие хранение квалифицированных сертификатов, используемых для создания квалифицированных ЭП доверенного лица, которое исключает модификацию, подмену хранящихся квалифицированных сертификатов, несанкционированное добавление сертификатов в хранилище и удаление из хранилища квалифицированных сертификатов.

7. Для подтверждения сведений, предоставляемых заявителем в соответствии с пунктами 1 и 2 части 1, частями 2 и 2.1 статьи 18 Закона об электронной подписи, доверенное лицо должно применять информационные системы, обеспечивающие получение необходимых сведений посредством единой системы межведомственного электронного взаимодействия из информационных систем органов государственной власти, Пенсионного фонда Российской Федерации, единой информационной системы нотариата, единой системы идентификации и аутентификации и единой биометрической системы, для которых обеспечивается защита от атак, реализуемых с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

8. При реализации полномочий по созданию ключей ЭП по обращению заявителей, а также при создании ключей ЭП доверенного лица, которые используются для подписания электронных документов и информации, доверенное лицо должно:

применять средства ЭП классов КВ2 и (или) КА1[1], имеющие в своем составе датчик, вырабатывающий случайную последовательность чисел путем преобразования сигнала случайного процесса, генерируемого недетерминируемой физической системой, устойчивой по отношению к реально возможным изменениям внешних условий и своих параметров, и механизм контроля срока действия ключей ЭП;

записывать ключи ЭП, созданные по обращению заявителя, на специализированные ключевые носители, исключающие их несанкционированное использование и копирование;

хранить, использовать и уничтожать ключи ЭП доверенного лица, предназначенные для подписания электронных документов и информации, в средстве ЭП, в котором они были созданы.

---

[1] Пункты 17 и 18 Требований к средствам ЭП.

применять СКЗИ, не являющиеся средствами ЭП, классов КВ и (или) КА[1];

применять средства ЭП классов, отличных от классов КВ2 и (или) КА1, СКЗИ, не являющиеся средствами ЭП, классов, отличных от классов КВ и (или) КА, в схеме доставки заявления о получении квалифицированного сертификата юридического лица в УЦ в соответствии с пунктом 7 дополнительных требований.

9. Для исключения возможности доступа работников доверенного лица к ключам ЭП заявителей[2] при реализации полномочий по созданию ключа ЭП доверенное лицо должно применять информационные системы, поддерживающие следующее распределение между отдельными работниками раздельных групп обязанностей:

системного администратора, осуществляющего установку, конфигурирование и поддержку функционирования используемых для реализации полномочий информационных систем, создание и поддержку профилей членов группы администраторов, конфигурирование профиля и параметров журнала регистрации событий;

администратора регистрации, осуществляющего регистрацию заявлений о создании квалифицированных сертификатов юридических лиц и передачу их в УЦ;

администратора информационной безопасности, осуществляющего контроль и обеспечение функционирования средств защиты информации используемых средств и информационных систем, анализ и мониторинг состояния их защищенности, контроль выполнения организационных мер защиты;

---

[1] Требования к СКЗИ классов КВ и КА содержатся в рекомендациях по стандартизации Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации, утвержденных приказом Росстандарта от 22 декабря 2017 г. № 2068-ст (Стандартинформ, 2018).

[2] Часть 6.1 статьи 15 Закона об электронной подписи.

администратора аудита, осуществляющего мониторинг функционирования используемых средств и информационных систем путем просмотра и поддержки журналов регистрации событий (журналов аудита);

администратора средства ЭП, осуществляющего установку, конфигурирование и поддержку функционирования средства ЭП, конфигурирование профиля и параметров журнала регистрации событий для средства ЭП;

администратора по резервному копированию и восстановлению используемых средств и информационных систем, осуществляющего функции по созданию и управлению резервными копиями соответствующей информации.

10. При реализации полномочий по хранению ключей квалифицированных ЭП для дистанционного использования и по созданию при помощи указанных ключей квалифицированных ЭП электронных документов доверенное лицо должно:

применять средства ЭП и СКЗИ для дистанционного использования ключей ЭП, имеющие подтверждение соответствия требованиям, установленным в соответствии с пунктом 2.1 части 5 статьи 8 Закона об электронной подписи;

хранить, использовать и уничтожать криптографические ключи, созданные по обращению заявителя для применения в СКЗИ для дистанционного использования ключей ЭП, в соответствии с эксплуатационной документацией на такие СКЗИ.

11. При выдаче по обращению заявителя средств ЭП, специализированного ключевого носителя с ключом ЭП, СКЗИ для дистанционного использования ключей ЭП, криптографических ключей, созданных по обращению заявителя для применения в СКЗИ для дистанционного использования ключей ЭП, доверенное лицо должно:

применять способ, исключающий подмену, модификацию или уничтожение выдаваемых средств, эксплуатационной документации на них, специализированных ключевых носителей и ключей;

обеспечивать учет сроков, в течение которых действуют подтверждение соответствия выдаваемых средств ЭП Требованиям к средствам ЭП, результаты экспертизы тематических исследований выдаваемых СКЗИ, осуществленной в соответствии с пунктом 33 Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 9 февраля 2005 г. № 66[1] (с изменениями, внесенными приказом ФСБ России от 12 апреля 2010 г. № 173[2]);

информировать заявителя о сроках, указанных в абзаце третьем настоящего пункта, а также направлять ему уведомления об истечении указанных сроков за месяц до их окончания;

информировать заявителей об условиях и о порядке использования ЭП, средств ЭП, СКЗИ, о рисках, связанных с использованием ЭП, в том числе при дистанционном использовании ключей ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и ее проверки в виде памятки в письменной форме;

информировать заявителя о сроках действия выданных ему ключей.

12. При реализации полномочий на выполнение требований статьи 18 Закона об электронной подписи от имени УЦ в части выдачи заявителю квалифицированного сертификата юридического лица доверенное лицо должно:

применять способ, исключающий подмену, модификацию или уничтожение выдаваемых заявителю квалифицированного сертификата юридического лица, квалифицированного сертификата УЦ, с использованием

---

[1] Зарегистрирован Минюстом России 3 марта 2005 г., регистрационный № 6382.
[2] Зарегистрирован Минюстом России 25 мая 2010 г., регистрационный № 17350.

которого подписан квалифицированный сертификат юридического лица, квалифицированного сертификата головного удостоверяющего центра Минцифры России, с использованием которого подписан соответствующий квалифицированный сертификат УЦ;

информировать заявителя о сроках действия выданных ему квалифицированных сертификатов.

13. При реализации полномочий на выполнение требований части 3 статьи 18 Закона об электронной подписи от имени УЦ, установленных для подтверждения ознакомления с информацией, содержащейся в квалифицированном сертификате, доверенное лицо должно:

применять информационные системы, для которых обеспечивается защита от атак, реализуемых с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер;

передавать подтверждения ознакомления с информацией, содержащейся в квалифицированном сертификате, в УЦ не реже чем раз в месяц.