Приказ Минцифры России от 26.11.2020 N 624
(ред. от 31.01.2022)
"Об утверждении перечня угроз безопасности, актуальных при идентификации заявителя - физического лица в аккредитованном удостоверяющем центре, выдаче квалифицированного сертификата без его личного присутствия с применением информационных технологий путем предоставления сведений из единой системы идентификации и аутентификации и единой информационной системы персональных данных, обеспечивающей обработку, сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, а также хранении и использовании ключа электронной подписи в аккредитованном удостоверяющем центре"
(Зарегистрировано в Минюсте России 22.12.2020 N 61689)

Зарегистрировано в Минюсте России 22 декабря 2020 г. N 61689

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 26 ноября 2020 г. N 624

ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ УГРОЗ БЕЗОПАСНОСТИ, АКТУАЛЬНЫХ ПРИ ИДЕНТИФИКАЦИИ ЗАЯВИТЕЛЯ - ФИЗИЧЕСКОГО ЛИЦА В АККРЕДИТОВАННОМ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ, ВЫДАЧЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА БЕЗ ЕГО ЛИЧНОГО ПРИСУТСТВИЯ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПУТЕМ ПРЕДОСТАВЛЕНИЯ СВЕДЕНИЙ ИЗ ЕДИНОЙ СИСТЕМЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ И ЕДИНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБЕСПЕЧИВАЮЩЕЙ ОБРАБОТКУ, СБОР И ХРАНЕНИЕ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИХ ПРОВЕРКУ И ПЕРЕДАЧУ ИНФОРМАЦИИ О СТЕПЕНИ ИХ СООТВЕТСТВИЯ ПРЕДОСТАВЛЕННЫМ БИОМЕТРИЧЕСКИМ ПЕРСОНАЛЬНЫМ ДАННЫМ ГРАЖДАНИНА РОССИЙСКОЙ ФЕДЕРАЦИИ, А ТАКЖЕ ХРАНЕНИИ И ИСПОЛЬЗОВАНИИ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ В АККРЕДИТОВАННОМ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

Список изменяющих документов
(в ред. Приказа Минцифры России от 31.01.2022 N 71)

Во исполнение положений пункта 7 части 4 статьи 8 Федерального закона от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" (Собрание законодательства Российской Федерации, 2011, N 15, ст. 2036; 2019, N 52, ст. 7794) <1> приказываю:

<1> Пункт 1 Положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 г. N 418 (Собрание законодательства Российской Федерации, 2008, N 23, ст. 2708; 2018, N 40, ст. 6142).

1. Утвердить прилагаемый перечень угроз безопасности, актуальных при идентификации заявителя - физического лица в аккредитованном удостоверяющем центре, выдаче квалифицированного сертификата без его личного присутствия с применением информационных технологий путем предоставления сведений из единой системы идентификации и аутентификации и единой информационной системы персональных данных, обеспечивающей обработку, сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина

Российской Федерации, а также хранении и использовании ключа электронной подписи в аккредитованном удостоверяющем центре.

2. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

3. Настоящий приказ вступает в силу с 1 января 2021 г. и действует до 1 января 2027 г.

Министр
М.И.ШАДАЕВ

Утвержден
приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 26.11.2020 N 624

ПЕРЕЧЕНЬ УГРОЗ БЕЗОПАСНОСТИ, АКТУАЛЬНЫХ ПРИ ИДЕНТИФИКАЦИИ ЗАЯВИТЕЛЯ - ФИЗИЧЕСКОГО ЛИЦА В АККРЕДИТОВАННОМ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ, ВЫДАЧЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА БЕЗ ЕГО ЛИЧНОГО ПРИСУТСТВИЯ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПУТЕМ ПРЕДОСТАВЛЕНИЯ СВЕДЕНИЙ ИЗ ЕДИНОЙ СИСТЕМЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ И ЕДИНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБЕСПЕЧИВАЮЩЕЙ ОБРАБОТКУ, СБОР И ХРАНЕНИЕ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИХ ПРОВЕРКУ И ПЕРЕДАЧУ ИНФОРМАЦИИ О СТЕПЕНИ ИХ СООТВЕТСТВИЯ ПРЕДОСТАВЛЕННЫМ БИОМЕТРИЧЕСКИМ ПЕРСОНАЛЬНЫМ ДАННЫМ ГРАЖДАНИНА РОССИЙСКОЙ ФЕДЕРАЦИИ, А ТАКЖЕ ХРАНЕНИИ И ИСПОЛЬЗОВАНИИ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ В АККРЕДИТОВАННОМ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

Список изменяющих документов
(в ред. Приказа Минцифры России от 31.01.2022 N 71)

1. Угрозы безопасности, актуальные при идентификации заявителя - физического лица (далее - физическое лицо) в аккредитованном удостоверяющем центре, выдаче квалифицированного сертификата ключа проверки электронной подписи (далее - квалифицированный сертификат) без его личного присутствия с применением информационных технологий путем предоставления сведений из единой системы идентификации и аутентификации и единой информационной системы персональных данных, обеспечивающей обработку, 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):

1.1. при обработке, хранении, проверке биометрических персональных данных, обработке и передаче информации о степени соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в единой биометрической системе - угрозы, определяемые в соответствии с частью 14 статьи 14.1 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2018, N 1, ст. 66);

1.2. при передаче информации о степени соответствия биометрических персональных данных предоставленным биометрическим персональным данным гражданина Российской Федерации из единой биометрической системы и персональных данных из единой системы идентификации и аутентификации (далее - информация о степени соответствия) в аккредитованный удостоверяющий центр:

1.2.1. угроза нарушения целостности (подмены, удаления) информации о степени соответствия, в том числе путем реализации целенаправленных действий 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 Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 (зарегистрирован Министерством юстиции Российской Федерации 18 августа 2014 г., регистрационный N 33620) (далее - Состав и содержание организационных и технических мер, приказ ФСБ России N 378);

1.2.2. угроза нарушения конфиденциальности информации о степени соответствия, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер;

1.3. при направлении в аккредитованный удостоверяющий центр запроса на выдачу квалифицированного сертификата, хранение которого осуществляется на устройстве владельца квалифицированного сертификата:

1.3.1. угроза нарушения целостности (подмены) информации о ключе проверки электронной подписи лица, обратившегося с заявлением на выдачу квалифицированного сертификата, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 Требований к средствам электронной подписи, утвержденных приказом Федеральной службы безопасности Российской Федерации от 27.12.2011 N 796 (зарегистрирован Министерством юстиции Российской Федерации 9 февраля 2012 г., регистрационный N 23191) (далее - приказ ФСБ России N 796);

1.3.2. угроза нарушения целостности (подмены) и конфиденциальности персональных данных, содержащихся в запросе на выдачу квалифицированного сертификата, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10

Состава и содержания организационных и технических мер;

1.4. при создании и подписании удостоверяющим центром квалифицированного сертификата:

1.4.1. угроза нарушения целостности (подмены) квалифицированного сертификата, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 11 Требований к средствам удостоверяющего центра, утвержденных приказом ФСБ России N 796, при условии отсутствия подключения средств удостоверяющего центра к информационно-телекоммуникационной сети, доступ к которой не ограничен определенным кругом лиц;

1.4.2. угроза нарушения целостности (подмены) квалифицированного сертификата, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 Требований к средствам удостоверяющего центра, утвержденных приказом ФСБ России N 796, при условии подключения средств удостоверяющего центра к информационно-телекоммуникационной сети, доступ к которой не ограничен определенным кругом лиц;
(п. 1.4 в ред. Приказа Минцифры России от 31.01.2022 N 71)

1.5. при получении аккредитованным удостоверяющим центром от физического лица подтверждения ознакомления с информацией, содержащейся в выдаваемом ему квалифицированном сертификате, - угроза нарушения целостности (подмены) данных о подтверждении физическим лицом ознакомления с информацией, содержащейся в выдаваемом ему квалифицированном сертификате, при взаимодействии физического лица с удостоверяющим центром, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 Требовании к средствам электронной подписи, утвержденных приказом ФСБ России N 796;

1.6. при обработке в инфраструктуре аккредитованного удостоверяющего центра информации о подтверждении ознакомления физического лица с информацией, содержащейся в выдаваемом ему квалифицированном сертификате, - угроза нарушения целостности (подмены) данных о подтверждении физическим лицом ознакомления с информацией, содержащейся в выдаваемом ему квалифицированном сертификате, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 11 Требований к средствам удостоверяющего центра, утвержденных приказом ФСБ России N 796;

1.7. при направлении запроса на выдачу квалифицированного сертификата, при выдаче квалифицированного сертификата и при получении подтверждения ознакомления физическим лицом с информацией, содержащейся в выданном квалифицированном сертификате, - угроза нарушения доступности сервисов удостоверяющего центра, единой биометрической системы, единой системы идентификации и аутентификации.

2. Угрозы безопасности, актуальные при хранении ключа электронной подписи в аккредитованном удостоверяющем центре:

2.1. угрозы нарушения целостности (подмены, удаления) и конфиденциальности ключа электронной подписи, в том числе путем реализации целенаправленных действий с использованием следующих возможностей:

2.1.1. проведение целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемой информации или с целью создания условий для этого (далее - атака) извне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона);

2.1.2. проведение на этапах разработки (модернизации), производства, хранения, транспортировки средств электронной подписи (далее - средства ЭП), используемых для хранения ключа электронной подписи и этапе ввода в эксплуатацию средств ЭП (пусконаладочные работы) атаки путем внесения несанкционированных изменений в средства ЭП и (или) в компоненты аппаратных и программных средств, совместно с которыми функционируют средства ЭП и в совокупности представляющие среду функционирования средства ЭП (далее - СФ), которые способны повлиять на выполнение предъявляемых к средствам ЭП требований, в том числе с использованием вредоносных программ;

2.1.3. проведение атак на этапе эксплуатации средства ЭП на:

а) ключ электронной подписи;

б) аутентифицирующую и парольную информацию средства ЭП;

в) средство ЭП и его программные и аппаратные компоненты;

г) аппаратные средства, входящие в СФ, включая микросхемы с записанным микрокодом BIOS, осуществляющей инициализацию этих средств (далее - аппаратные компоненты СФ);

д) программные компоненты СФ;

е) помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы средства ЭП и СФ;

2.1.4. получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") информации об удостоверяющем центре, использующем средство ЭП:

а) общих сведений об удостоверяющем центре, использующем средство ЭП (состав, оператор, объекты, в которых размещены ресурсы удостоверяющего центра);

б) сведений об информационных технологиях, базах данных, автоматизированных системах, программном обеспечении, используемых удостоверяющим центром совместно со средством ЭП;

в) сведений о физических мерах защиты объектов, в которых размещены средства ЭП;

г) сведений о мерах по обеспечению контролируемой зоны объектов удостоверяющего центра, в котором используется средство ЭП;

д) сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на

которых реализованы средства ЭП и СФ;

е) документации на аппаратные и программные компоненты средства ЭП и СФ;

ж) общих сведений о защищаемой информации, используемой в процессе эксплуатации средства ЭП;

з) всех возможных данных, передаваемых в открытом виде по каналам связи, не защищенным от несанкционированного доступа (далее - НСД) к информации организационно-техническими мерами;

и) сведений о линиях связи, по которым передается защищаемая средством ЭП информация;

к) сведений обо всех проявляющихся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушениях правил эксплуатации средства ЭП и СФ;

л) сведений обо всех проявляющихся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправностях и сбоях аппаратных компонентов средства ЭП и СФ;

м) сведений, получаемых в результате анализа любых сигналов от аппаратных компонентов средства ЭП и СФ, которые может перехватить нарушитель;

2.1.5. применение специально разработанных автоматизированных систем и программного обеспечения;

2.1.6. использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки каналов распространения сигналов, сопровождающих функционирование средства ЭП и СФ;

2.1.7. проведение атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц;

2.1.8. использование аппаратных средств и программного обеспечения из состава средств удостоверяющего центра, используемых на местах эксплуатации средства ЭП (далее - штатные средства) и находящихся за пределами контролируемой зоны;

2.1.9. проведение атаки лицом при нахождении как вне пределов, так и в пределах контролируемой зоны;

2.1.10. использование штатных средств, ограниченное мерами, реализованными в удостоверяющем центре, использующем средство ЭП, и направленными на предотвращение и пресечение несанкционированных действий;

2.1.11. доступ к средствам вычислительной техники, на которых реализованы средства ЭП и СФ;

2.1.12. создание способов атак, подготовки и проведения атак с привлечением специалистов, имеющих опыт разработки и анализа средств ЭП, включая специалистов в области анализа

сигналов, сопровождающих функционирование средства ЭП и СФ;

2.1.13. проведение лабораторных исследований средства ЭП, используемого вне контролируемой зоны, в объеме, зависящем от мер, направленных на предотвращение и пресечение несанкционированных действий, реализованных удостоверяющим центром, использующим средство ЭП;

2.1.14. создание способов атак, подготовки и проведения атак с привлечением специалистов, имеющих опыт разработки и анализа средств ЭП, включая специалистов в области использования для реализации атак возможностей прикладного программного обеспечения, не описанных в документации на прикладное программное обеспечение и имеющих доступ к исходным текстам входящего в СФ прикладного программного обеспечения;

2.1.15. проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа средств ЭП и СФ;

2.2. угроза нарушения доступности ключа электронной подписи.

3. Угрозы безопасности, актуальные при использовании ключа электронной подписи в аккредитованном удостоверяющем центре:

3.1. при направлении поручения об использовании ключа электронной подписи (далее - поручение):

3.1.1. угроза нарушения целостности (подмены) поручения, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пунктах 2.1.1 - 2.1.8 настоящего Перечня;

3.1.2. угроза нарушения конфиденциальности персональных данных, содержащихся в поручении, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 приложения к приказу ФСБ России N 378;

3.2. при исполнении поручения аккредитованным удостоверяющим центром:

3.2.1. угроза нарушения целостности (подмены) ключа электронной подписи, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пунктах 2.1.1 - 2.1.15 настоящего Перечня;

3.2.2. угроза нарушения доступности ключа электронной подписи;

3.2.3. угроза отказа владельца сертификата ключа проверки электронной подписи от авторства поручения, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте в пунктах 2.1.1 - 2.1.8 настоящего Перечня;

3.2.4. угроза нарушения конфиденциальности подписываемой информации, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 Состава и содержания организационных и технических мер, а также угроза нарушения целостности подписываемой информации при ее подписании в аккредитованном удостоверяющем центре, в том числе с использованием возможностей, указанных в пунктах 2.1.1 - 2.1.15

настоящего Перечня;

3.2.5. угроза нарушения конфиденциальности информации, отображаемой физическому лицу при подписании электронного документа, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 Состава и содержания организационных и технических мер, а также угроза нарушения целостности (подмены) информации, отображаемой физическому лицу при подписании электронного документа, в том числе с использованием возможностей, указанных в пунктах 2.1.1 - 2.1.8 настоящего Перечня;

3.2.6. угроза нарушения целостности (подмены) информации о результате исполнения поручения, а также истории использования ключа электронной подписи в инфраструктуре удостоверяющем центре, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пунктах 2.1.1 - 2.1.15 настоящего Перечня;

3.2.7. угроза нарушения доступности информации о результате исполнения поручения, а также истории использования ключа электронной подписи.