О требованиях к созданию, развитию и функционированию трансграничного пространства доверия

Решение Совета Евразийской экономической комиссии от 5 декабря 2018 года № 96

В целях реализации пункта 18 Протокола об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза (приложение № 3 к Договору о Евразийском экономическом союзе от 29 мая 2014 года) Совет Евразийской экономической комиссии **решил:**

1. Утвердить прилагаемые:

Требования к созданию, развитию и функционированию трансграничного пространства доверия;

Положение о комиссии по проверке компонентов общей инфраструктуры документирования информации в электронном виде на соответствие требованиям к созданию, развитию и функционированию трансграничного пространства доверия.

2. Просить правительства государств – членов Евразийского экономического союза в месячный срок с даты вступления настоящего Решения в силу представить в Евразийскую экономическую комиссию кандидатуры на уровне заместителей руководителей уполномоченных органов и организаций (или начальников соответствующих самостоятельных подразделений либо их заместителей) для включения в состав комиссии по проверке компонентов общей инфраструктуры документирования информации в электронном виде на соответствие требованиям к созданию, развитию и функционированию трансграничного пространства доверия.

3. Настоящее Решение вступает в силу по истечении 30 календарных дней с даты его официального опубликования.

Члены Совета Евразийской экономической комиссии:

От Республики Армения	От Республики Беларусь	От Республики Казахстан	От Кыргызской Республики	От Российской Федерации
М. Григорян	И. Петришенко	А. Мамин	Ж. Разаков	А. Силуанов

УТВЕРЖДЕНЫ
Решением Совета
Евразийской экономической
комиссии
от 5 декабря 2018 г. № 96

ТРЕБОВАНИЯ
к созданию, развитию и функционированию трансграничного пространства доверия

I. Общие положения

1. Настоящие Требования разработаны в соответствии с пунктом 18 Протокола об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза (приложение № 3 к Договору о Евразийском экономическом союзе от 29 мая 2014 года) и устанавливают требования к созданию, развитию и функционированию трансграничного пространства доверия в рамках Евразийского экономического союза (далее – Союз).

2. Целью настоящих Требований является обеспечение взаимоприемлемого уровня доверия при межгосударственном обмене данными и электронными документами органов государственной власти государств – членов Союза (далее – государства-члены) между собой и с Евразийской экономической комиссией (далее – Комиссия), а также защищенности и надежности функционирования трансграничного пространства доверия в результате применения субъектами электронного взаимодействия в рамках Союза данных требований.

3. Требования к элементам трансграничного пространства доверия устанавливают правовые, организационные и технические условия обеспечения доверия при межгосударственном обмене данными и электронными документами, в том числе охватывают вопросы защиты информации.

4. Требования к элементам трансграничного пространства доверия определяются в соответствии с актуальными для таких элементов угрозами безопасности информации и действиями нарушителя.

5. Настоящие Требования не распространяются на какие-либо сервисы, элементы и компоненты, которые используются исключительно для целей внутригосударственного обмена данными и электронными документами.

6. Для целей настоящих Требований используются понятия, которые означают следующее:

"криптографический стандарт" – совокупность технических спецификаций, устанавливающих правила и алгоритмы преобразования информации с использованием криптографического ключа (криптографическое преобразование), в том числе формирования и проверки ЭЦП;

"межгосударственная комиссия" – комиссия, сформированная из представителей уполномоченных органов и Комиссии, выполняющая проверку компонентов общей

инфраструктуры документирования информации в электронном виде на соответствие настоящим Требованиям;

"общая инфраструктура документирования информации в электронном виде" – совокупность информационно-технологических и организационно-правовых мероприятий, правил и решений, реализуемых в целях придания юридической силы электронным документам, используемым в рамках Союза;

"операторы общей инфраструктуры документирования информации в электронном виде" – Комиссия и уполномоченные органы или определенные ими в соответствии с законодательством государств-членов организации, предоставляющие услуги и осуществляющие функции в рамках трансграничного пространства доверия в соответствии с настоящими Требованиями;

"проверка элемента общей инфраструктуры документирования информации в электронном виде" – комплекс мероприятий, в результате которых документально подтверждается соответствие настоящим Требованиям элемента, входящего в состав государственного или интеграционного компонента общей инфраструктуры документирования информации в электронном виде, а также мер и способов обеспечения защиты информации, реализуемых оператором компонента общей инфраструктуры документирования информации в электронном виде в отношении такого элемента;

"сертификат ключа проверки ЭЦП" – электронный документ, изданный удостоверяющим центром, подписанный ЭЦП удостоверяющего центра с использованием ключа ЭЦП и содержащий информацию, подтверждающую принадлежность указанного в сертификате ключа проверки ЭЦП определенному участнику обмена электронными документами, и иную информацию, предусмотренную соответствующими криптографическими стандартами и настоящими Требованиями;

"служба доверенной третьей стороны" – совокупность сервисов доверенной третьей стороны, функционирующих в составе интеграционного сегмента Комиссии и национальных сегментов интегрированной информационной системы Союза, обеспечивающих единое трансграничное пространство доверия ЭЦП при электронной форме взаимодействия субъектов средствами интегрированной информационной системы Союза;

"средства доверенной третьей стороны" – программные и (или) аппаратные средства, используемые для реализации функций доверенной третьей стороны;

"средства удостоверяющего центра" – программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

"средства ЭЦП" – криптографические средства, используемые для реализации хотя бы одной из следующих функций: создание ЭЦП, проверка ЭЦП, создание ключа ЭЦП и создание ключа проверки ЭЦП;

"удостоверяющий центр" – уполномоченный орган или организация, обеспечивающие в соответствии с актами Комиссии, законодательством государства-члена предоставление услуг по изданию, распространению, хранению сертификатов ключей проверки ЭЦП и проверки действительности этих сертификатов;

"удостоверяющий центр Комиссии" – удостоверяющий центр, предназначенный для обеспечения сертификатами ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии;

"удостоверяющий центр службы доверенной третьей стороны" – удостоверяющий центр, предназначенный для обеспечения сертификатами ключей проверки ЭЦП уполномоченных доверенных третьих сторон интеграционного и национальных сегментов интегрированной информационной системы Союза;

"уполномоченный орган" – орган государственной власти государства-члена или определенная им организация, наделенные полномочиями по реализации государственной политики в отдельных сферах;

"штамп времени" – реквизит электронного документа, удостоверяющий дату и время создания электронного документа;

"электронная цифровая подпись (электронная подпись)", "ЭЦП" – информация в электронном виде, которая присоединена к другой информации в электронном виде или иным образом связана с такой информацией, служит для контроля целостности и подлинности этой информации, обеспечивает невозможность отказа от авторства, вырабатывается путем применения в отношении данной информации криптографического преобразования с использованием закрытого (личного) ключа (ключа ЭЦП) и проверяется с использованием открытого ключа (ключа проверки ЭЦП).

II. Создание, развитие и функционирование трансграничного пространства доверия

7. Создание, развитие и функционирование трансграничного пространства доверия обеспечивается Комиссией и уполномоченными органами в соответствии с Концепцией использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов, утвержденной Решением Совета Евразийской экономической комиссии от 18 сентября 2014 г. № 73, Стратегией развития трансграничного пространства доверия, утвержденной Решением Коллегии Евразийской экономической комиссии от 27 сентября 2016 г. № 105, Положением об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической

комиссией, утвержденным Решением Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125, а также с иными актами Комиссии по вопросам создания, развития и функционирования трансграничного пространства доверия.

8. Сведения о соответствующих настоящим Требованиям элементах, входящих в состав государственных и интеграционного компонентов общей инфраструктуры документирования информации в электронном виде (в том числе сведения об операторах таких элементов), включаются в перечень элементов общей инфраструктуры документирования информации в электронном виде, утверждаемый Комиссией на основании заключений межгосударственной комиссии.

9. В целях обеспечения развития и контроля функционирования трансграничного пространства доверия в рамках национальных сегментов государств-членов интегрированной информационной системы Союза (далее – интегрированная система) государствами-членами определяются уполномоченные органы для осуществления контроля за соблюдением требований к правовым, организационным, техническим условиям обеспечения трансграничного пространства доверия, в том числе касающихся защиты информации государственных компонентов общей инфраструктуры документирования информации в электронном виде.

10. Общая инфраструктура документирования информации в электронном виде состоит из государственных компонентов и интеграционного компонента.

11. Оператором интеграционного компонента общей инфраструктуры документирования информации в электронном виде выступает Комиссия.

12. Операторами государственных компонентов общей инфраструктуры документирования информации в электронном виде выступают уполномоченные органы.

13. Субъектами электронного взаимодействия в рамках Союза являются государственные органы, физические или юридические лица, взаимодействующие в рамках отношений, возникающих в процессе составления, отправления, передачи, получения, хранения и использования электронных документов и информации в электронном виде.

14. При электронном взаимодействии в рамках Союза доверие между субъектами электронного взаимодействия обеспечивается операторами общей инфраструктуры документирования информации в электронном виде, осуществляющими функции и предоставляющими услуги в рамках трансграничного пространства доверия в соответствии с настоящими Требованиями.

15. Элементы трансграничного пространства доверия, входящие в состав государственных компонентов и интеграционного компонента общей инфраструктуры документирования информации в электронном виде, должны соответствовать описанию согласно приложению № 1.

16. Элементы трансграничного пространства доверия эксплуатируются операторами общей инфраструктуры документирования информации в электронном виде для предоставления услуг и осуществления функций в рамках трансграничного пространства доверия в соответствии с настоящими Требованиями.

17. Оператор общей инфраструктуры документирования информации в электронном виде может обеспечивать эксплуатацию нескольких элементов трансграничного пространства доверия.

18. Операторы общей инфраструктуры документирования информации в электронном виде несут ответственность за ущерб, причиненный субъектам электронного взаимодействия в результате:

а) неисполнения или ненадлежащего исполнения обязанностей, предусмотренных настоящими Требованиями;

б) неисполнения или ненадлежащего исполнения обязанностей, предусмотренных законодательством государства-члена, в государственный компонент которого они входят.

19. Комиссия и государства-члены устанавливают согласованные требования к ответственности за нарушение настоящих Требований в части деятельности операторов общей инфраструктуры документирования информации в электронном виде.

20. Проверка элементов общей инфраструктуры документирования информации в электронном виде осуществляется в соответствии с Положением о комиссии по проверке компонентов общей инфраструктуры документирования информации в электронном виде на соответствие требованиям к созданию, развитию и функционированию трансграничного пространства доверия, утвержденным Решением Совета Евразийской экономической комиссии от 5 декабря 2018 г. № 96.

III. Общая инфраструктура документирования информации в электронном виде

1. Требования к удостоверяющему центру службы доверенной третьей стороны

21. Удостоверяющий центр службы доверенной третьей стороны осуществляет деятельность по созданию сертификатов ключей проверки ЭЦП, предназначенных для организации электронного взаимодействия доверенной третьей стороны, функционирующей в составе интеграционного сегмента Комиссии интегрированной системы (далее – доверенная третья сторона Комиссии), и уполномоченных доверенных третьих сторон, функционирующих в национальных сегментах государств-членов интегрированной системы (далее – доверенные третьи стороны государств-членов).

22. Владельцами сертификатов ключей проверки ЭЦП, выдаваемых удостоверяющим центром службы доверенной третьей стороны, являются:

доверенная третья сторона Комиссии;

доверенные третьи стороны государств-членов.

23. Удостоверяющий центр службы доверенной третьей стороны должен функционировать в соответствии с международными рекомендациями по построению инфраструктуры открытых ключей (Public Key Infrastructure) и согласованными с уполномоченными органами требованиями.

24. Удостоверяющий центр службы доверенной третьей стороны для создания сертификатов ключей проверки ЭЦП должен использовать средства удостоверяющего центра, соответствующие требованиям согласно приложению № 2. Перед использованием указанных средств их соответствие указанным установленным требованиям должно быть подтверждено уполномоченными органами страны пребывания Комиссии в порядке, установленном ее законодательством. Перед использованием средств удостоверяющего центра, разработанных для удостоверяющего центра службы доверенной третьей стороны в рамках проекта по совместной разработке специализированных средств криптографической защиты информации Союза, их соответствие указанным установленным требованиям должно быть подтверждено уполномоченными органами всех государств-членов в порядке, установленном их законодательством.

25. Требования к функционированию удостоверяющего центра службы доверенной третьей стороны устанавливаются с учетом утверждаемых Комиссией моделей угроз безопасности информации и действий нарушителя.

26. Удостоверяющий центр службы доверенной третьей стороны должен обеспечивать выполнение следующих основных функций:

а) регистрация доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов;

б) создание и выдача сертификатов ключей проверки ЭЦП по запросам доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов;

в) определение полномочий лиц, выступающих от имени доверенной третьей стороны Комиссии или доверенных третьих сторон государств-членов при обращении за получением сертификата ключа проверки ЭЦП, и хранение информации об указанных полномочиях в соответствии с утверждаемыми Комиссией документами, регламентирующими функционирование удостоверяющего центра службы доверенной третьей стороны;

г) подтверждение владения ключом ЭЦП, который соответствует ключу проверки ЭЦП, указанному соответствующей доверенной третьей стороной в запросе на

создание и получение сертификата ключа проверки ЭЦП, и отказ в создании указанного сертификата в случае отрицательного результата при подтверждении владения данным ключом;

д) установление сроков действия сертификатов ключей проверки ЭЦП. Сертификат ключа проверки ЭЦП действует с момента его выдачи, если иная дата начала действия такого сертификата не указана в самом сертификате, при этом информация о сертификате ключа проверки ЭЦП должна быть внесена удостоверяющим центром службы доверенной третьей стороны в реестр выданных, прекративших действие и аннулированных сертификатов ключей проверки ЭЦП (далее – реестр сертификатов) не позднее указанной в нем даты начала действия такого сертификата;

е) прекращение действия и аннулирование сертификатов ключей проверки ЭЦП;

ж) ведение реестра сертификатов с включением в него информации, содержащейся в выданных удостоверяющим центром службы доверенной третьей стороны сертификатах ключей проверки ЭЦП, а также информации о дате прекращения действия или аннулирования таких сертификатов и об основаниях прекращения действия или аннулирования;

з) ведение списка прекративших действие и аннулированных сертификатов ключей проверки ЭЦП (далее – список отозванных сертификатов);

и) уведомление владельца сертификата ключа проверки ЭЦП об аннулировании его сертификата до внесения соответствующих изменений в реестр сертификатов и список отозванных сертификатов;

к) проверка уникальности ключей проверки ЭЦП в реестре сертификатов и отказ в создании сертификата ключа проверки ЭЦП в случае отрицательного результата проверки уникальности ключа проверки ЭЦП, указанного в запросе доверенной третьей стороны Комиссии или доверенной третьей стороны государства-члена;

л) актуализация информации, содержащейся в реестре сертификатов и списке отозванных сертификатов, а также ее защита от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий;

м) хранение информации, внесенной в реестр сертификатов, в течение всего срока деятельности удостоверяющего центра службы доверенной третьей стороны;

н) доступ на безвозмездной основе доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов к реестру сертификатов с использованием средств интегрированной системы в любое время;

о) осуществление проверок ЭЦП по обращениям доверенной третьей стороны Комиссии или доверенных третьих сторон государств-членов, созданных с использованием выданных им сертификатов ключей проверки ЭЦП;

п) создание штампов времени на квитанциях доверенной третьей стороны Комиссии и квитанциях доверенных третьих сторон государств-членов, содержащих результаты проверки ЭЦП, которыми подписаны электронные документы, при

обращении таких доверенных третьих сторон с целью подтверждения времени создания электронных документов и их подписания соответствующей ЭЦП;

р) осуществление иных, связанных с использованием ЭЦП, функций.

27. Для функционирования удостоверяющего центра службы доверенной третьей стороны Комиссия во взаимодействии с уполномоченными органами разрабатывает и утверждает технические, технологические, методические и организационные документы, предусматривающие детализацию требований к удостоверяющему центру службы доверенной третьей стороны.

28. Настоящие Требования и требования, содержащиеся в актах, утверждаемых Комиссией для обеспечения функционирования удостоверяющего центра службы доверенной третьей стороны, применяются межгосударственной комиссией для проверки удостоверяющего центра службы доверенной третьей стороны в рамках проверки интеграционного компонента общей инфраструктуры документирования информации в электронном виде.

2. Требования к службе доверенной третьей стороны и входящим в ее состав доверенным третьим сторонам

29. Служба доверенной третьей стороны является функциональной частью интегрированной системы.

30. Служба доверенной третьей стороны должна включать в себя сервисы доверенной третьей стороны Комиссии и сервисы доверенных третьих сторон государств-членов.

31. Каждая из доверенных третьих сторон, сервисы которых входят в состав службы доверенной третьей стороны, в соответствии с пунктом 21 Протокола об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза должна выполнять следующие задачи:

а) осуществление легализации (подтверждение подлинности) электронных документов и ЭЦП субъектов информационного взаимодействия в фиксированный момент времени;

б) обеспечение гарантий доверия в межгосударственном (трансграничном) обмене электронными документами;

в) обеспечение правомерности применения ЭЦП в исходящих и (или) входящих электронных документах в соответствии с законодательством государств-членов и актами Комиссии.

32. Доверенная третья сторона Комиссии и доверенные третьи стороны государств-членов должны обеспечивать функционирование в своем составе

следующей совокупности сервисов, реализуемых с использованием средств доверенной третьей стороны:

а) сервис подтверждения подлинности (проверка ЭЦП, действительности и соответствия сертификата ключа проверки ЭЦП установленным требованиям, получение результата от сервиса проверки полномочий и формирование квитанций с результатом проверки подлинности электронного документа);

б) сервис проверки полномочий (проверка полномочий субъекта электронного взаимодействия, сформировавшего и подписавшего электронный документ в национальном сегменте государства-члена или интеграционном сегменте Комиссии интегрированной системы);

в) сервис штампа времени (создание штампов времени для электронных документов , входящих в национальный сегмент государства-члена или интеграционный сегмент Комиссии интегрированной системы, и квитанций с результатом проверки подлинности электронного документа);

г) сервис хранения данных (документирование выполняемых доверенной третьей стороной операций);

д) сервис предоставления информации (об операциях доверенной третьей стороны по запросам уполномоченных органов и Комиссии).

33. Сервисы, реализуемые средствами доверенной третьей стороны Комиссии или средствами доверенных третьих сторон государств-членов, должны соответствовать настоящим Требованиям, Положению об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, а также актам Комиссии, касающимся вопросов функционирования доверенных третьих сторон.

34. Доверенная третья сторона Комиссии и доверенные третьи стороны государств-членов при выполнении своих функций должны обеспечить соблюдение в совокупности следующих основных условий:

а) обеспечение конфиденциальности ключа ЭЦП, ключ проверки которого содержится в выданном удостоверяющим центром службы доверенной третьей стороны сертификате ключа проверки ЭЦП;

б) уведомление удостоверяющего центра службы доверенной третьей стороны, доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов о нарушении конфиденциальности ключа ЭЦП, предназначенного для электронного взаимодействия в рамках Союза, в течение не более чем 12 часов с момента получения информации о таком нарушении;

в) прекращение использования ключа ЭЦП, предназначенного для электронного взаимодействия в рамках Союза, при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

г) использование ключа ЭЦП, предназначенного для электронного взаимодействия в рамках Союза, исключительно для подписания квитанций с результатами проверки ЭЦП электронного документа;

д) использование для создания и проверки ЭЦП, создания ключей ЭЦП и ключей проверки ЭЦП, предназначенных для электронного взаимодействия в рамках Союза, средств криптографической защиты информации, реализующих криптографические алгоритмы, определенные в соответствии с Решением Коллегии Евразийской экономической комиссии от 2 июня 2016 г. № 49 (ДСП), до реализации проекта по совместной разработке специализированных средств криптографической защиты информации Союза;

е) при проверке ЭЦП в электронных документах проверка соблюдения в совокупности следующих условий:

целостность данных, подписываемых ЭЦП, не нарушена;

ЭЦП выработана с использованием ключа ЭЦП, соответствующий сертификат ключа проверки ЭЦП имеется в распоряжении доверенной третьей стороны на момент начала проверки либо получен доверенной третьей стороной в процессе выполнения процедур проверки;

сертификат ключа проверки ЭЦП действителен на момент подписания электронного документа;

каждый сертификат ключа проверки ЭЦП из цепочки сертификатов ключей проверки ЭЦП удостоверяющих центров действителен на момент подписания;

ж) документирование и хранение в течение периода, установленного актами Комиссии или законодательством государств-членов, всей необходимой информации относительно всех проводимых проверок ЭЦП в электронных документах для обеспечения непрерывности оказания услуг и представления (в случае необходимости) доказательств в суде. Хранение указанной информации может осуществляться в электронном виде.

35. Доверенная третья сторона Комиссии должна использовать средства доверенной третьей стороны и средства ЭЦП в их составе, соответствующие требованиям согласно приложению № 3.

36. Комиссия для обеспечения функционирования доверенной третьей стороны Комиссии разрабатывает во взаимодействии с уполномоченными органами и утверждает технические, технологические, методические и организационные документы, предусматривающие детализацию компонентов и требований к доверенной третьей стороне интеграционного сегмента Комиссии интегрированной системы.

37. Требования к взаимодействию доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов между собой и с удостоверяющим

центром службы доверенной третьей стороны устанавливаются с учетом соответствующих утверждаемых Комиссией моделей угроз безопасности информации и действий нарушителя.

38. Для обеспечения функционирования доверенных третьих сторон государств-членов уполномоченные органы разрабатывают и утверждают в соответствии с законодательством государств-членов и актами Комиссии технические, технологические, методические и организационные документы, предусматривающие детализацию компонентов и требований к доверенным третьим сторонам государств-членов.

39. Комиссия осуществляет передачу программных и аппаратных средств криптографической защиты информации, разработанных в рамках работ по созданию и развитию интегрированной системы и предназначенных для функционирования доверенных третьих сторон, уполномоченным органам заинтересованных государств-членов для использования в составе национальных сегментов в порядке, утверждаемом Комиссией.

40. Настоящие Требования и требования, содержащиеся в документах, утверждаемых государствами-членами и Комиссией для обеспечения функционирования доверенных третьих сторон, используются межгосударственной комиссией для проверки службы доверенной третьей стороны и входящих в ее состав доверенных третьих сторон в рамках проверки компонентов общей инфраструктуры документирования информации в электронном виде.

3. Требования к удостоверяющему центру Комиссии и удостоверяющим центрам государств-членов, обеспечивающим субъектов электронного взаимодействия в рамках Союза сертификатами ключей проверки ЭЦП

41. Удостоверяющий центр Комиссии и удостоверяющие центры государств-членов , обеспечивающие субъектов электронного взаимодействия сертификатами ключей ЭЦП для электронного взаимодействия в рамках Союза, в соответствии со Стратегией развития трансграничного пространства доверия, являются элементами трансграничного пространства доверия и входят в состав компонентов общей инфраструктуры документирования информации в электронном виде.

42. К электронному взаимодействию в рамках Союза допускаются только уполномоченные в соответствии с законодательством государств-членов или актами Комиссии удостоверяющие центры, сведения о которых включены в перечень элементов общей инфраструктуры документирования информации в электронном виде.

43. Удостоверяющий центр Комиссии и удостоверяющие центры государств-членов должны функционировать в соответствии с международными рекомендациями по

построению инфраструктуры открытых ключей (Public Key Infrastructure) и выполнять минимально необходимые требования, указанные в пункте 49 настоящих Требований.

44. Требования к деятельности удостоверяющих центров государств-членов, в том числе по защите информации, устанавливаются с учетом актуальных угроз безопасности информации и действий нарушителя в соответствии с законодательством государств-членов в сфере защиты информации.

45. Требования к деятельности удостоверяющего центра Комиссии устанавливаются с учетом утверждаемой Комиссией модели угроз безопасности информации и действий нарушителя в удостоверяющем центре Комиссии.

Удостоверяющий центр Комиссии для создания сертификатов ключей проверки ЭЦП должен использовать средства ЭЦП и средства удостоверяющего центра, соответствующие требованиям согласно приложению № 4. Перед использованием указанных средств их соответствие указанным требованиям должно быть подтверждено уполномоченными органами страны пребывания Комиссии в порядке, установленном ее законодательством.

46. Удостоверяющие центры государств-членов создают сертификаты ключей проверки ЭЦП в соответствии с законодательством соответствующего государства-члена.

47. Удостоверяющий центр Комиссии создает сертификаты ключей проверки ЭЦП в соответствии с настоящими Требованиями.

48. Для создания и проверки ЭЦП в государствах-членах должны использоваться сертифицированные (получившие подтверждение соответствия установленным требованиям) в соответствии с их законодательством средства ЭЦП.

49. Для функционирования удостоверяющих центров в соответствии с законодательством государств-членов устанавливаются следующие минимально необходимые требования:

а) обеспечение проверки личности субъектов электронного взаимодействия при выдаче сертификатов ключей проверки ЭЦП. Проверка личности получателя сертификата осуществляется либо непосредственно удостоверяющим центром, либо с привлечением третьего лица (центра регистрации и т. п.), если это предусмотрено законодательством государств-членов;

б) публикация в информационно-коммуникационной сети "Интернет" в режиме общего доступа информации об условиях пользования услугами удостоверяющего центра, включая любые ограничения по их использованию;

в) выдача субъектам электронного взаимодействия в соответствии с законодательством государств-членов или актами Комиссии сертификатов ключей проверки ЭЦП, соответствующих требованиям, утверждаемым Комиссией;

г) своевременное предоставление всем субъектам электронного взаимодействия информации о статусе (актуальности) всех выданных сертификатов ключей проверки

ЭЦП. Такая информация должна быть доступна в любое время, в том числе и после прекращения действия сертификата ключа проверки ЭЦП, и предоставляться автоматизированным способом;

д) оперативное (в день получения запроса в соответствии с режимом работы удостоверяющего центра) внесение информации в реестр сертификатов и список отозванных сертификатов при отзыве сертификатов. Сертификат считается отозванным с момента публикации списка отозванных сертификатов, содержащего информацию о соответствующем статусе (актуальности) такого сертификата и доступного в любое время субъектам электронного взаимодействия;

е) документирование и хранение не менее 15 лет всей необходимой информации относительно выдачи, получения и изменения статусов (актуальности) сертификатов ключей проверки ЭЦП (в том числе после прекращения деятельности по обеспечению субъектов электронного взаимодействия в рамках Союза сертификатами ключей ЭЦП) для обеспечения непрерывности оказания услуг и представления (при необходимости) доказательств в суде. Хранение указанной информации может осуществляться в электронном виде;

ж) обеспечение конфиденциальности, целостности созданных и хранимых удостоверяющим центром криптографических ключей;

з) информирование уполномоченных органов о намерении прекратить деятельность по обеспечению субъектов электронного взаимодействия в рамках Союза сертификатами ключей ЭЦП или иных случаях прекращения деятельности.

50. Для функционирования удостоверяющих центров государств-членов уполномоченные органы разрабатывают и утверждают технические, технологические, методические и организационные документы в соответствии с законодательством своих государств-членов.

51. Комиссия для обеспечения функционирования удостоверяющего центра Комиссии разрабатывает во взаимодействии с уполномоченными органами и утверждает технические, технологические, методические и организационные документы.

52. Настоящие Требования и требования, содержащиеся в документах, утверждаемых государствами-членами и Комиссией для обеспечения функционирования удостоверяющих центров, используются межгосударственной комиссией для проверки службы доверенной третьей стороны в рамках проверки компонентов общей инфраструктуры документирования информации в электронном виде.

4. Требования к инфраструктуре обеспечения взаимодействия информационных систем и ресурсов государств-членов и Комиссии при межгосударственном обмене данными и электронными документами

53. Инфраструктура обеспечения взаимодействия информационных систем и ресурсов государств-членов и Комиссии при межгосударственном обмене данными и электронными документами состоит из интеграционной платформы интегрированной системы и систем межведомственного информационного взаимодействия государств-членов, выполняющих функции в соответствии с техническим заданием на создание интегрированной информационной системы Евразийского экономического союза, утвержденным Решением Коллегии Евразийской экономической комиссии от 12 октября 2015 г. № 137.

54. Интеграционная платформа интегрированной системы состоит из интеграционных шлюзов, подсистемы синхронизации данных, транспортной подсистемы, подсистемы взаимодействия с внешними информационными системами и подсистемы сопряжения.

55. Интеграционная платформа интегрированной системы включает в себя интеграционные шлюзы государств-членов, функционирующие в составе национальных сегментов государств-членов интегрированной системы, и интеграционный шлюз Комиссии, функционирующий в составе интеграционного сегмента Комиссии интегрированной системы.

56. Интеграционная платформа интегрированной системы в рамках подсистемы синхронизации данных должна обеспечивать информационное взаимодействие подсистем интегрированной системы в рамках интеграционного сегмента Комиссии.

57. Интеграционная платформа интегрированной системы в рамках транспортной подсистемы должна обеспечивать гарантированную доставку электронных сообщений между компонентами интеграционной платформы с использованием очередей сообщений.

58. Интеграционная платформа интегрированной системы в рамках подсистемы взаимодействия с внешними информационными системами должна обеспечивать единую точку подключения к интеграционной платформе при организации информационного взаимодействия с информационными системами интеграционных объединений, международных организаций и государств, не являющихся членами Союза (далее – внешние информационные системы).

59. Интеграционная платформа интегрированной системы в рамках подсистемы сопряжения должна обеспечивать взаимодействие между интеграционным шлюзом интеграционной платформы и применяемыми в государствах-членах системами межведомственного информационного взаимодействия (для интеграционных шлюзов национальных сегментов государств-членов, реализованных на основе типового интеграционного шлюза), а также между подсистемой взаимодействия с внешними информационными системами.

60. Обмен информацией между интеграционным шлюзом интеграционного сегмента Комиссии интегрированной системы и подсистемой синхронизации данных, а также обмен информацией между интеграционными шлюзами национальных сегментов государств-членов интегрированной системы, между интеграционным шлюзом интеграционного сегмента Комиссии интегрированной системы и интеграционными шлюзами национальных сегментов государств-членов интегрированной системы должен выполняться в соответствии с Правилами электронного обмена данными в интегрированной информационной системе внешней и взаимной торговли, утвержденными Решением Коллегии Евразийской экономической комиссии от 27 января 2015 г. № 5.

61. Вычислительные ресурсы интеграционных шлюзов национальных сегментов государств-членов и интеграционного шлюза Комиссии должны обеспечить уровень своей доступности 24 часа в сутки, 7 дней в неделю, 365 (366) дней в году, за исключением периодов технического обслуживания.

62. Интеграционная платформа интегрированной системы должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверным форматом или недопустимыми значениями входных данных. В указанных случаях интеграционная платформа интегрированной системы должна обеспечивать сохранение информации об аварийных ситуациях в соответствующих журналах, после чего возвращаться в рабочее состояние, предшествовавшее поступлению некорректных входных данных.

63. Интеграционные шлюзы и системы межведомственного информационного взаимодействия государств-членов должны обеспечивать защиту передаваемых данных

.

64. Операторы интеграционных шлюзов должны ограничить круг сотрудников, имеющих доступ к передаваемым данным, при этом доступ к данным должен предоставляться таким сотрудникам только для расследования нештатных (конфликтных) ситуаций.

65. Интеграционные шлюзы и системы межведомственного информационного взаимодействия государств-членов должны обеспечивать идентификацию и аутентификацию отправителей и получателей передаваемых данных.

66. Интеграционные шлюзы должны обеспечивать документирование информации относительно операций, проведенных с передаваемыми и получаемыми данными, в том числе с электронными документами, и ее хранение в течение периода, установленного законодательством государств-членов или актами Комиссии, в том числе для возможности представления доказательств в суде.

67. Сервисы интеграционных шлюзов, используемые для реализации обмена электронными документами при трансграничном взаимодействии органов государственной власти государств-членов между собой и с Комиссией, должны соответствовать настоящим Требованиям, требованиям Положения об обмене

электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией и иным актам Комиссии по вопросам функционирования интеграционных шлюзов.

5. Требования к инфраструктуре и системам обеспечения защиты информации

68. Для защиты интеграционного сегмента Комиссии интегрированной системы Комиссией используется подсистема информационной безопасности, предназначенная в соответствии с техническим заданием на создание интегрированной информационной системы Евразийского экономического союза обеспечивать конфиденциальность, целостность и доступность данных при их обработке и хранении в интеграционном сегменте Комиссии, а также при их передаче по каналам связи при взаимодействии с национальными сегментами государств-членов интегрированной системы.

69. Для защиты национальных сегментов государств-членов интегрированной системы уполномоченными органами должны обеспечиваться создание и внедрение в государствах-членах подсистем защиты информации национальных сегментов государств-членов, предназначенных в соответствии с техническим заданием на создание интегрированной системы обеспечивать конфиденциальность, целостность и доступность данных при их создании, обработке и хранении в национальном сегменте государства-члена, а также при их передаче по каналам связи при взаимодействии с интеграционным сегментом Комиссии и национальными сегментами других государств-членов интегрированной системы. Для обеспечения конфиденциальности, целостности, доступности и сохранности информации в национальном сегменте государства-члена интегрированной системы принимается и реализуется комплекс правовых, организационных и техническим мер защиты информации в соответствии с законодательством соответствующего государства-члена.

70. Операторы государственных компонентов общей инфраструктуры документирования информации в электронном виде должны принимать технические и организационные меры, направленные на нейтрализацию угроз для выполняемых ими функций. Указанные меры должны реализовываться на основе определения угроз безопасности информации и действий нарушителя, отраженных в документах (заданиях по безопасности, моделях угроз и др.), разрабатываемых в соответствии с законодательством государств-членов.

71. Операторы государственных компонентов общей инфраструктуры документирования информации в электронном виде должны обеспечивать наличие у своих сотрудников необходимых знаний, надежности, лояльности, опыта и квалификации, а также прохождение ими достаточной подготовки в области защиты информации в соответствии с законодательством соответствующего государства-члена.

72. В случае выявления любых фактов нарушения конфиденциальности, целостности и доступности информации элементов трансграничного пространства доверия операторы государственных компонентов общей инфраструктуры документирования информации в электронном виде должны незамедлительно уведомить об этом свой уполномоченный орган.

Если нарушение защиты информации затрагивает 2 или более государства-члена, получивший такое уведомление уполномоченный орган уведомляет об этом уполномоченные органы других государств-членов и межгосударственную комиссию.

73. Меры и способы обеспечения защиты информации, реализуемые операторами государственных компонентов общей инфраструктуры документирования информации в электронном виде в отношении элементов трансграничного пространства доверия и предоставляемых ими сервисов, должны соответствовать требованиям согласно приложению № 5.

УТВЕРЖДЕНО
Решением Совета
Евразийской экономической
комиссии
от 5 декабря 2018 г. № 96

ПОЛОЖЕНИЕ
о комиссии по проверке компонентов общей инфраструктуры документирования информации в электронном виде на соответствие требованиям к созданию, развитию и функционированию трансграничного пространства доверия

1. Комиссия по проверке компонентов общей инфраструктуры документирования информации в электронном виде на соответствие требованиям к созданию, развитию и функционированию трансграничного пространства доверия (далее – межгосударственная комиссия) создается в соответствии с пунктом 18 Протокола об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза (приложение № 3 к Договору о Евразийском экономическом союзе от 29 мая 2014 года).

2. Понятия, применяемые в настоящем Положении, используются в значениях, определенных Требованиями к созданию, развитию и функционированию трансграничного пространства доверия, утвержденными Решением Совета Евразийской экономической комиссии от 5 декабря 2018 г. № 96 (далее – Требования).

3. В состав межгосударственной комиссии включаются должностные лица Евразийской экономической комиссии (далее – Комиссия) и представители уполномоченных органов государств – членов Евразийского экономического союза (

далее соответственно – уполномоченные органы, государства-члены), к компетенции которых относятся вопросы создания национальных сегментов государств-членов интегрированной информационной системы Евразийского экономического союза, обеспечения информационной безопасности и юридической значимости электронных документов, используемых в рамках трансграничного электронного документооборота, с учетом равного представительства государств-членов.

4. Состав межгосударственной комиссии утверждается распоряжением Совета Комиссии.

5. Председателем межгосударственной комиссии является член Коллегии Комиссии , к компетенции которого относятся вопросы информатизации и информационно-коммуникационных технологий.

Председатель межгосударственной комиссии осуществляет общее руководство работой межгосударственной комиссии.

6. По решению межгосударственной комиссии в ее составе могут быть сформированы подкомиссии, а также рабочие и экспертные группы.

7. Решения межгосударственной комиссии принимаются консенсусом.

8. Порядок проведения заседаний межгосударственной комиссии, формирования подкомиссий, рабочих и экспертных групп, привлечения экспертов, принятия межгосударственной комиссией решений и их оформления, а также формы документов , принимаемых межгосударственной комиссией, устанавливаются регламентом работы межгосударственной комиссии, определяемым Комиссией.

9. Межгосударственная комиссия выполняет следующие основные функции:

а) по предложениям уполномоченных органов и Комиссии формирует и утверждает план-график проведения проверок государственных и интеграционного компонентов общей инфраструктуры документирования информации в электронном виде на соответствие Требованиям;

б) разрабатывает и представляет для рассмотрения Коллегией Комиссии методические документы по проведению проверок на соответствие Требованиям элементов, входящих в состав государственных и интеграционного компонентов общей инфраструктуры документирования информации в электронном виде, а также мер и способов обеспечения защиты информации, реализуемых операторами общей инфраструктуры документирования информации в электронном виде в отношении таких элементов (далее – проверки);

в) проводит на основании заявлений уполномоченных органов и Комиссии проверки в соответствии пунктом 11 данного Положения;

г) подготавливает заключение о необходимости включения сведений об элементах, входящих в состав государственных и интеграционного компонентов общей инфраструктуры документирования информации в электронном виде, в том числе сведений об операторах таких элементов, в перечень элементов общей инфраструктуры

документирования информации в электронном виде, утверждаемый Комиссией (далее – перечень);

д) оценивает перечень на предмет соответствия приложению № 1 к Требованиям, в том числе достаточности включенных в перечень сведений для осуществления межгосударственного обмена данными и электронными документами органов государственной власти государств-членов между собой и с Комиссией.

10. Проверки проводятся в порядке и сроки, которые определяются регламентом работы межгосударственной комиссии.

11. Проверка выполняется последовательно в 2 этапа:

I этап – оценка соответствия элемента, входящего в состав государственного или интеграционного компонента общей инфраструктуры документирования информации в электронном виде Требованиям, осуществляемая на основании сведений, представленных уполномоченным органом или Комиссией в составе заявления о включении такого элемента в перечень (далее – заявление);

II этап – подготовка заключения о необходимости включения в перечень элемента, входящего в состав государственного или интеграционного компонента общей инфраструктуры документирования информации в электронном виде.

12. Порядок представления заявлений и состав указываемых в нем сведений определяются межгосударственной комиссией.

13. В случае выявления несоответствия представленных в составе заявления сведений либо их неполноты межгосударственная комиссия направляет в уполномоченный орган или Комиссию соответствующий акт.

По результатам рассмотрения акта уполномоченный орган или Комиссия представляет в межгосударственную комиссию соответствующие сведения либо отзывает заявление.

14. Межгосударственная комиссия подготавливает заключения о необходимости исключения из перечня элементов, входящих в состав государственных или интеграционного компонентов общей инфраструктуры документирования информации в электронном виде, на основании ходатайств представлявших заявления уполномоченных органов или Комиссии.

15. Заключения о необходимости включения в перечень элементов, входящих в состав государственных или интеграционного компонентов общей инфраструктуры документирования информации в электронном виде, или исключения их из перечня подписываются председателем межгосударственной комиссии и направляются в Комиссию.

16. В случае выявления несоответствия перечня приложению № 1 к Требованиям, в том числе недостаточности включенных в перечень сведений для осуществления межгосударственного обмена данными и электронными документами органов государственной власти государств-членов между собой и с Комиссией,

межгосударственная комиссия уведомляет об этом уполномоченные органы или Комиссию и запрашивает недостающие сведения.

17. В случае прекращения полномочий оператора элемента, входящего в состав государственного или интеграционного компонента общей инфраструктуры документирования информации в электронном виде и включенного в перечень, или выявления существенного нарушения Требований и (или) законодательства государства-члена уполномоченный орган или Комиссия, представившие заявление в отношении такого элемента, направляют в межгосударственную комиссию ходатайство об исключении этого элемента из перечня.

ПРИЛОЖЕНИЕ № 1
к Требованиям к созданию,
развитию
и функционированию
трансграничного пространства
доверия

АРХИТЕКТУРА
трансграничного пространства доверия

1. Настоящий документ определяет состав элементов, входящих в государственные и интеграционный компоненты общей инфраструктуры документирования информации в электронном виде, необходимый и достаточный для обеспечения межгосударственного обмена данными и электронными документами органов государственной власти государств – членов Евразийского экономического союза (далее соответственно – государства-члены, Союз) между собой и с Евразийской экономической комиссией (далее – Комиссия) в рамках реализации первого этапа Стратегии развития трансграничного пространства доверия, утвержденной Решением Коллегии Евразийской экономической комиссии от 27 сентября 2016 г. № 105.

2. Для обеспечения доверия при осуществлении межгосударственного информационного взаимодействия с использованием имеющих юридическую силу электронных документов в рамках Союза создается общая инфраструктура документирования информации в электронном виде, которая гарантирует, что:

электронные документы своевременно и точно передаются между субъектами электронного взаимодействия с обеспечением (сохранением) их юридической силы, а также с обеспечением взаимоприемлемого уровня защиты информации;

в случае возникновения любых разногласий существуют соответствующие методы подготовки и представления требуемых свидетельств, позволяющих восстановить ход событий и определить их причину.

3. В каждом государстве-члене создается государственный компонент общей инфраструктуры документирования информации в электронном виде, в Комиссии

создается интеграционный компонент общей инфраструктуры документирования информации в электронном виде.

4. Интеграционный компонент общей инфраструктуры документирования информации в электронном виде включает в себя следующие элементы:

удостоверяющий центр службы доверенной третьей стороны интегрированной информационной системы Союза (далее соответственно – удостоверяющий центр службы доверенной третьей стороны, интегрированная система), предназначенный для создания и проверки актуальности сертификатов ключей проверки ЭЦП уполномоченных доверенных третьих сторон интеграционного сегмента Комиссии и национальных сегментов государств-членов интегрированной системы. В состав сервисов удостоверяющего центра службы доверенной третьей стороны входит сервис штампа времени, используемый доверенными третьими сторонами интеграционного сегмента Комиссии и национальных сегментов государств-членов интегрированной системы в соответствии с Положением об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, утвержденным Решением Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125;

доверенная третья сторона, функционирующая в интеграционном сегменте Комиссии интегрированной системы (далее – доверенная третья сторона Комиссии), предназначенная для проверки ЭЦП в электронных документах в фиксированный момент времени в отношении лица, подписавшего электронный документ, и для выполнения основных задач доверенной третьей стороны Комиссии в соответствии с Протоколом об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза (приложение № 3 к Договору о Евразийском экономическом союзе от 29 мая 2014 года). В состав сервисов доверенной третьей стороны Комиссии входит сервис штампа времени, используемый доверенной третьей стороной Комиссии и функционирующими в национальных сегментах государств-членов интегрированной системы уполномоченными доверенными третьими сторонами (далее – доверенные третьи стороны государств-членов) в соответствии с Положением об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией;

удостоверяющий центр Комиссии, предназначенный для обеспечения сертификатами ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии, являющихся субъектами электронного взаимодействия в рамках Союза, и для проверки актуальности выданных сертификатов ключей проверки ЭЦП;

интеграционная платформа интегрированной системы, обеспечивающая маршрутизацию и гарантированную доставку электронных документов и данных при электронном взаимодействии между интеграционным сегментом Комиссии и национальными сегментами государств-членов интегрированной системы;

интеграционный шлюз интегрированной системы, обеспечивающий взаимодействие подсистем интеграционного сегмента Комиссии интегрированной системы с интеграционной платформой интегрированной системы;

подсистема информационной безопасности интегрированной системы, предназначенная для обеспечения конфиденциальности, целостности и доступности данных при их обработке и хранении в интеграционном сегменте Комиссии, а также при их передаче по каналам связи, объединяющим интеграционные шлюзы интеграционного сегмента Комиссии и интеграционные шлюзы национальных сегментов государств-членов интегрированной системы.

5. Каждый государственный компонент общей инфраструктуры документирования информации в электронном виде включает в себя следующие элементы:

доверенная третья сторона государства-члена, предназначенная для проверки ЭЦП в электронных документах в фиксированный момент времени в отношении лица, подписавшего электронный документ, и для выполнения основных задач доверенной третьей стороны государства-члена в соответствии с Протоколом об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза. В состав сервисов доверенной третьей стороны государства-члена входит сервис штампа времени, используемый доверенной третьей стороной в соответствии с Положением об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией;

удостоверяющие центры государства-члена, а также другая инфраструктура, предназначенные для обеспечения сертификатами ключей проверки ЭЦП субъектов электронного взаимодействия в рамках Союза и для проверки актуальности выданных сертификатов ключей проверки ЭЦП;

интеграционный шлюз национального сегмента государства-члена интегрированной системы, обеспечивающий подключение системы межведомственного информационного взаимодействия государства-члена к интеграционной платформе интегрированной системы;

подсистема защиты национального сегмента государства-члена интегрированной системы, предназначенная для обеспечения конфиденциальности, целостности и доступности данных при их обработке и хранении в национальном сегменте государства-члена интегрированной системы. Для обеспечения конфиденциальности, целостности, доступности и сохранности информации в национальном сегменте

государства-члена интегрированной системы принимается и реализуется комплекс правовых, организационных и технических мер защиты информации в соответствии с законодательством соответствующего государства-члена.

ПРИЛОЖЕНИЕ № 2
к Требованиям к созданию,
развитию
и функционированию
трансграничного пространства
доверия

ТРЕБОВАНИЯ
к средствам удостоверяющего центра службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза

I. Общие положения

1. Настоящие Требования устанавливают требования к средствам удостоверяющего центра службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза (далее соответственно – удостоверяющий центр, Союз).

II. Требования к программному обеспечению средств удостоверяющего центра

2. Программное обеспечение средств удостоверяющего центра не должно содержать средств, позволяющих модифицировать или искажать алгоритм работы программного обеспечения средств удостоверяющего центра.

3. Прикладное программное обеспечение средств удостоверяющего центра и программное обеспечение средств криптографической защиты информации, используемых удостоверяющим центром, должны использовать только документированные функции системного программного обеспечения.

4. Системное и прикладное программное обеспечение средств удостоверяющего центра должно обеспечивать разграничение доступа системного администратора средств удостоверяющего центра, администратора сертификации средств удостоверяющего центра, операторов средств удостоверяющего центра и пользователей удостоверяющего центра к информации, обрабатываемой средствами удостоверяющего центра, в соответствии с правилами разграничения доступа, установленными системным администратором средств удостоверяющего центра.

5. В состав системного и (или) прикладного программного обеспечения средств удостоверяющего центра должен входить механизм, обеспечивающий очистку

оперативной и внешней памяти, используемой для хранения информации ограниченного доступа.

6. Исходные тексты системного и прикладного программного обеспечения средств удостоверяющего центра должны пройти проверку реализации методов и способов защиты информации от атак, для подготовки и проведения которых используются возможности нарушителя безопасности информации, указанные в утверждаемой Евразийской экономической комиссией (далее – Комиссия) модели угроз безопасности информации и действий нарушителя в удостоверяющем центре службы доверенной третьей стороны.

7. В состав программного обеспечения средств удостоверяющего центра должен входить механизм, обеспечивающий устойчивость к компьютерным атакам из внешних сетей.

8. Исходные тексты системного и прикладного программного обеспечения средств удостоверяющего центра должны пройти формальную верификацию отсутствия недекларированных возможностей, а также формальную верификацию реализации методов и способов защиты информации противостояния атакам, для подготовки и проведения которых используются возможности нарушителя безопасности информации, указанные в утверждаемой Комиссией модели угроз безопасности информации и действий нарушителя в удостоверяющем центре службы доверенной третьей стороны.

III. Требования к аппаратным средствам удостоверяющего центра

9. К аппаратным средствам удостоверяющего центра предъявляются следующие требования:

а) проведение проверки соответствия реализации целевых функций удостоверяющего центра с использованием определяемой Комиссией системы тестов аппаратных средств удостоверяющего центра;

б) проведение специальной проверки аппаратных средств удостоверяющего центра, произведенных в третьих странах, в целях выявления устройств, предназначенных для негласного получения информации;

в) проведение исследований аппаратных средств удостоверяющего центра и анализа программного кода BIOS с целью исключения наличия недекларированных возможностей, а также исследований на соответствие требованиям к защите от утечки информации по каналам побочных электромагнитных излучений и наводок, установленным в соответствии с законодательством государств – членов Союза (далее – государства-члены).

IV. Требования к ролевому разграничению

10. В средствах удостоверяющего центра должны реализовываться следующие обязательные роли:

а) системный администратор, в полномочия которого входят инсталляция, конфигурация и поддержка функционирования средств удостоверяющего центра, создание и поддержка профилей членов группы администраторов средств удостоверяющего центра, конфигурация профиля и параметров журнала аудита;

б) администратор сертификации, в полномочия которого входят создание и аннулирование сертификатов ключей проверки электронной цифровой подписи (электронной подписи) (далее – ЭЦП);

в) администратор аудита, в полномочия которого входят просмотр, копирование и полная очистка журнала аудита;

г) администратор информационной безопасности, в полномочия которого входят контроль и обеспечение функционирования средств защиты информации, анализ и контроль состояния защищенности средств удостоверяющего центра, контроль за выполнением организационных мер защиты информации.

11. В средствах удостоверяющего центра должен реализовываться механизм, исключающий возможность авторизации одного члена группы администраторов средств удостоверяющего центра с целью использования полномочий различных ролей .

12. Системный администратор не должен иметь возможности вносить изменения в журнал аудита.

V. Требования к целостности средств удостоверяющего центра

13. В средствах удостоверяющего центра должен реализовываться механизм, исключающий возможность несанкционированного случайного и (или) преднамеренного искажения (изменения, модификации) и (или) разрушения информации, программных и (или) аппаратных средств удостоверяющего центра (далее – контроль целостности). Требования к механизму контроля целостности определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

14. Контроль целостности должен осуществляться при каждой перезагрузке операционной системы до ее загрузки, а также динамически в процессе функционирования средств удостоверяющего центра (динамический контроль целостности).

15. Динамический контроль целостности должен выполняться не реже 1 раза в сутки.

16. В составе программных и (или) аппаратных средств удостоверяющего центра должны иметься средства восстановления целостности программных средств удостоверяющего центра.

VI. Требования к управлению доступом

17. Средства удостоверяющего центра должны обеспечивать реализацию дискреционного и мандатного принципов управления доступом, а также создание замкнутой рабочей среды (программной среды, которая допускает существование в ней только фиксированного набора программ и процессов). Требования к управлению доступом определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

VII. Требования к идентификации и аутентификации

18. Идентификация и аутентификация включают в себя распознавание пользователя средств удостоверяющего центра, члена группы администраторов средств удостоверяющего центра или процесса, а также проверку их подлинности. Механизм аутентификации при отрицательном результате аутентификации должен блокировать доступ этих субъектов доступа к функциям удостоверяющего центра.

19. В средствах удостоверяющего центра для любой реализованной процедуры аутентификации должен применяться механизм ограничения количества следующих подряд попыток аутентификации одного субъекта доступа, число которых не должно быть более 20. При превышении числа следующих подряд попыток аутентификации одного субъекта доступа доступ этого субъекта доступа к средствам удостоверяющего центра должен быть заблокирован на 15 минут.

20. Описание процедуры регистрации пользователей средств удостоверяющего центра (внесения данных в реестр пользователей средств удостоверяющего центра), в том числе требование о необходимости предъявления пользователем средств удостоверяющего центра при регистрации документов, удостоверяющих личность, должны содержаться в эксплуатационной документации на средства удостоверяющего центра.

21. В отношении лиц, осуществляющих доступ к средствам удостоверяющего центра, должна проводиться двухфакторная аутентификация.

22. Для пользователей средств удостоверяющего центра и членов группы администраторов средств удостоверяющего центра допускается реализация механизмов удаленной аутентификации на основе разрешенных криптографических алгоритмов с использованием сертификатов аутентификации.

23. При осуществлении локального доступа к средствам удостоверяющего центра аутентификация членов группы администраторов средств удостоверяющего центра

должна выполняться до перехода в рабочее состояние таких средств (например, до загрузки базовой операционной системы).

24. При использовании для локальной аутентификации символьного, периодически изменяемого пароля он должен состоять из не менее 8 символов (при общем количестве символов алфавита не менее 36). Период изменения пароля не должен превышать 6 месяцев.

VIII. Требования к защите данных, полученных или передаваемых удостоверяющим центром

25. Самоподписанный сертификат ключа проверки ЭЦП удостоверяющего центра должен храниться способом, исключающим его модификацию или искажение.

26. Средства удостоверяющего центра должны обеспечивать передачу данных, содержащих информацию ограниченного доступа, полученных удостоверяющим центром или передаваемых из удостоверяющего центра, способом, исключающим несанкционированный доступ к информации.

27. Средства удостоверяющего центра должны реализовывать защиту от навязывания ложных сообщений (действий, воспринимаемых субъектами электронного взаимодействия или средствами удостоверяющего центра как передача истинного сообщения способом, защищенным от несанкционированного доступа) путем применения разрешенных криптографических алгоритмов с использованием сертификатов ключа проверки ЭЦП. Требования к процедуре защиты от навязывания ложных сообщений определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

28. Средства удостоверяющего центра должны реализовывать процедуру защищенной передачи пользователем средств удостоверяющего центра первоначального запроса на создание для него сертификата ключа проверки ЭЦП.

29. Средства удостоверяющего центра должны принимать критичную для функционирования удостоверяющего центра информацию в случае, если она подписана ЭЦП.

30. Все компоненты средств удостоверяющего центра должны размещаться в одной контролируемой зоне.

IX. Требования к регистрации событий

31. Операционная система средств удостоверяющего центра должна поддерживать ведение журнала аудита, содержащего информацию о системных событиях и событиях, связанных с выполнением удостоверяющим центром своих функций.

32. Список регистрируемых в журнале аудита событий должен содержаться в эксплуатационной документации на средства удостоверяющего центра.

33. Журнал аудита должен быть доступен только администратору аудита.

34. Полная очистка журнала аудита проводится только после копирования всей информации, подлежащей очистке. После такой очистки в качестве первой записи в журнале аудита должен автоматически регистрироваться факт проведения очистки (с указанием даты, времени проведения указанной очистки и информации о лице, которое ее проводило).

X. Требования к надежности и устойчивости функционирования средств удостоверяющего центра

35. Производится расчет вероятности возникновения сбоев и неисправностей аппаратных средств удостоверяющего центра, приводящих к невыполнению удостоверяющим центром своих функций.

36. В течение суток вероятность возникновения сбоев и неисправностей аппаратных средств удостоверяющего центра, приводящих к невыполнению удостоверяющим центром своих функций, не должна превышать аналогичную вероятность возникновения сбоев и неисправностей используемых в составе удостоверяющего центра криптографических средств.

37. Средняя наработка средств удостоверяющего центра (комплексно) на отказ составляет не менее 18 000 ч.

38. Должно осуществляться тестирование устойчивости функционирования средств удостоверяющего центра.

39. Время восстановления средств удостоверяющего центра составляет не более 4 часов.

40. Меры и средства повышения надежности и устойчивости функционирования средств удостоверяющего центра должны предусматривать квотирование ресурсов средств удостоверяющего центра.

XI. Требования к созданию, использованию, хранению и уничтожению ключевой информации

41. Порядок создания, использования, хранения, уничтожения ключевой информации и сроки ее действия определяются в соответствии с требованиями, установленными в эксплуатационной документации на средства ЭЦП и иные криптографические средства, используемые средствами удостоверяющего центра, а также в соответствии с принципами разработки и модернизации шифровальных (криптографических) средств защиты информации, утверждаемыми Комиссией.

42. Копирование ключевой информации должно осуществляться в соответствии с эксплуатационной документацией на используемые в удостоверяющем центре криптографические средства.

43. Ключи ЭЦП, используемые для подписания создаваемых средствами удостоверяющего центра сертификатов ключей проверки ЭЦП и подписания сообщений службы доверенного времени и службы подтверждения статусов сертификатов, должны генерироваться, храниться, использоваться и уничтожаться в отдельных криптографических модулях (доверенных вычислительных устройствах).

44. Ключ ЭЦП, используемый для подписания создаваемых сертификатов ключей проверки ЭЦП и подписания списка уникальных номеров сертификатов ключей проверки ЭЦП, действие которых в определенный момент времени до истечения срока их действия было прекращено удостоверяющим центром (далее – список отозванных сертификатов), не должен использоваться в иных целях.

XII. Требования к резервному копированию информации и восстановлению работоспособности средств удостоверяющего центра

45. Средства удостоверяющего центра должны реализовывать функции резервного копирования информации, обрабатываемой средствами удостоверяющего центра, и восстановления работоспособности аппаратных средств удостоверяющего центра в случае повреждения такой информации и таких средств. В ходе резервного копирования должна быть исключена возможность копирования криптографических ключей.

46. Данные, сохраненные при резервном копировании, должны быть достаточными для восстановления функционирования средств удостоверяющего центра до состояния, зафиксированного на момент копирования данных.

47. Должны быть приняты меры по обнаружению несанкционированных изменений сохраненных данных.

48. Требования к времени восстановления работоспособности средств удостоверяющего центра должны быть определены в техническом задании на разработку (модернизацию) средств удостоверяющего центра, а также в эксплуатационной документации на средства удостоверяющего центра.

49. Сохраняемая при резервном копировании защищаемая информация должна сохраняться только в зашифрованном виде.

XIII. Требования к созданию и аннулированию сертификатов ключей проверки ЭЦП

50. Протоколы создания и аннулирования сертификатов ключей проверки ЭЦП должны быть описаны в эксплуатационной документации на средства удостоверяющего центра.

51. Создаваемые удостоверяющим центром сертификаты ключей проверки ЭЦП и списки отозванных сертификатов должны соответствовать требованиям, утверждаемым Комиссией.

52. Средства удостоверяющего центра должны реализовывать механизм контроля соответствия создаваемых сертификатов ключей проверки ЭЦП требованиям, утверждаемым Комиссией.

53. Средства удостоверяющего центра должны реализовывать с использованием списков отозванных сертификатов и протокола OCSP отзыв сертификата ключа проверки ЭЦП в случае прекращения его действия или аннулирования. Порядок такого отзыва утверждается Комиссией.

54. Средства удостоверяющего центра в отношении владельца сертификата ключа проверки ЭЦП должны реализовывать проверку уникальности ключа проверки ЭЦП и проверку обладания соответствующим ключом ЭЦП.

XIV. Требования к реестру выданных, прекративших действие и аннулированных сертификатов ключей проверки ЭЦП и к предоставлению доступа к нему

55. В средствах удостоверяющего центра должны быть реализованы механизмы хранения и поиска по атрибутам выданных удостоверяющим центром, прекративших действие и аннулированных сертификатов ключей проверки ЭЦП в реестре выданных, прекративших действие и аннулированных сертификатов ключей проверки ЭЦП (далее – реестр сертификатов), а также механизмы предоставления сетевого доступа к реестру сертификатов.

56. Все вносимые в реестр сертификатов ключей проверки ЭЦП изменения должны регистрироваться в журнале аудита.

XV. Требования к криптографическим средствам

57. Средства удостоверяющего центра должны использовать средства ЭЦП и иные криптографические средства, имеющие заключение уполномоченных органов государства пребывания Комиссии о соответствии требованиям, установленным законодательством этого государства к криптографическим средствам класса КА, а также соответствующие принципам разработки и модернизации шифровальных (криптографических) средств защиты информации, утверждаемым Комиссией.

58. Для создания и проверки ЭЦП средства удостоверяющего центра должны использовать средства ЭЦП, реализуемые на основе криптографического модуля, имеющего в своем составе средства отображения результатов создания (проверки) ЭЦП.

XVI. Требования к криптографическим стандартам

59. Средства удостоверяющего центра должны использовать средства ЭЦП и иные криптографические средства, реализующие криптографические алгоритмы, идентификаторы которых указаны в приложении № 8 к Положению об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, утвержденному Решением Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125.

XVII. Требования к проверке действительности сертификата ключа проверки ЭЦП

60. Реализованный в средствах удостоверяющего центра механизм проверки ЭЦП в выдаваемых удостоверяющим центром сертификатах ключей проверки ЭЦП должен быть указан в эксплуатационной документации на средства удостоверяющего центра. Такой механизм должен обеспечивать проверку ЭЦП в выдаваемых удостоверяющим центром сертификатах ключей проверки ЭЦП после создания сертификата ключа проверки ЭЦП и до его выдачи.

61. При проверке действительности сертификата ключа проверки ЭЦП средства удостоверяющего центра проверяют действительность каждого сертификата из цепочки сертификатов ключей проверки ЭЦП, в том числе действительность ЭЦП, которыми подписаны такие сертификаты. Данная цепочка состоит из корневого самоподписанного сертификата ключа проверки ЭЦП удостоверяющего центра и проверяемого сертификата ключа проверки ЭЦП.

XVIII. Дополнительные требования

62. В целях ограничения возможностей построения атак на средства удостоверяющего центра с использованием каналов связи должны применяться средства межсетевого экранирования, применяемые серверами, обслуживающими сайты, веб-службы и веб-приложения. Средства межсетевого экранирования должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера.

63. Должны применяться средства защиты от компьютерных вирусов, обеспечивающие обнаружение компьютерных программ или иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования , модификации, копирования защищаемой информации или нейтрализации средств защиты информации, а также обеспечиваться реагирование на обнаружение таких программ и информации.

64. Должны применяться средства защиты от компьютерных атак, обеспечивающие обнаружение действий, направленных на получение несанкционированного доступа к информации, оказание специальных воздействий на средства удостоверяющего центра в целях получения, уничтожения, искажения защищаемой информации и (или) блокирования доступа к ней, а также обеспечиваться реагирование на такие действия (предотвращение таких действий).

65. Средства межсетевого экранирования, средства защиты от компьютерных вирусов и средства защиты от компьютерных атак должны соответствовать требованиям, определяемым уполномоченными органами государств-членов.

66. Исследования средств удостоверяющего центра с целью подтверждения их соответствия настоящим Требованиям должны проводиться с использованием определяемых уполномоченными органами государств-членов числовых значений параметров и характеристик реализуемых в средствах удостоверяющего центра механизмов защиты информации.

67. Средства удостоверяющего центра должны эксплуатироваться в соответствии с эксплуатационной документацией на них. Организационно-технические мероприятия, необходимые для обеспечения безопасного функционирования средств удостоверяющего центра, должны указываться в эксплуатационной документации на средства удостоверяющего центра.

ПРИЛОЖЕНИЕ № 3
к Требованиям к созданию,
развитию
и функционированию
трансграничного пространства
доверия

ТРЕБОВАНИЯ
к средствам доверенной третьей стороны интеграционного сегмента Евразийской экономической комиссии интегрированной информационной системы Евразийского экономического союза и средству электронной цифровой подписи (электронной подписи) в их составе

I. Общие положения

1. Настоящие Требования устанавливают требования к средствам доверенной третьей стороны интеграционного сегмента Евразийской экономической комиссии интегрированной информационной системы Евразийского экономического союза (далее соответственно – средства доверенной третьей стороны, интеграционный сегмент , Комиссия, интегрированная система, Союз), а также к средству электронной цифровой подписи (электронной подписи) (далее – ЭЦП) в их составе.

II. Требования к средствам доверенной третьей стороны

1. Требования к составу и функциям компонентов средств доверенной третьей стороны

2. В состав средств доверенной третьей стороны должны входить следующие компоненты:

а) компонент проверки ЭЦП;

б) компонент проверки действительности сертификата ключа проверки ЭЦП;

в) компонент проверки соответствия сертификата ключа проверки ЭЦП установленным требованиям;

г) компонент проверки полномочий отправителя, сформировавшего и подписавшего электронный документ в интеграционном сегменте Комиссии;

д) компонент формирования квитанций с результатом проверки ЭЦП и их подписания соответствующими ЭЦП доверенной третьей стороны, функционирующей в составе интеграционного сегмента Комиссии (далее – доверенная третья сторона Комиссии);

е) компонент фиксации времени для электронных документов, входящих в интеграционный сегмент Комиссии;

ж) компонент документирования операций, выполняемых средствами доверенной третьей стороны;

з) компонент предоставления информации об операциях, выполняемых доверенной третьей стороной Комиссии, по запросам, предусмотренным правом Союза.

3. Компонент проверки ЭЦП должен осуществлять:

а) проверку ЭЦП электронного документа с применением сертификата ключа проверки ЭЦП отправителя, сформировавшего и подписавшего этот электронный документ в интеграционном сегменте Комиссии или информационной системе Комиссии;

б) проверку ЭЦП квитанции доверенной третьей стороны государства – члена Союза, функционирующей в составе национального сегмента интегрированной информационной системы Союза (далее соответственно – государство-член, доверенная третья сторона государства-члена), которой подписан результат проверки ЭЦП электронного документа, входящего в интеграционный сегмент Комиссии;

в) проверку ЭЦП штампа времени квитанции доверенной третьей стороны государства-члена, которой подписан результат проверки ЭЦП электронного документа, входящего в интеграционный сегмент Комиссии;

г) проверку ЭЦП:

сертификата ключа проверки ЭЦП отправителя;

корневого сертификата ключа проверки ЭЦП удостоверяющего центра Комиссии, на соответствующем ключе ЭЦП которого основана ЭЦП, которой подписан сертификат ключа проверки ЭЦП отправителя;

сертификата ключа проверки ЭЦП доверенной третьей стороны Комиссии, выданного удостоверяющим центром службы доверенной третьей стороны интегрированной системы Союза (далее – удостоверяющий центр службы доверенной третьей стороны);

корневого сертификата ключа проверки ЭЦП удостоверяющего центра службы доверенной третьей стороны, на соответствующем ключе ЭЦП которого основана ЭЦП , которой подписан сертификат ключа проверки ЭЦП доверенной третьей стороны Комиссии;

сертификата ключа проверки ЭЦП удостоверяющего центра службы доверенной третьей стороны, на соответствующем ключе ЭЦП которого основана ЭЦП штампа времени, сформированная для квитанций, используемых при взаимодействии доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов.

4. Компонент проверки действительности сертификата ключа проверки ЭЦП должен осуществлять:

а) проверку действительности сертификата ключа проверки ЭЦП отправителя на момент подписания им электронного документа и корневого сертификата ключа проверки ЭЦП удостоверяющего центра Комиссии, на соответствующем ключе ЭЦП которого основана ЭЦП, которой подписан сертификат ключа проверки ЭЦП отправителя;

б) проверку действительности:

сертификата ключа проверки ЭЦП доверенной третьей стороны государства-члена, выданного удостоверяющим центром службы доверенной третьей стороны, на момент подписания ею квитанции с результатом проверки ЭЦП электронного документа, входящего в интеграционный сегмент Комиссии;

корневого сертификата удостоверяющего центра службы доверенной третьей стороны на момент подписания сертификата доверенной третьей стороны государства-члена;

в) проверку действительности сертификатов ключей проверки ЭЦП, на соответствующих ключах ЭЦП которых основываются ЭЦП, используемые средствами доверенной третьей стороны Комиссии для подписания:

результатов проверок ЭЦП исходящих электронных документов;

результатов проверок ЭЦП квитанций с результатами проверок ЭЦП входящих электронных документов на момент их подписания;

г) проверку действительности сертификата ключа проверки ЭЦП удостоверяющего центра службы доверенной третьей стороны, на соответствующем ключе ЭЦП

которого основана ЭЦП штампа времени для квитанций, используемых при взаимодействии доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов.

5. Компонент проверки соответствия сертификата ключа проверки ЭЦП установленным требованиям должен осуществлять проверку соответствия требованиям права Союза, предъявляемым к сертификатам ключей проверки ЭЦП, включая требования к их форме, содержанию, к средствам удостоверяющего центра, с использованием которых они созданы, и средствам ЭЦП, с использованием которых они подписаны:

а) сертификата ключа проверки ЭЦП отправителя;

б) корневого сертификата ключа проверки ЭЦП удостоверяющего центра Комиссии , на соответствующем ключе ЭЦП которого основана ЭЦП, которой подписан сертификат ключа проверки ЭЦП отправителя;

в) корневого сертификата ключа проверки ЭЦП удостоверяющего центра службы доверенной третьей стороны, на соответствующем ключе ЭЦП которого основана ЭЦП , которой подписан сертификат ключа проверки ЭЦП доверенной третьей стороны государства-члена;

г) сертификата ключа проверки ЭЦП, на соответствующем ключе ЭЦП которого основывается ЭЦП, используемая средствами доверенной третьей стороны Комиссии для подписания результатов проверок ЭЦП квитанций с результатами проверок ЭЦП входящих электронных документов;

д) сертификата ключа проверки ЭЦП, на соответствующем ключе ЭЦП которого основывается ЭЦП, используемая средствами доверенной третьей стороны Комиссии для подписания результатов проверок ЭЦП исходящих электронных документов;

е) сертификата ключа проверки ЭЦП доверенной третьей стороны государства-члена интегрированной системы, выданного удостоверяющим центром службы доверенной третьей стороны, на соответствующем ключе ЭЦП которого основана ЭЦП квитанции с результатом проверки ЭЦП входящего электронного документа;

ж) сертификата ключа проверки ЭЦП удостоверяющего центра службы доверенной третьей стороны, на соответствующем ключе которого основана ЭЦП штампа времени для квитанций, используемых при взаимодействии доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов.

6. Компонент проверки полномочий отправителя, сформировавшего и подписавшего электронный документ, должен осуществлять проверку полномочий отправителя электронного документа – должностного лица или сотрудника Комиссии, являющегося владельцем сертификата ключа проверки ЭЦП и выступающего от имени члена Коллегии Комиссии в соответствии с требованиями права Союза.

7. Компонент формирования квитанций с результатом проверки ЭЦП и их подписания соответствующими ЭЦП доверенной третьей стороны Комиссии должен осуществлять:

а) формирование и подписание ЭЦП, основанной на ключе ЭЦП, соответствующем сертификату ключа проверки ЭЦП, выданному доверенной третьей стороне Комиссии удостоверяющим центром службы доверенной третьей стороны, а также квитанции с результатом проверки ЭЦП исходящего электронного документа;

б) формирование и подписание ЭЦП, основанной на ключе ЭЦП, соответствующем сертификату ключа проверки ЭЦП, выданному доверенной третьей стороне Комиссии удостоверяющим центром Комиссии, а также квитанции с результатом проверки ЭЦП квитанции доверенной третьей стороны государства-члена с результатом проверки входящего электронного документа.

8. Компонент фиксации времени для электронных документов, входящих в интеграционный сегмент Комиссии, должен осуществлять запрос в удостоверяющий центр Комиссии на простановку штампа времени для сформированной и подписанной квитанции с результатом проверки ЭЦП квитанции доверенной третьей стороны государства-члена с результатом проверки ЭЦП входящего электронного документа в соответствии с пунктом 28 Положения об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, утвержденного Решением Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125. При этом простановка штампов времени на квитанции с результатом проверки ЭЦП исходящего электронного документа осуществляется удостоверяющим центром службы доверенной третьей стороны.

9. Компонент документирования выполняемых средствами доверенной третьей стороны Комиссии операций должен предусматривать хранение электронных документов, соответствующих выполненным данной доверенной третьей стороной операциям, в течение установленного времени. Указанные электронные документы должны быть подписаны ЭЦП, основанной на ключе ЭЦП, соответствующем специально предназначенному для этой цели сертификату ключа проверки ЭЦП, выданном удостоверяющим центром Комиссии доверенной третьей стороне Комиссии. По истечении срока действия ключей проверки указанной ЭЦП должны быть предусмотрены процедура переподписания этих электронных документов с использованием новых ключей ЭЦП, а также преемственность полномочий лиц, уполномоченных осуществлять переподписание таких электронных документов.

10. Компонент предоставления информации об операциях доверенной третьей стороны Комиссии по запросам, предусмотренным правом Союза, должен

осуществлять предоставление информации в соответствии с требованиями, установленными правом Союза.

2. Требования к программному обеспечению средств доверенной третьей стороны

11. Программное обеспечение средств доверенной третьей стороны не должно содержать средств, позволяющих модифицировать или искажать алгоритмы работы этого программного обеспечения.

12. Программное обеспечение должно использовать только документированные функции операционной системы.

13. Системное программное обеспечение, используемое средствами доверенной третьей стороны, не должно содержать известных уязвимостей.

14. Программное обеспечение должно обеспечивать разграничение доступа системного администратора, оператора и пользователей к информации, обрабатываемой средствами доверенной третьей стороны, на основании правил разграничения доступа, заданных системным администратором.

15. Исходные тексты системного и прикладного программного обеспечения криптографического модуля (доверенного вычислительного устройства), используемого для создания, хранения, применения и уничтожения ключей ЭЦП доверенной третьей стороны Комиссии и создаваемого в соответствии с Решением Коллегии Евразийской экономической комиссии от 2 июня 2016 г. № 49 (ДСП) совместно с анализом программного кода BIOS, должны пройти формальную верификацию в части отсутствия в них недекларированных возможностей, а также формальную верификацию реализации в них методов и способов защиты информации в порядке, установленном в государстве пребывания Комиссии.

16. Программное обеспечение должно содержать в своем составе механизм, обеспечивающий очистку оперативной и внешней памяти, используемой для хранения защищаемой информации, перечень которой устанавливается техническим заданием на создание (модернизацию) средств доверенной третьей стороны, при освобождении (перераспределении) памяти путем записи маскирующей информации (случайной или псевдослучайной последовательности символов) в память.

17. Программное обеспечение должно содержать в своем составе компоненты, обеспечивающие экстренное стирание информации ограниченного доступа, в соответствии с перечнем информации ограниченного доступа и требованиями к реализации и надежности стирания, устанавливаемыми техническим заданием на создание (модернизацию) средств доверенной третьей стороны.

18. Программное обеспечение должно содержать в своем составе механизм, обеспечивающий устойчивость к компьютерным атакам из внешних сетей.

19. Исходные тексты системного и прикладного программного обеспечения должны пройти проверку в части реализации в них методов и способов защиты информации, противостоящих атакам, осуществляемым нарушителем из сетей общего пользования, являющимся квалифицированным групповым нарушителем, использующим возможности научных центров, анализирующих системное программное обеспечение с целью поиска уязвимостей.

20. Инженерно-криптографическая защита средств доверенной третьей стороны должна исключить события, приводящие к возможности проведения успешных атак в условиях возможных неисправностей или сбоев аппаратных средств доверенной третьей стороны либо аппаратного компонента средства вычислительной техники, на котором реализованы средства доверенной третьей стороны.

3. Требования к аппаратным средствам средств доверенной третьей стороны

21. Реализация целевых функций средств доверенной третьей стороны, включая исходный код BIOS, должна подтверждаться проверкой на основе системы тестов для аппаратных средств, утверждаемой Комиссией.

22. Должна проводиться оценка параметров надежности функционирования аппаратных средств средств доверенной третьей стороны.

23. Отсутствие в составе аппаратных средств средств доверенной третьей стороны устройств, предназначенных для негласного получения информации, а также уровень защиты от утечки информации по каналам побочных электромагнитных излучений и наводок должны быть подтверждены проверкой на соответствие требованиям, утверждаемым Комиссией.

4. Требования к обеспечению целостности средств доверенной третьей стороны

24. В средствах доверенной третьей стороны должен быть реализован механизм контроля случайного или преднамеренного искажения информации, программных средств и аппаратных средств до загрузки операционной системы.

5. Требования к управлению доступом

25. В средствах доверенной третьей стороны должны быть реализованы механизмы разграничения доступа, поддерживающие следующие обязательные роли:

а) системный администратор, в полномочия которого входят инсталляция, конфигурация и поддержка функционирования средств доверенной третьей стороны, создание и поддержка профилей членов группы администраторов средств доверенной третьей стороны, конфигурация профиля и параметров журнала аудита (за исключением возможности вносить изменения в журнал аудита);

б) администратор информационной безопасности, в полномочия которого входят анализ и контроль состояния защищенности средств доверенной третьей стороны, просмотр журнала аудита, контроль за выполнением организационных мер защиты;

в) администратор средств защиты информации, в полномочия которого входят контроль и обеспечение функционирования средств защиты информации доверенной третьей стороны, а также контроль за условиями функционирования таких средств.

26. Средства доверенной третьей стороны должны обеспечивать реализацию дискреционного и мандатного принципов управления доступом, а также создание замкнутой рабочей среды (программная среда, которая допускает существование в ней только фиксированного набора программ и процессов).

27. В средствах доверенной третьей стороны должен быть реализован механизм, исключающий возможность авторизации 1 члена из группы администраторов средств удостоверяющего центра с целью использования полномочий различных ролей.

6. Требования к идентификации и аутентификации

28. Средства доверенной третьей стороны должны распознавать пользователя, члена группы администраторов таких средств или процесса (далее – субъекты доступа), а также выполнять проверку их подлинности.

29. Механизм аутентификации должен блокировать доступ субъектов доступа к функциям средств доверенной третьей стороны при отрицательном результате аутентификации.

30. Для любой реализованной процедуры аутентификации должен быть применен механизм ограничения количества следующих подряд попыток аутентификации 1 субъекта доступа, число которых не должно превышать 3.

31. При превышении числа следующих подряд попыток аутентификации 1 субъекта доступа над установленным предельным значением доступ этого субъекта доступа к средствам доверенной третьей стороны должен быть заблокирован на промежуток времени, устанавливаемый техническим заданием на создание (модернизацию) средств доверенной третьей стороны.

32. Для всех лиц, осуществляющих доступ к средствам доверенной третьей стороны , должна проводиться двухфакторная аутентификация.

33. Для всех пользователей средств доверенной третьей стороны допускается использование механизмов удаленной аутентификации с использованием сертификатов проверки ключей аутентификации на основе криптографических средств, разработанных в соответствии с требованиями к криптографическим средствам, используемым средствами доверенной третьей стороны, утверждаемыми Комиссией.

34. При осуществлении локального доступа к средствам доверенной третьей стороны аутентификация членов группы администраторов средств доверенной третьей стороны должна выполняться до перехода в рабочее состояние таких средств (например, до загрузки операционной системы).

35. При использовании для локальной аутентификации символьного, периодически изменяемого пароля он должен состоять из не менее чем 8 символов (при общем количестве символов алфавита не менее 36). Период изменения пароля не должен превышать 3 месяцев.

7. Требования к защите данных, входящих в средства доверенной третьей стороны и исходящих из средств доверенной третьей стороны

36. Средства доверенной третьей стороны должны обеспечивать передачу данных, содержащих защищаемую информацию, перечень которой устанавливается техническим заданием на создание (модернизацию) средств доверенной третьей стороны, способом, защищенным от несанкционированного доступа.

37. Средства доверенной третьей стороны должны иметь в своем составе механизмы защиты данных при передаче их между физически разделенными компонентами, использующие криптографические средства, соответствующие требованиям к криптографическим средствам, используемым средствами доверенной третьей стороны, утверждаемыми Комиссией.

38. Средства доверенной третьей стороны должны принимать все входящие сообщения при условии, что они подписаны ЭЦП и проверка ЭЦП имеет положительный результат.

8. Требования к регистрации событий

39. Операционная система средств доверенной третьей стороны должна поддерживать ведение защищенного журнала аудита системных событий и событий, связанных с выполнением средствами доверенной третьей стороны своих функций.

40. Операционная система средств доверенной третьей стороны должна регистрировать события в соответствии с перечнем подлежащих регистрации событий и требованиями к операционной системе, определяемыми и обосновываемыми в техническом задании на создание (модернизацию) средств доверенной третьей стороны .

41. Журнал аудита должен быть доступен только администратору аудита, который может осуществлять только его просмотр, копирование и полную очистку.

42. Полная очистка журнала аудита должна производиться только после создания копии всей информации, подлежащей очистке. После очистки журнала аудита первой записью в таком журнале аудита должен автоматически регистрироваться факт очистки с указанием даты, времени и информации о лице, производившем эту очистку.

9. Требования к надежности и устойчивости функционирования средства доверенной третьей стороны

43. Вероятность возникновения сбоев и неисправностей аппаратных средств, приводящих к невыполнению средствами доверенной третьей стороны своих функций, в течение суток не должна превышать аналогичной вероятности для используемых в составе средств доверенной третьей стороны криптографических средств.

44. Средняя наработка средств доверенной третьей стороны (комплексно) на отказ составляет не менее 20 000 часов.

45. Должно осуществляться тестирование устойчивости функционирования средств доверенной третьей стороны.

46. Время восстановления средств доверенной третьей стороны после сбоев и аварий не должно превышать 4 часа.

47. Меры и средства повышения надежности и устойчивости функционирования средств доверенной третьей стороны должны содержать механизмы квотирования ресурсов средств доверенной третьей стороны.

10. Требования к созданию, использованию, хранению и уничтожению ключевой информации

48. Порядок создания, использования, хранения и уничтожения ключевой информации, в том числе сроки ее действия, должен соответствовать требованиям эксплуатационной документации на средства ЭЦП и иные криптографические средства , используемые средствами доверенной третьей стороны, а также требованиям к криптографическим средствам, используемым средствами доверенной третьей стороны , утверждаемым Комиссией.

49. Копирование ключевых документов должно осуществляться только в соответствии с эксплуатационной документацией на используемые средствами доверенной третьей стороны криптографические средства.

50. Копирование информации ключевых документов на носители, не являющиеся специализированными ключевыми носителями, должно осуществляться только после проведения процедуры ее предварительного шифрования, реализуемой встроенной функцией используемого криптографического средства.

51. Ключ ЭЦП, используемый для подписания ЭЦП квитанций, создаваемых доверенной третьей стороной Комиссии, должен генерироваться, храниться, использоваться и уничтожаться в криптографическом модуле (доверенном вычислительном устройстве), создаваемом в соответствии с Решением Коллегии Евразийской экономической комиссии от 2 июня 2016 г. № 49 (ДСП).

11. Требования к резервному копированию информации

52. Средства доверенной третьей стороны должны реализовывать функции резервного копирования и восстановления данных.

53. Порядок эксплуатации средств доверенной третьей стороны должен предусматривать меры по обнаружению несанкционированных изменений сохраненных данных.

12. Требования к анализу (разбору) сертификата ключа проверки ЭЦП

54. Средства доверенной третьей стороны должны работать только с сертификатами ключа проверки ЭЦП, которые соответствуют требованиям, утверждаемым Комиссией.

55. В средствах доверенной третьей стороны должен быть реализован механизм контроля соответствия сертификатов ключей проверки ЭЦП установленным Комиссией требованиям.

56. Средства доверенной третьей стороны в целях определения их соответствия требованиям, утверждаемым Комиссией, должны иметь механизмы, взаимодействующие с информационными ресурсами государств-членов и Комиссии и осуществляющие анализ расширений сертификата ключа проверки ЭЦП, содержащих:

а) сведения об уровне (классе) криптографической защищенности средств удостоверяющего центра, с использованием которых он был создан;

б) сведения об уровне (классе) криптографической защищенности средства ЭЦП владельца сертификата ключа проверки ЭЦП;

в) сведения о соответствии сертификата ключа проверки ЭЦП политике безопасности, установленной в трансграничном пространстве доверия;

г) наименования средств ЭЦП и средств удостоверяющего центра, которые использованы для создания ключа ЭЦП, ключа проверки ЭЦП и сертификата ключа проверки ЭЦП;

д) наименование средства ЭЦП, используемого владельцем сертификата.

57. Средства доверенной третьей стороны должны осуществлять анализ (разбор) всех расширений сертификата ключа проверки ЭЦП и списков уникальных номеров сертификатов ключей проверки ЭЦП, действие которых на определенный момент времени было прекращено удостоверяющим центром до истечения срока их действия (список отозванных сертификатов) для каждого сертификата из цепочки сертификатов ключей проверки ЭЦП, впервые подвергающейся проверке, а также повторный анализ (разбор) сертификатов из ранее проверенной цепочки сертификатов ключей проверки ЭЦП для вновь изданных сертификатов ключей проверки ЭЦП.

13. Требования к криптографическим стандартам

58. Средства доверенной третьей стороны должны использовать только те средства ЭЦП и иные криптографические средства, которые реализуют криптографические алгоритмы, идентификаторы которых указаны в приложении № 8 к Положению об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, утвержденному Решением Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125.

14. Требования к проверке действительности сертификата ключа проверки ЭЦП

59. При проверке действительности сертификата ключа проверки ЭЦП средства доверенной третьей стороны должны проверять действительность каждого сертификата ключа проверки ЭЦП, а также действительность каждой ЭЦП, которыми подписаны такие сертификаты, из следующих 4 цепочек сертификатов ключей проверки ЭЦП:

а) 1 цепочка сертификатов ключей проверки ЭЦП начинается корневым сертификатом ключа проверки ЭЦП удостоверяющего центра Комиссии и заканчивается проверяемым сертификатом ключа проверки ЭЦП отправителя;

б) 2 цепочка сертификатов ключей проверки ЭЦП начинается корневым сертификатом ключа проверки ЭЦП удостоверяющего центра службы доверенной третьей стороны и заканчивается проверяемым сертификатом ключа проверки ЭЦП доверенной третьей стороны государства-члена;

в) 3 цепочка сертификатов ключей проверки ЭЦП начинается корневым сертификатом ключа проверки ЭЦП удостоверяющего центра службы доверенной третьей стороны и заканчивается проверяемым сертификатом ключа проверки ЭЦП доверенной третьей стороны Комиссии;

г) 4 цепочка сертификатов ключей проверки ЭЦП начинается корневым сертификатом ключа проверки ЭЦП удостоверяющего центра службы доверенной третьей стороны и заканчивается проверяемым сертификатом ключа проверки ЭЦП, на соответствующем ключе ЭЦП которого основана ЭЦП штампа времени для квитанций, используемых при взаимодействии доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов.

60. Каждый сертификат из цепочки сертификатов ключей проверки ЭЦП подлежит анализу (разбору) в соответствии с подразделом 12 настоящего раздела.

61. Проверка ЭЦП в сертификате ключа проверки ЭЦП должна осуществляться в соответствии с международными рекомендациями ITU-T X.509 "Информационные технологии. Взаимосвязь открытых систем. Справочник: Структуры сертификатов открытых ключей и атрибутов" (версия 3) и включать в себя обязательную проверку всех критических расширений в соответствии с политикой безопасности, установленной в трансграничном пространстве доверия.

15. Дополнительные требования

62. Для ограничения возможностей по построению атак на средства доверенной стороны с использованием каналов связи должны применяться средства межсетевого экранирования, обеспечивающие контроль и фильтрацию по протоколу передачи гипертекста информационных потоков, проходящих к веб-серверу и от веб-сервера.

63. Должны применяться средства защиты от компьютерных вирусов, обеспечивающие обнаружение компьютерных программ или иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования

, модификации, копирования защищаемой информации или нейтрализации средств защиты информации, а также должно обеспечиваться реагирование на обнаружение этих программ и информации.

64. Должны применяться средства защиты от компьютерных атак, обеспечивающие обнаружение действий, направленных на несанкционированный доступ к информации, специальные воздействия на средства доверенной третьей стороны в целях получения, уничтожения, искажения защищаемой информации и (или) блокирования доступа к ней , а также должно обеспечиваться реагирование на такие действия (предотвращение этих действий).

65. Применяемые средства межсетевого экранирования, средства защиты от компьютерных вирусов и средства защиты от компьютерных атак должны соответствовать требованиям, утверждаемым Комиссией.

66. Исследования средств доверенной третьей стороны с целью подтверждения их соответствия настоящим Требованиям должны проводиться с использованием числовых значений параметров и характеристик механизмов защиты, реализуемых в средствах доверенной третьей стороны, которые определяются уполномоченным органом государства пребывания Комиссии.

III. Требования к средству ЭЦП в составе средств доверенной третьей стороны

1. Общие требования

67. Средство ЭЦП в составе средств доверенной третьей стороны (далее – средство ЭЦП) должно использоваться при взаимодействии доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов.

68. Средство ЭЦП должно обеспечивать возможность его функционирования в 2 режимах: в режиме автоматической проверки и создания ЭЦП и в режиме проверки и создания ЭЦП под руководством администратора.

69. В режиме проверки и создания ЭЦП под руководством администратора средство ЭЦП должно:

а) при создании ЭЦП:

показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

создавать ЭЦП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭЦП;

однозначно показывать, что ЭЦП создана;

б) при проверке ЭЦП:

показывать содержание электронного документа, подписанного ЭЦП;

показывать информацию о внесении изменений в подписанный ЭЦП электронный документ;

указывать на лицо, с использованием ключа ЭЦП которого подписаны электронные документы.

2. Требования к программному обеспечению средства ЭЦП

70. Программное обеспечение средства ЭЦП не должно содержать средств, позволяющих модифицировать или искажать алгоритмы работы программного обеспечения.

71. Программное обеспечение средства ЭЦП должно использовать только документированные функции операционной системы.

72. Системное программное обеспечение, используемое средством ЭЦП, не должно содержать известных уязвимостей.

73. Исходные тексты программного обеспечения средства ЭЦП должны соответствовать уровню контроля отсутствия недекларированных возможностей, устанавливаемому Комиссией.

74. В состав программного обеспечения средства ЭЦП должен входить механизм, обеспечивающий очистку оперативной и внешней памяти, используемой для хранения защищаемой информации, при освобождении (перераспределении) памяти путем записи маскирующей информации (случайной или псевдослучайной последовательности символов) в память.

75. В состав программного обеспечения средства ЭЦП должны входить компоненты, обеспечивающие экстренное стирание защищаемой информации, перечень и требования к реализации и надежности стирания которой задаются в техническом задании на создание (модернизацию) средства ЭЦП.

76. Исходные тексты программного обеспечения средства ЭЦП должны пройти проверку реализации в них методов и способов защиты информации, противостоящих атакам, осуществляемым нарушителем из сетей общего пользования, являющимся квалифицированным групповым нарушителем, использующим возможности научных центров, анализирующих системное программное обеспечение с целью поиска уязвимостей.

77. Инженерно-криптографическая защита средства ЭЦП должна исключать события, приводящие к возможности проведения успешных атак в условиях возможных неисправностей или сбоев аппаратных средств средства ЭЦП или аппаратного компонента средства вычислительной техники, на котором реализовано средство ЭЦП.

3. Требования к аппаратным средствам средства ЭЦП

78. Реализация целевых функций средства ЭЦП, включая исходный код BIOS, должна быть подтверждена проверкой на основе системы тестов для аппаратных средств, утверждаемой Комиссией.

79. Должна проводиться оценка параметров надежности функционирования аппаратных средств средства ЭЦП.

80. Отсутствие в составе аппаратных средств устройств, предназначенных для негласного получения информации, а также уровень защиты от утечки информации по каналам побочных электромагнитных излучений и наводок должны быть подтверждены проверкой на соответствие требованиям, определяемым уполномоченным органом государства пребывания Комиссии.

81. Для создания и проверки ЭЦП средство ЭЦП должно использовать криптографический модуль, имеющий средства отображения результатов создания и проверки ЭЦП.

4. Требования к обеспечению целостности средства ЭЦП

82. Средство ЭЦП должно содержать механизм контроля несанкционированного случайного и (или) преднамеренного искажения (изменения, модификации) и (или) разрушения информации, средства ЭЦП (далее – контроль целостности).

83. Контроль целостности должен выполняться:

а) при каждой перезагрузке операционной системы до ее загрузки;

б) в процессе функционирования средства ЭЦП (динамический контроль целостности);

в) в ходе регламентных проверок средства ЭЦП в местах эксплуатации (регламентный контроль) в соответствии с периодом, определяемым в техническом задании на создание (модернизацию) средства ЭЦП.

84. Динамический контроль целостности должен выполняться не реже 1 раза в сутки.

85. Механизм регламентного контроля целостности должен входить в состав средства ЭЦП.

86. В составе программных и (или) аппаратных средств доверенной третьей стороны должны иметься средства восстановления целостности средства ЭЦП.

5. Требования к управлению доступом

87. Управление доступом субъектов к различным компонентам и (или) целевым функциям средства ЭЦП должно осуществляться средствами доверенной третьей стороны, в составе которых функционирует данное средство ЭЦП, в соответствии с требованиями к средствам доверенной третьей стороны.

6. Требования к идентификации и аутентификации

88. Средство ЭЦП должно распознавать пользователя средства ЭЦП или процесса, а также выполнять проверку их подлинности.

89. Механизм аутентификации должен блокировать доступ субъектов к функциям средства ЭЦП при отрицательном результате аутентификации.

90. В средстве ЭЦП для любой реализованной процедуры аутентификации должен применяться механизм ограничения количества следующих подряд попыток аутентификации 1 субъекта доступа, число которых не должно превышать 3.

91. При превышении числа следующих подряд попыток аутентификации 1 субъекта доступа над установленным предельным значением доступ этого субъекта доступа к средствам ЭЦП должен быть заблокирован на промежуток времени, устанавливаемый техническим заданием на создание (модернизацию) средства ЭЦП.

92. При доступе к средству ЭЦП должна проводиться двухфакторная аутентификация.

93. Допускается использование механизмов удаленной аутентификации с использованием сертификатов проверки ключей аутентификации на основе криптографических средств, разработанных в соответствии с требованиями к криптографическим средствам, используемым средствами доверенной третьей стороны , утверждаемыми Комиссией.

94. При осуществлении локального доступа к средству ЭЦП аутентификация пользователя средства ЭЦП должна выполняться до перехода в рабочее состояние этого средства ЭЦП (например, до загрузки операционной системы, используемой этим средством).

95. При использовании для локальной аутентификации символьного, периодически изменяемого пароля он должен состоять из не менее 8 символов (при общем количестве символов алфавита не менее 36). Период изменения пароля не должен превышать 3 месяцев.

7. Требования к регистрации событий

96. В состав средства ЭЦП должно входить средство, производящее регистрацию в защищенном электронном журнале событий, связанных с выполнением средством ЭЦП своих целевых функций. Требования к указанному средству и перечень регистрируемых событий определяются и обосновываются в техническом задании на создание (модернизацию) средства ЭЦП.

97. Журнал регистрации событий должен быть доступен только лицам, определенным оператором информационной системы, в которой используется средство ЭЦП. При этом доступ к журналу регистрации событий должен осуществляться только для просмотра записей и для перемещения содержимого журнала регистрации событий на архивные носители. Пользователю средства ЭЦП журнал должен быть доступен только для просмотра.

8. Требования к надежности и устойчивости функционирования средства ЭЦП

98. Должен быть проведен расчет вероятности сбоев и неисправностей аппаратных средств средства ЭЦП, приводящих к невыполнению средством ЭЦП своих функций.

99. Средняя наработка аппаратных средств средства ЭЦП на отказ составляет не менее 20 000 часов.

9. Требования к датчику случайных чисел, используемому в составе средства ЭЦП

100. Выработка ключей ЭЦП и создание ЭЦП должны производиться средством ЭЦП с использованием физического датчика случайных чисел (устройство, вырабатывающее случайную последовательность чисел путем преобразования сигнала случайного процесса, генерируемого недетерминируемой физической системой, устойчивой к реально возможным изменениям внешних условий и своих параметров), являющегося составной частью средства ЭЦП.

101. Для физического датчика случайных чисел, входящего в состав средства ЭЦП, должна быть разработана теоретико-вероятностная модель используемого в таком датчике случайного физического процесса, а также должна быть проведена экспериментальная проверка соответствия указанной модели реализации физического датчика случайных чисел.

102. По параметрам теоретико-вероятностной модели должна быть теоретически обоснована оценка качества выходной последовательности физического датчика случайных чисел, а также должна быть проведена статистическая проверка полученной оценки для реализации физического датчика случайных чисел.

103. При эксплуатации средства ЭЦП должна осуществляться проверка статистического качества выходной последовательности физического датчика случайных чисел. Данная проверка должна осуществляться в ходе регламентных проверок физического датчика случайных чисел (регламентный контроль) и в автоматическом режиме в процессе функционирования средства ЭЦП (динамический контроль).

104. Период регламентного контроля, а также способ проверки статистического качества выходной последовательности физического датчика случайных чисел в ходе регламентного и динамического контроля определяются и обосновываются в техническом задании на создание (модернизацию) средства ЭЦП.

10. Требования к созданию, использованию, хранению и уничтожению ключевой информации

105. Порядок создания, использования, хранения и уничтожения ключевой информации определяется в соответствии с требованиями эксплуатационной документации на средство ЭЦП.

106. Копирование ключевых документов должно осуществляться только в соответствии с эксплуатационной документацией на средство ЭЦП.

107. Копирование информации ключевых документов на носители, не являющиеся специализированными ключевыми носителями, должно осуществляться только после проведения процедуры ее предварительного шифрования, реализуемой встроенной функцией используемого криптографического средства.

108. Криптографические протоколы, обеспечивающие операции с ключевой информацией средства ЭЦП, должны быть реализованы непосредственно в средстве ЭЦП.

109. Сроки действия ключей ЭЦП и ключей проверки ЭЦП, используемых средством ЭЦП, определяются в соответствии с эксплуатационной документацией на средство ЭЦП, но не должны быть более 3 и 7 лет соответственно.

110. В средстве ЭЦП должен быть реализован механизм контроля срока действия ключей ЭЦП.

111. Механизм контроля срока действия ключей ЭЦП должен позволять задавать срок действия ключа ЭЦП и предупреждать о завершении срока действия ключа ЭЦП в течение установленного техническим заданием на создание (модернизацию) средства ЭЦП интервала времени до завершения срока действия ключа ЭЦП, а также блокировать работу средства ЭЦП, срок действия ключа ЭЦП которого завершен.

11. Требования к криптографическим стандартам

112. Средство ЭЦП должно реализовывать только криптографические алгоритмы, идентификаторы которых указаны в приложении № 8 к Положению об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, утвержденному Решением Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125.

12. Требования к проверке действительности сертификата ключа проверки ЭЦП

113. Проверка действительности сертификата ключа проверки ЭЦП должна осуществляться средствами доверенной третьей стороны, в составе которых функционирует данное средство ЭЦП, в соответствии с требованиями к средствам доверенной третьей стороны.

13. Дополнительные требования

114. Исследования средства ЭЦП с целью подтверждения его соответствия настоящим Требованиям должны проводиться с использованием определяемых уполномоченным органом государства пребывания Комиссии числовых значений параметров и характеристик механизмов защиты, реализуемых в средстве ЭЦП.

ПРИЛОЖЕНИЕ № 4
к Требованиям к созданию,

развитию и функционированию
трансграничного пространства
доверия

ТРЕБОВАНИЯ
к средствам электронной цифровой подписи и средствам удостоверяющего центра Евразийской экономической комиссии

I. Общие положения

1. Настоящие Требования определяют требования к средствам электронной цифровой подписи (электронной подписи) (далее – ЭЦП), используемым в интеграционном сегменте Евразийской экономической комиссии (далее – Комиссия) интегрированной информационной системы Евразийского экономического союза (далее – Союз) и информационных системах Комиссии, а также к средствам удостоверяющего центра Комиссии (далее – удостоверяющий центр), предназначенным для обеспечения функционирования подсистем интеграционного сегмента Комиссии интегрированной информационной системы Союза и информационных систем Комиссии, использующих средства ЭЦП.

II. Требования к средствам ЭЦП

1. Требования к функциям средств ЭЦП

2. При создании ЭЦП средства ЭЦП должны:

а) показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

б) создавать ЭЦП после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭЦП;

в) однозначно показывать, что ЭЦП была создана.

3. При проверке ЭЦП средства ЭЦП должны:

а) показывать содержание электронного документа, подписанного ЭЦП;

б) показывать информацию о внесении изменений в подписанный ЭЦП электронный документ;

в) проверять принадлежность ЭЦП, с использованием которой подписан электронный документ, владельцу сертификата ключа проверки ЭЦП.

4. Указанные в пунктах 2 и 3 настоящих Требований требования к функциональности средств ЭЦП реализуются с использованием аппаратных и программных средств, совместно с которыми штатно функционируют средства ЭЦП, которые способны повлиять на выполнение предъявляемых к средствам ЭЦП требований и которые в совокупности представляют собой среду функционирования средств ЭЦП (далее – среда функционирования).

2. Требования к программному обеспечению средств ЭЦП

5. Программное обеспечение средств ЭЦП не должно содержать средств, позволяющих модифицировать или искажать алгоритмы работы программного обеспечения средства ЭЦП.

6. Программное обеспечение средств ЭЦП должно использовать только документированные функции операционной системы.

7. Системное программное обеспечение, используемое средством ЭЦП, не должно содержать известных уязвимостей.

8. Исходные тексты программного обеспечения средств ЭЦП должны пройти проверку на отсутствие недекларированных возможностей. Программное обеспечение средств ЭЦП должно соответствовать уровню контроля отсутствия недекларированных возможностей, определяемому уполномоченными органами государств – членов Союза (далее – государства-члены).

9. В состав программного обеспечения средств ЭЦП должен входить механизм, обеспечивающий очистку оперативной и внешней памяти, используемой для хранения информации ограниченного доступа, при освобождении (перераспределении) памяти путем записи маскирующей информации (случайной или псевдослучайной последовательности символов) в память.

10. Исходные тексты программного обеспечения средств ЭЦП должны пройти проверку реализации методов и способов защиты информации противостояния атакам, осуществляемым нарушителем с использованием штатных средств (при нахождении как за пределами, так и в пределах контролируемой зоны) при наличии у него доступа к средствам вычислительной техники, в которых реализованы средства ЭЦП, а также возможности располагать аппаратными компонентами средства ЭЦП и среды функционирования в объеме, зависящем от мер, направленных на предотвращение и пресечение несанкционированных действий, реализованных в информационной системе, в которой используется средство ЭЦП.

11. Инженерно-криптографическая защита средств ЭЦП должна исключить наступление событий, приводящих к возможности проведения успешных атак в условиях возможного возникновения неисправностей или сбоев аппаратных средств ЭЦП или аппаратного компонента средства вычислительной техники, на котором реализовано программное средство ЭЦП.

3. Требования к аппаратным средствам средств ЭЦП

12. К аппаратным средствам средств ЭЦП предъявляются следующие требования:

а) проведение проверки соответствия реализации целевых функций средств ЭЦП с использованием определяемой Комиссией системы тестов аппаратных средств средств ЭЦП;

б) проведение оценки параметров надежности функционирования аппаратных средств средств ЭЦП;

в) проведение исследований аппаратных средств средств ЭЦП на соответствие определяемым уполномоченным органом государства пребывания Комиссии требованиям к защите от утечки информации по каналам побочных электромагнитных излучений и наводок.

4. Требования к целостности средств ЭЦП

13. В средствах ЭЦП должен реализовываться механизм контроля несанкционированного случайного и (или) преднамеренного искажения (изменения, модификации) и (или) разрушения информации, а также модификации средства ЭЦП (далее – контроль целостности).

14. Контроль целостности должен осуществляться при каждой перезагрузке операционной системы до ее загрузки и в процессе функционирования средства ЭЦП (динамический контроль целостности), а также в ходе регламентных проверок средства ЭЦП в местах эксплуатации (регламентный контроль целостности).

15. Динамический контроль целостности должен выполняться не реже 1 раза в сутки. Механизм регламентного контроля целостности должен реализовываться в составе средства ЭЦП. Периодичность осуществления регламентного контроля целостности должна определяться и обосновываться в технических заданиях на разработку (модернизацию) средств ЭЦП.

16. В состав программных и (или) аппаратных средств удостоверяющего центра должны входить средства восстановления целостности средства ЭЦП.

5. Требования к управлению доступом

17. В состав средств ЭЦП или среды функционирования должны входить компоненты, обеспечивающие управление доступом субъектов доступа к различным компонентам и (или) целевым функциям средств ЭЦП на основе параметров, заданных администраторами информационных систем, в которых используются средства ЭЦП, или разработчиками средств ЭЦП. Требования к указанным компонентам определяются и обосновываются в технических заданиях на разработку (модернизацию) средств ЭЦП.

6. Требования к идентификации и аутентификации

18. Идентификация и аутентификация включают в себя распознавание пользователя средств ЭЦП или процесса, а также проверку их подлинности. Механизм аутентификации при отрицательном результате аутентификации должен блокировать доступ этих субъектов доступа к функциям средств ЭЦП.

19. В средствах ЭЦП для любой реализованной процедуры аутентификации должен применяться механизм ограничения количества следующих подряд попыток аутентификации одного субъекта доступа, число которых не должно превышать 3. При превышении числа следующих подряд попыток аутентификации одного субъекта

доступа доступ этого субъекта доступа к средствам ЭЦП должен быть заблокирован на промежуток времени, который определяется в технических заданиях на разработку (модернизацию) средств ЭЦП.

20. В отношении лиц, осуществляющих доступ к средствам ЭЦП, должна проводиться двухфакторная аутентификация.

21. Допускается применение механизмов удаленной аутентификации на основе разрешенных криптографических алгоритмов с использованием сертификатов аутентификации.

22. При осуществлении локального доступа к средству ЭЦП аутентификация пользователя средства ЭЦП должна выполняться до перехода этого средства в рабочее состояние (например, до загрузки операционной системы, используемой средством ЭЦП).

23. При использовании для локальной аутентификации символьного периодически изменяемого пароля он должен состоять из не менее чем 8 символов (при общем количестве символов алфавита не менее 36). Период изменения пароля не должен превышать 6 месяцев.

7. Требования к регистрации событий

24. В состав средств ЭЦП должно входить средство, осуществляющее регистрацию в защищенном электронном журнале событий, связанных с выполнением средствами ЭЦП своих целевых функций. Требования к указанному средству и перечень регистрируемых событий определяются в технических заданиях на разработку (модернизацию) средств ЭЦП.

25. Электронный журнал регистрации событий должен быть доступен только лицам , определенным оператором информационной системы, в которой используется средство ЭЦП. Доступ к электронному журналу регистрации событий должен предоставляться в целях просмотра записей и перемещения его содержимого на архивные носители. Пользователю средства ЭЦП журнал должен быть доступен только для просмотра.

8. Требования к надежности и устойчивости функционирования средств ЭЦП

26. Производится расчет вероятности сбоев и неисправностей аппаратных средств средств ЭЦП, приводящих к невыполнению средствами ЭЦП своих функций.

27. Средняя наработка аппаратных средств средств ЭЦП на отказ составляет не менее 10 000 ч.

9.Требования к ключевой информации

28. Выработка ключей ЭЦП должна производиться средством ЭЦП с использованием физического датчика случайных чисел (устройство, вырабатывающее случайную последовательность чисел путем преобразования сигнала случайного процесса, генерируемого недетерминируемой физической системой, устойчивой к

реально возможным изменениям внешних условий и своих параметров), входящего в состав средства ЭЦП.

29. Для физического датчика случайных чисел, входящего в состав средства ЭЦП, должна быть разработана теоретико-вероятностная модель используемого в нем случайного физического процесса и экспериментальная проверка соответствия указанной модели реализации соответствующего физического датчика случайных чисел.

На основании параметров теоретико-вероятностной модели должна быть теоретически обоснована оценка качества выходной последовательности физического датчика случайных чисел и проведена статистическая проверка такой оценки в целях реализации физического датчика случайных чисел.

30. При эксплуатации средства ЭЦП должна проводиться статистическая проверка качества выходной последовательности физического датчика случайных чисел. Данная проверка должна проводиться:

а) в ходе проведения регламентных проверок физического датчика случайных чисел (регламентный контроль);

б) в автоматическом режиме в процессе функционирования средства ЭЦП (динамический контроль).

31. Периодичность проведения регламентного контроля и способ статистической проверки качества выходной последовательности физического датчика случайных чисел в ходе осуществления регламентного и динамического контроля определяются в техническом задании на разработку (модернизацию) средства ЭЦП.

32. Порядок создания, использования, хранения и уничтожения ключевой информации определяется в соответствии с требованиями, установленными эксплуатационной документацией на средство ЭЦП, а также законодательством государства-члена, в состав средств доверенной третьей стороны которого входит средство ЭЦП. В отношении средств доверенной третьей стороны Комиссии указанный порядок регламентируется актами органов Союза.

33. Копирование ключевых документов должно осуществляться в соответствии с эксплуатационной документацией на средство ЭЦП. Не допускается копирование ключей ЭЦП на носители (например, жесткий диск), не являющиеся специализированными ключевыми носителями, без их предварительного шифрования.

34. Криптографические протоколы, обеспечивающие проведение операций с ключевой информацией средства ЭЦП, должны быть реализованы в средстве ЭЦП.

35. Сроки действия ключей ЭЦП и ключей проверки ЭЦП, используемых средством ЭЦП, определяются в соответствии с эксплуатационной документацией на средство ЭЦП, но не должны составлять более 1 года и 3 месяцев и 7 лет соответственно.

36. В средстве ЭЦП должен быть реализован механизм контроля срока действия ключа ЭЦП. Механизм контроля срока действия ключа ЭЦП должен позволять задавать срок действия ключа ЭЦП и сигнализировать о завершении срока его действия в течение заданного интервала времени до завершения срока действия ключа ЭЦП, а также блокировать работу средства ЭЦП, срок действия ключа ЭЦП которого завершен . Интервал времени сигнализации о завершении срока действия ключа ЭЦП определятся в техническом задании на разработку (модернизацию) средства ЭЦП.

10. Требования к криптографическим стандартам

37. Средство ЭЦП должно реализовывать криптографические алгоритмы в соответствии с Решением Коллегии Евразийской экономической комиссии от 3 февраля 2015 г. № 10 (ДСП).

11. Требования к проверке действительности сертификата ключа проверки ЭЦП

38. Средство ЭЦП проверяет действительность каждого сертификата из цепочки сертификатов ключей проверки ЭЦП, в том числе действительность ЭЦП, которыми подписаны такие сертификаты. Данная цепочка состоит из корневого самоподписанного сертификата ключа проверки ЭЦП удостоверяющего центра и сертификата ключа проверки ЭЦП, который используется средством ЭЦП для проверки ЭЦП.

12. Дополнительные требования

39. Исследования средств ЭЦП с целью подтверждения их соответствия настоящим Требованиям должны проводиться с использованием числовых значений параметров и характеристик механизмов защиты, реализуемых в средствах ЭЦП, определяемых уполномоченным органом государства пребывания Комиссии.

III. Требования к средствам удостоверяющего центра

1. Требования к программному обеспечению средств удостоверяющего центра

40. Программное обеспечение средств удостоверяющего центра не должно содержать средств, позволяющих модифицировать или искажать алгоритмы работы программных и аппаратных средств удостоверяющего центра.

41. Системное и прикладное программное обеспечение средств удостоверяющего центра не должно содержать известных уязвимостей.

42. Прикладное программное обеспечение средств удостоверяющего центра и программное обеспечение средств криптографической защиты информации,

используемых удостоверяющим центром, должны использовать только документированные функции системного программного обеспечения.

43. Системное и прикладное программное обеспечение средств удостоверяющего центра должно обеспечивать разграничение доступа системного администратора средств удостоверяющего центра, администратора сертификации средств удостоверяющего центра, операторов средств удостоверяющего центра и пользователей удостоверяющего центра к информации, обрабатываемой средствами удостоверяющего центра, в соответствии с правилами разграничения доступа, установленными системным администратором средств удостоверяющего центра.

44. В состав системного и (или) прикладного программного обеспечения средств удостоверяющего центра должен входить механизм, обеспечивающий очистку оперативной и внешней памяти, используемой для хранения информации ограниченного доступа.

45. Исходные тексты системного и прикладного программного обеспечения средств удостоверяющего центра должны пройти проверку реализации методов и способов защиты информации противостояния атакам, для подготовки и проведения которых используются возможности нарушителя, указанные в Модели угроз безопасности информации и действий нарушителя в удостоверяющем центре Евразийской экономической комиссии, утвержденной Решением Коллегии Евразийской экономической комиссии от 30 мая 2017 г. № 58 (ДСП).

46. В состав программного обеспечения средств удостоверяющего центра должен входить механизм, обеспечивающий устойчивость к компьютерным атакам из внешних сетей.

47. Прикладное программное обеспечение средств удостоверяющего центра должно пройти проверку на отсутствие недекларированных возможностей. Программное обеспечение средств удостоверяющего центра должно соответствовать уровню контроля отсутствия недекларированных возможностей, определяемому уполномоченным органом государства пребывания Комиссии.

2. Требования к аппаратным средствам удостоверяющего центра

48. К аппаратным средствам удостоверяющего центра предъявляются следующие требования:

а) проведение проверки соответствия реализации целевых функций удостоверяющего центра с использованием определяемой Комиссией системы тестов аппаратных средств удостоверяющего центра;

б) проведение оценки параметров надежности функционирования аппаратных средств удостоверяющего центра;

в) проведение исследований аппаратных средств удостоверяющего центра на соответствие определяемым уполномоченным органом государства пребывания

Комиссии требованиям к защите от утечки информации по каналам побочных электромагнитных излучений и наводок.

3. Требования к ролевому разграничению

49. В средствах удостоверяющего центра должны реализовываться следующие обязательные роли:

а) системный администратор, в полномочия которого входят инсталляция, конфигурация и поддержка функционирования средств удостоверяющего центра, создание и поддержка профилей членов группы администраторов средств удостоверяющего центра, конфигурация профиля и параметров журнала аудита;

б) администратор сертификации, в полномочия которого входят создание и аннулирование сертификатов ключей проверки ЭЦП;

в) администратор аудита, в полномочия которого входят просмотр и поддержка журнала аудита;

г) оператор, в полномочия которого входят регистрация заявителей и формирование запросов на управление сертификатами ключей проверки ЭЦП.

50. В средствах удостоверяющего центра должен реализовываться механизм, исключающий возможность авторизации одного члена группы администраторов средств удостоверяющего центра с целью использования полномочий различных ролей
.

51. Оператор не должен иметь возможности вносить изменения в журнал аудита.

4. Требования к целостности средств удостоверяющего центра

52. В средствах удостоверяющего центра должен реализовываться механизм контроля целостности, требования к которому определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

53. Контроль целостности должен осуществляться при каждой перезагрузке операционной системы до ее загрузки и в процессе функционирования средств удостоверяющего центра (динамический контроль целостности).

54. Динамический контроль целостности должен выполняться не реже 1 раза в сутки.

55. В состав программных и (или) аппаратных средств удостоверяющего центра должны входить средства восстановления целостности программных средств удостоверяющего центра.

5. Требования к управлению доступом

56. Средства удостоверяющего центра должны обеспечивать реализацию дискреционного и мандатного принципов управления доступом, а также создание замкнутой рабочей среды (программная среда, которая допускает существование в ней только фиксированного набора программ и процессов). Требования к управлению доступом определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

6. Требования к идентификации и аутентификации

57. Идентификация и аутентификация включают в себя распознавание пользователя средств удостоверяющего центра, члена группы администраторов средств удостоверяющего центра или процесса, а также проверку их подлинности. Механизм аутентификации при отрицательном результате аутентификации должен блокировать доступ субъектов доступа к функциям удостоверяющего центра.

58. В средствах удостоверяющего центра для любой реализованной процедуры аутентификации должен применяться механизм ограничения количества следующих подряд попыток аутентификации одного субъекта доступа, число которых не должно быть более 3. При превышении числа следующих подряд попыток аутентификации одного субъекта доступа доступ этого субъекта доступа к средствам удостоверяющего центра должен быть заблокирован на промежуток времени, который определяется в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

59. Описание процедуры регистрации пользователей средств удостоверяющего центра (внесения данных в реестр пользователей средств удостоверяющего центра), в том числе требование о необходимости предъявления пользователем средств удостоверяющего центра при регистрации документов, удостоверяющих личность, должны содержаться в эксплуатационной документации на средства удостоверяющего центра.

60. В отношении лиц, осуществляющих доступ к средствам удостоверяющего центра, должна проводиться двухфакторная аутентификация.

61. В отношении пользователей средств удостоверяющего центра и членов группы администраторов средств удостоверяющего центра допускается использование механизмов удаленной аутентификации на основе разрешенных криптографических алгоритмов с использованием сертификатов аутентификации.

62. При осуществлении локального доступа к средствам удостоверяющего центра аутентификация членов группы администраторов средств удостоверяющего центра должна выполняться до перехода таких средств в рабочее состояние (например, до загрузки базовой операционной системы).

63. При использовании для локальной аутентификации символьного периодически изменяемого пароля он должен состоять из не менее 8 символов (при общем количестве символов алфавита не менее 36). Период изменения пароля не должен превышать 6 месяцев.

7. Требования к защите данных, полученных или передаваемых удостоверяющим центром

64. Самоподписанный сертификат ключа проверки ЭЦП удостоверяющего центра должен храниться способом, исключающим его модификацию или искажение.

65. Средства удостоверяющего центра должны обеспечивать передачу данных, содержащих информацию ограниченного доступа, полученных удостоверяющим

центром или передаваемых из удостоверяющего центра, способом, исключающим несанкционированный доступ к информации.

66. Средства удостоверяющего центра должны реализовывать защиту от навязывания ложных сообщений (действие, воспринимаемое субъектами электронного взаимодействия или средствами удостоверяющего центра как передача истинного сообщения способом, защищенным от несанкционированного доступа) на основе разрешенных криптографических алгоритмов с использованием сертификатов ключа проверки ЭЦП. Требования к процедуре защиты от навязывания ложных сообщений определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

67. Средства удостоверяющего центра должны реализовывать процедуру защищенной передачи пользователем средств удостоверяющего центра первоначального запроса на создание для него сертификата ключа проверки ЭЦП.

68. Средства удостоверяющего центра должны принимать критичную для функционирования удостоверяющего центра информацию, в случае, если она подписана ЭЦП.

69. Компоненты средств удостоверяющего центра должны размещаться в одной контролируемой зоне.

8. Требования к регистрации событий

70. Операционная система средств удостоверяющего центра должна поддерживать ведение журнала аудита, содержащего информацию системных событий. В средствах удостоверяющего центра должен реализовываться механизм выборочной регистрации в журнале аудита событий, связанных с выполнением удостоверяющим центром своих функций.

71. Список регистрируемых событий должен содержаться в эксплуатационной документации на средства удостоверяющего центра.

72. Должны быть приняты меры обнаружения несанкционированного внесения изменений в журнал аудита пользователями средств удостоверяющего центра, не являющимися членами группы администраторов средств удостоверяющего центра.

9. Требования к надежности и устойчивости функционирования средств удостоверяющего центра

73. Требования к надежности и устойчивости функционирования средств удостоверяющего центра определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

74. Производится расчет вероятности возникновения сбоев и неисправностей аппаратных средств удостоверяющего центра, приводящих к невыполнению удостоверяющим центром своих функций.

75. В течение суток вероятность возникновения сбоев и неисправностей аппаратных средств удостоверяющего центра, приводящих к невыполнению удостоверяющим

центром своих функций, не должна превышать аналогичную вероятность возникновения сбоев и неисправностей используемых в составе удостоверяющего центра криптографических средств.

76. Средняя наработка средств удостоверяющего центра (комплексно) на отказ составляет не менее 10 000 ч.

77. Должно осуществляться тестирование устойчивости функционирования средств удостоверяющего центра.

78. Требования к времени восстановления средств удостоверяющего центра после сбоя определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

79. Меры и средства повышения надежности и устойчивости функционирования средств удостоверяющего центра должны предусматривать квотирование ресурсов средств удостоверяющего центра.

10. Требования к созданию, использованию, хранению и уничтожению ключевой информации

80. Порядок создания, использования, хранения и уничтожения ключевой информации, а также сроки ее действия определяются в соответствии с требованиями, установленными эксплуатационной документацией на средства ЭЦП и иные криптографические средства, используемые средствами удостоверяющего центра, и принципами разработки и модернизации шифровальных (криптографических) средств защиты информации, утверждаемыми Комиссией.

81. Копирование ключевой информации должно осуществляться в соответствии с эксплуатационной документацией на используемые криптографические средства. Не допускается копирование информации ключевых документов (криптографических ключей, в том числе ключей ЭЦП) на носители (например, жесткий диск), не являющиеся специализированными ключевыми носителями, без ее предварительного шифрования, которое должно осуществляться с применением встроенной функции используемого средства криптографической защиты информации.

82. Ключ ЭЦП, используемый для подписания создаваемых сертификатов ключей проверки ЭЦП и списков уникальных номеров сертификатов ключей проверки ЭЦП, действие которых в определенный момент времени до истечения срока их действия было прекращено удостоверяющим центром (далее – списки отозванных сертификатов) , не должен использоваться в иных целях.

11. Требования к резервному копированию информации и восстановлению работоспособности средств удостоверяющего центра

83. Средства удостоверяющего центра должны реализовывать функции резервного копирования информации, обрабатываемой средствами удостоверяющего центра, и восстановления работоспособности аппаратных средств удостоверяющего центра в случае повреждения такой информации и таких средств. В ходе резервного

копирования должна быть исключена возможность копирования криптографических ключей.

84. Данные, сохраненные при резервном копировании, должны быть достаточными для восстановления функционирования средств удостоверяющего центра до состояния, зафиксированного на момент копирования данных.

85. Должны быть приняты меры по обнаружению несанкционированных изменений сохраненных данных.

86. Требования к времени восстановления работоспособности средств удостоверяющего центра определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра и в эксплуатационной документации на средства удостоверяющего центра.

12. Требования к созданию и аннулированию сертификатов ключей проверки ЭЦП

87. Протоколы создания и аннулирования сертификатов ключей проверки ЭЦП должны быть описаны в эксплуатационной документации на средства удостоверяющего центра.

88. Создаваемые удостоверяющим центром сертификаты ключей проверки ЭЦП и списки отозванных сертификатов должны соответствовать требованиям, установленным приложением № 5 к Требованиям к созданию, развитию и функционированию трансграничного пространства доверия, утвержденным Решением Совета Евразийской экономической комиссии от 5 декабря 2018 г. № 96.

89. Средства удостоверяющего центра должны реализовывать механизм контроля соответствия создаваемых сертификатов ключей проверки ЭЦП требованиям, установленным приложением № 5 к Требованиям к созданию, развитию и функционированию трансграничного пространства доверия, утвержденным Решением Совета Евразийской экономической комиссии от 5 декабря 2018 г. № 96.

90. Средства удостоверяющего центра должны реализовывать аннулирование сертификата ключа проверки ЭЦП с использованием списков отозванных сертификатов.

91. Средства удостоверяющего центра в отношении владельца сертификата ключа проверки ЭЦП должны реализовывать проверку уникальности ключа проверки ЭЦП и проверку обладания соответствующим ключом ЭЦП.

92. Погрешность значений времени в сертификатах ключей проверки ЭЦП и списках аннулированных сертификатов не должна превышать 10 минут.

13. Требования к реестру выданных, прекративших действие и аннулированных сертификатов ключей проверки ЭЦП и предоставлению доступа к нему

93. В средствах удостоверяющего центра должны быть реализованы механизмы хранения и поиска по атрибутам выданных удостоверяющим центром, прекративших действие и аннулированных сертификатов ключей проверки ЭЦП в реестре выданных, прекративших действие и аннулированных сертификатов ключей проверки ЭЦП (далее

– реестр сертификатов), а также механизмы предоставления сетевого доступа к реестру сертификатов.

94. Все вносимые в реестр сертификатов изменения должны регистрироваться в журнале аудита.

14. Требования к криптографическим средствам

95. Средства удостоверяющего центра должны использовать средства ЭЦП и иные криптографические средства, имеющие заключение уполномоченных органов государства пребывания Комиссии о соответствии требованиям, предъявляемым законодательством государства пребывания Комиссии к криптографическим средствам класса КС3, и принципам разработки и модернизации шифровальных (криптографических) средств защиты информации, утверждаемым Комиссией.

15. Требования к криптографическим стандартам

96. Средства удостоверяющего центра должны использовать криптографические средства, реализующие криптографические алгоритмы в соответствии с Решением Коллегии Евразийской экономической комиссии от 3 февраля 2015 г. № 10 (ДСП).

16. Требования к проверке действительности сертификата ключа проверки ЭЦП

97. Реализованный в средствах удостоверяющего центра механизм проверки ЭЦП в выдаваемых удостоверяющим центром сертификатах ключей проверки ЭЦП должен указываться в эксплуатационной документации на средства удостоверяющего центра. Такой механизм должен обеспечивать проверку ЭЦП в выдаваемых удостоверяющим центром сертификатах ключей проверки ЭЦП после создания сертификата ключа проверки ЭЦП и до его выдачи.

98. Средства удостоверяющего центра проверяют действительность каждого сертификата из цепочки сертификатов ключей проверки ЭЦП, в том числе действительность ЭЦП, которыми подписаны такие сертификаты. Данная цепочка состоит из корневого самоподписанного сертификата ключа проверки ЭЦП удостоверяющего центра и проверяемого сертификата ключа проверки ЭЦП.

17. Дополнительные требования

99. Подключение средств удостоверяющего центра к информационно-телекоммуникационной сети, доступ к которой не ограничен определенным кругом лиц, не допускается.

100. В целях ограничения возможностей построения атак на средства удостоверяющего центра с использованием каналов связи должны применяться средства межсетевого экранирования, применяемые серверами удостоверяющего центра, которые взаимодействуют с пользователями средств удостоверяющего центра.

101. Должны применяться средства защиты от компьютерных вирусов, обеспечивающие обнаружение компьютерных программ или иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования , модификации, копирования защищаемой информации или нейтрализации средств

защиты информации, а также обеспечиваться реагирование на обнаружение таких программ и информации.

102. Средства межсетевого экранирования и средства защиты от компьютерных вирусов должны соответствовать требованиям, определяемым уполномоченным органом государства пребывания Комиссии.

103. Исследования средств удостоверяющего центра с целью подтверждения их соответствия настоящим Требованиям должны проводиться с использованием определяемых уполномоченным органом государства пребывания Комиссии числовых значений параметров и характеристик механизмов защиты информации, реализуемых в средствах удостоверяющего центра.

104. Средства удостоверяющего центра должны эксплуатироваться в соответствии с эксплуатационной документацией на них. Организационно-технические мероприятия, необходимые для обеспечения безопасного функционирования средств удостоверяющего центра, должны указываться в эксплуатационной документации на средства удостоверяющего центра.

ПРИЛОЖЕНИЕ № 5
к Требованиям к созданию,
развитию
и функционированию
трансграничного пространства
доверия

ТРЕБОВАНИЯ
к мерам и способам обеспечения защиты информации

I. Общие положения

1. Настоящие Требования содержат описание мер и способов обеспечения защиты информации, которые должны реализоваться операторами общей инфраструктуры документирования информации в электронном виде в отношении элементов трансграничного пространства доверия и предоставляемых ими сервисов, эксплуатацию которых обеспечивает оператор общей инфраструктуры документирования информации в электронном виде (далее – объект защиты).

2. Защита элементов и сервисов интеграционного компонента общей инфраструктуры документирования информации в электронном виде осуществляется в соответствии с настоящими Требованиями.

3. Защита элементов и сервисов государственных компонентов общей инфраструктуры документирования информации в электронном виде осуществляется в соответствии с законодательством государств – членов Евразийского экономического союза или в соответствии с международными стандартами в области информационной безопасности и настоящими Требованиями.

4. Настоящие Требования определяют минимально необходимые требования к мерам и способам защиты информации, реализуемым на объектах защиты, и включают в себя:

а) требования к обеспечению физической защиты;

б) требования к обеспечению защиты от вредоносного программного обеспечения;

в) требования к обеспечению резервного копирования;

г) требования к учету событий и инцидентов информационной безопасности;

д) требования к контролю защищенности технических средств, программного обеспечения и информационных активов объекта защиты;

е) требования к работе со средствами криптографической защиты;

ж) требования к управлению доступом.

5. В целях реализации настоящих Требований для каждого элемента трансграничного пространства доверия операторами общей инфраструктуры документирования информации в электронном виде должна быть разработана соответствующая документация, которая должна подвергаться регулярному пересмотру и актуализации.

6. Лица, имеющие доступ к эксплуатации и сопровождению элементов трансграничного пространства доверия должны быть ознакомлены с указанной в пункте 5 настоящих Требований документацией в рамках свой компетенции.

II. Требования к обеспечению физической защиты

7. Для объекта защиты должны быть определены контролируемые зоны, доступ в которые должен быть ограничен физически, в том числе средствами системы контроля доступа.

8. Должен быть определен перечень лиц, которым разрешен доступ к объекту защиты, с указанием их ролей (уровней доступа).

9. Должна быть исключена возможность получения доступа к информации для посторонних лиц через средства отображения информации.

10. Перемещение посторонних лиц по территории контролируемой зоны должно быть запрещено.

11. Размещение средств вычислительной техники, посредством которой осуществляется обработка данных объекта защиты вне контролируемой зоны, должно быть запрещено.

12. Внос (вынос) средств вычислительной техники и средств хранения информации в контролируемую зону (из контролируемой зоны) должен регистрироваться в специальных журналах.

13. Документация о физической защите объекта защиты и контроле доступа должна содержать:

а) порядок обустройства контролируемых зон ограниченного доступа;

б) порядок ведения перечня лиц, которым разрешен доступ к объекту защиты, с указанием их ролей (уровней доступа);

в) порядок получения доступа в контролируемую зону и контроля перемещения по ней посторонних лиц;

г) порядок вноса (выноса) средств вычислительной техники и средств хранения информации в контролируемую зону (из контролируемой зоны);

д) описание ролей пользователей, имеющих доступ к элементам объекта защиты, находящимся в контролируемой зоне;

е) описание политики управления доступом, которая устанавливает набор допустимых операций пользователей различных ролей с сервисами и сервисов, выступающих от имени пользователей, с элементами и сервисами объекта защиты.

III. Требования к обеспечению защиты от вредоносного программного обеспечения

14. На всех серверах и рабочих станциях объекта защиты должны быть предусмотрены и должны выполняться меры защиты от вредоносного программного обеспечения.

15. Должна регулярно проводиться проверка серверов и рабочих станций объекта защиты на предмет наличия вредоносного программного обеспечения.

16. Отключение средств защиты от вредоносного программного обеспечения должно быть запрещено.

17. Должно проводиться регулярное обновление средств защиты от вредоносного программного обеспечения.

18. Все события по обнаружению вредоносного программного обеспечения должны протоколироваться.

19. Документация о защите объекта защиты от вредоносного программного обеспечения должна содержать:

а) требования к составу средств защиты объекта защиты от вредоносного программного обеспечения;

б) регламент проведения работ по защите объекта защиты от вредоносного программного обеспечения;

в) порядок действий персонала при выявлении вредоносного программного обеспечения;

г) порядок регистрации событий выявления и устранения вредоносного программного обеспечения;

д) порядок тестирования работоспособности средств защиты объекта от вредоносного программного обеспечения.

IV. Требования к обеспечению резервного копирования

20. В составе средств вычислительной техники объекта защиты должны быть предусмотрены средства копирования и восстановления данных, средства управления и учета резервных копий, средства хранения данных, носители информации, используемые для хранения резервных копий.

21. Все события резервного копирования должны регистрироваться в специальных журналах.

22. Должно проводиться регулярное тестирование работоспособности средств резервного копирования.

23. Документация о проведении резервного копирования данных должна содержать:

а) требования к составу средств копирования и восстановления данных;

б) регламент проведения работ по резервному копированию информации;

в) порядок действий персонала при возникновении необходимости восстановления данных из резервных копий;

г) порядок регистрации событий резервного копирования и восстановления данных;

д) порядок тестирования работоспособности средств резервного копирования.

V. Требования к учету событий и инцидентов информационной безопасности

24. Должен вестись учет событий и инцидентов информационной безопасности.

25. Должен быть разработан порядок обработки событий и инцидентов информационной безопасности.

26. Должны быть определены лица, ответственные за обработку событий и инцидентов информационной безопасности.

27. Документация о регистрации и учете событий и инцидентов информационной безопасности должна содержать:

а) порядок учета событий и инцидентов информационной безопасности;

б) политику обработки событий и инцидентов;

в) порядок назначения и описание действий лиц, ответственных за обработку событий и инцидентов.

VI. Требования к контролю защищенности технических средств, программного обеспечения и информационных активов объекта защиты

28. Должна проводиться регулярная инвентаризация элементов объекта защиты: технических средств, программного обеспечения и информационных активов, развернутых на объекте защиты, – а также должны фиксироваться все изменения, происходящие с объектом защиты.

29. Должен проводиться контроль уязвимостей, включающий в себя обнаружение уязвимостей (постоянное отслеживание уязвимостей), оценку угроз безопасности,

связанных с обнаруженными уязвимостями, принятие мер защиты по устранению (изоляции) уязвимостей.

30. Документация о контроле защищенности технических средств, программного обеспечения и информационных активов, развернутых на объекте защиты, должна содержать:

а) порядок проведения регулярной инвентаризации элементов объекта защиты: технических средств, программного обеспечения и информационных активов, развернутых на объекте защиты;

б) порядок проведения контроля уязвимостей, включающий в себя отслеживание уязвимостей, оценку угроз безопасности, связанных с обнаруженными уязвимостями, принятие мер защиты по устранению (изоляции) уязвимостей;

в) описание защитных мер.

VII. Требования к работе со средствами криптографической защиты информации

31. Должен осуществляться контроль целостности компонентов средств криптографической защиты информации.

32. Должны быть определены и корректно реализованы криптографические методы обеспечения контроля целостности компонентов средств защиты информации.

33. Должны быть определены и корректно реализованы аппаратные методы защиты информации.

34. Должны быть определены и корректно реализованы методы разделения секрета.

35. При экспорте данных из средств криптографической защиты информации должна устанавливаться защита таких данных и должен проводиться контроль целостности.

36. Все сеансовые критические объекты должны очищаться до завершения сеансов.

37. Должны использоваться только сертифицированные средства криптографической защиты информации.

38. Места хранения средств криптографической защиты информации должны быть оборудованы специальными средствами защиты, исключающими возможность любых способов доступа к таким местам посторонних лиц, включая физическую защиту от проникновения, защиту средств визуализации информации, защиту на уровне сетевого доступа и другие средства защиты.

39. Должен производиться поэкземплярный учет хранящихся средств криптографической защиты информации.

40. Должна выполняться регистрация всех работ обслуживающего персонала с средствами криптографической защиты информации в специальных журналах.

41. Должны быть оборудованы специальные хранилища (сейфы) для съемных носителей, хранящих ключи ЭЦП.

42. Эксплуатация средств криптографической защиты информации должна выполняться лицами, прошедшими подготовку и изучившими эксплуатационную документацию на средства криптографической защиты информации.

43. Документация о работе со средствами криптографической защиты информации должна содержать:

а) регламент осуществления контроля целостности компонентов средств криптографической защиты информации;

б) требования к реализации криптографических методов обеспечения контроля целостности компонентов средств криптографической защиты информации, аппаратных методов защиты;

в) требования к защите и контролю целостности при экспорте данных из средств криптографической защиты информации;

г) перечень сертифицированных средств криптографической защиты информации;

д) требования к оборудованию мест хранения средств криптографической защиты информации специальными средствами защиты, исключающими возможность любых способов доступа к ним посторонних лиц, включая физическую защиту от проникновения, защиту средств визуализации информации, защиту на уровне сетевого доступа и другие средства защиты;

е) порядок учета хранящихся средств криптографической защиты информации;

ж) порядок регистрации всех работ со средствами криптографической защиты информации;

з) требования к подготовке лиц, выполняющих эксплуатацию средств криптографической защиты информации.

VIII. Требования к управлению доступом

44. Для обеспечения управления доступом должны быть определены роли пользователей.

45. Операторами общей инфраструктуры документирования информации в электронном виде должен быть определен порядок управления доступом, который устанавливает набор допустимых операций пользователей различных ролей с сервисами и сервисов, выступающих от имени пользователей, с объектами и другими сервисами.