ПРИЛОЖЕНИЕ № 3

к Требованиям к созданию, развитию
и функционированию трансграничного
пространства доверия

Т Р Е Б О В А Н И Я
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, в полномочия которого входят управление созданием и проверкой ЭЦП, используемыми для подписания квитанций с результатами проверки ЭЦП электронных документов;

в) администратор информационной безопасности, в полномочия которого входят контроль и обеспечение функционирования средств защиты информации, анализ и мониторинг состояния защищенности средств доверенной третьей стороны, выполнение и контроль за выполнением организационных мер защиты;

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

д) оператор, в полномочия которого входят резервное копирование и восстановление информации, хранимой в средствах доверенной третьей стороны.

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.