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 резервное копирование и восстановление информации, хранимой в средствах удостоверяющего центра.

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 2017 г. № .

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 2017 г. № .

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.