

Утверждено:  
Служба информации и  
безопасности Республики Молдова  
приказ № 13 от 3 апреля 2006 г.

Зарегистрировано:  
Министерство юстиции  
Республики Молдова  
рег. номер 452 от 21 июня 2006 г.

\_\_\_\_\_ Ион УРСУ

\_\_\_\_\_ Виктория ИФТОДИ

Приложение № 2  
к Приказу директора Службы  
информации и безопасности  
Республики Молдова  
№ 13 от 3 апреля 2006 г.

## **Специальные условия деятельности центров сертификации открытых ключей**

### **I. Общие положения**

1. Специальные условия деятельности центров сертификации открытых ключей (далее – специальные условия) разработаны в соответствии с Законом об электронном документе и цифровой подписи № 264-XV от 15 июля 2004 г. и Постановлением Правительства № 945 от 5 сентября 2005 г. "О центрах сертификации открытых ключей".

2. Специальные условия устанавливают общие требования, предъявляемые к центрам сертификации, их инфраструктуре и организации основных процедур, к системе управления информационной безопасностью, а также требования по регистрации, организации и проверки деятельности центров сертификации.

3. Специальные условия являются регламентирующим документом в сфере цифровой подписи и обязательны для всех юридических лиц, оказывающих услуги по сертификации открытых ключей и иные виды услуг, связанных с цифровой подписью.

4. В настоящих специальных условиях используются следующие понятия:

*пользователь цифровой подписи* – юридическое или физическое лицо, а также устройство или приложение, пользующееся услугами центра сертификации;

*идентификация* – присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

*аутентификация* – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности;

*целостность* – достоверность, непротиворечивость и актуальность информации, ее защищенность от разрушения и несанкционированного изменения;

*доступность* – возможность получить требуемую информацию или информационную услугу в течение удовлетворяющего стороны периода времени;

*конфиденциальность* – защита информации от несанкционированного разглашения;

*средства криптографической защиты информации (СКЗИ)* – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации, предназначенные для защиты целостности и конфиденциальности информации при ее обработке, хранении и передаче по каналам связи;

*список отозванных сертификатов* – созданный центром сертификации список сертификатов открытых ключей, действие которых приостановлено или прекращено до окончания срока их действия;

*криптографическая и техническая защита информации* – защита информации с применением специальных математических (криптографических) методов, программных, технических, программно-технических и иных средств, а также организационно-технических процедур;

*защита информации от утечки* – комплекс мер, направленных на предотвращение неконтролируемого распространения защищаемой информации по техническим и побочным каналам с помощью специальных технических средств;

*защита информации от несанкционированного доступа* – комплекс мер, направленных на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением прав или правил доступа к защищаемой информации, установленных правовыми документами или собственником (владельцем) информации;

*защита информации от непреднамеренного воздействия* – комплекс мер, направленных на предотвращение непреднамеренного воздействия на защищаемую информацию вследствие ошибок пользователя, сбоев программно-технических средств, природных явлений или иных причин, не целенаправленных на изменение информации, но приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к ее утрате, уничтожению или сбою функционирования материального носителя информации;

*политика безопасности* – совокупность документированных управленческих решений, направленных на защиту информации, технических и программных средств информационных систем.

## **II. Услуги и процедуры центра сертификации**

5. Центр сертификации оказывает обязательные и необязательные услуги в сфере цифровой подписи.

6. Обязательной услугой центра сертификации является услуга по сертификации открытых ключей физических лиц.

7. Центр сертификации может оказывать следующие необязательные услуги:

а) сертификация открытых ключей уполномоченных лиц центров сертификации третьего уровня (только для центров сертификации второго уровня);

б) сертификация открытых ключей услуг, предоставляемых в информационной сфере (информационные услуги e-mail, VPN, web и т.д.);

с) фиксирование времени наступления событий, в том числе фиксирование времени подписания электронного документа;

д) другие услуги в сфере цифровой подписи.

8. В процессе предоставления услуг по сертификации открытых ключей физических лиц центр сертификации должен обеспечить выполнение следующих процедур:

а) регистрация физического лица;

б) создание (выпуск) сертификата открытого ключа физического лица;

с) приостановление действия сертификата открытого ключа физического лица;

д) возобновление действия сертификата открытого ключа физического лица;

е) отзыв сертификата открытого ключа физического лица;

ф) публикация сертификатов открытых ключей;

г) распространение информации о приостановленных и отозванных сертификатах (списков отозванных сертификатов);

9. Центр сертификации обеспечивает процесс администрирования (управления) сертификатами открытых ключей путем комплексного выполнения указанных процедур.

### **III. Общие требования, предъявляемые к центру сертификации**

10. Объекты, используемые центром сертификации, должны принадлежать ему на правах собственности, находиться в аренде, хозяйственном управлении или пользовании.

11. Центр сертификации должен использовать средства цифровой подписи, имеющие сертификат соответствия, выданный в соответствии с действующим законодательством.

12. Организация внутреннего режима работы центра сертификации должна исключать возможность несанкционированного физического доступа к средствам цифровой подписи, их несанкционированное использование или модификацию.

13. Центр сертификации должен создать необходимые условия для обеспечения безопасности открытого и закрытого ключей уполномоченных лиц центра сертификации и реестра сертификатов открытых ключей.

14. Центр сертификации должен обеспечить использование закрытого ключа уполномоченного лица центра сертификации только для подписания выдаваемых им сертификатов открытых ключей и списков отозванных сертификатов.

15. Центр сертификации должен исключить возможность использования закрытого ключа уполномоченного лица центра сертификации при наличии оснований полагать, что нарушена конфиденциальность соответствующего закрытого ключа.

16. Центр сертификации должен разработать и утвердить политику сертификации, содержащую набор правил, определяющих использование сертификата, выданного центром сертификации в соответствии с установленными требованиями по безопасности.

17. Центр сертификации должен разработать и утвердить Регламент центра сертификации, устанавливающий организационные, технические и другие условия деятельности центра сертификации при предоставлении услуг по сертификации открытых ключей.

18. Регламент центра сертификации должен содержать:

- a) перечень услуг центра сертификации и порядок их оказания;
- b) функции, обязанности и права центра сертификации;
- c) права и обязанности пользователей цифровой подписи;
- d) финансовые обязательства центра сертификации;
- e) ответственность сторон;
- f) основные организационно-технические мероприятия по обеспечению безопасности центра сертификации, включая политику конфиденциальности;
- g) процедуры центра сертификации;
- h) порядок публикации и распространения информации;
- i) порядок осуществления доступа к информационным ресурсам центра сертификации;
- j) порядок архивного хранения документированной информации;
- k) процедуры управления ключами уполномоченных лиц центра сертификации;
- l) порядок действий в случае компрометации закрытого ключа уполномоченного лица центра сертификации и пользователя цифровой подписи;
- m) описание принятых в центре сертификации форматов данных;
- n) структуру сертификата открытого ключа уполномоченного лица центра сертификации;
- o) структуру сертификатов открытых ключей пользователей цифровой подписи;
- p) структуру списка отозванных сертификатов;
- q) порядок синхронизации времени;
- r) порядок разрешения спорных ситуаций в сфере применения цифровой подписи;
- s) порядок доведения до пользователей цифровой подписи политики сертификации и содержания Регламента центра сертификации.

19. Политика сертификации и Регламент центра сертификации должны соответствовать рекомендациям IETF (Internet Engineering Task Force) RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).

20. Центр сертификации должен исключить возможность разглашения регистрационной информации пользователей цифровой подписи, за исключением информации, которая используется для идентификации их сертификатов открытых ключей и публикуется путем включения в сертификаты пользователей цифровой подписи.

21. Режим конфиденциальности при обращении со сведениями, которые доверены или стали известны центру сертификации при осуществлении его деятельности, должен обеспечивать:

а) ограничение круга должностных лиц, имеющих доступ к конфиденциальной информации;

б) порядок контролируемого допуска должностных лиц к работам, связанным с конфиденциальной информацией;

с) функциональное разграничение обязанностей должностных лиц;

д) идентификацию и аутентификацию пользователей цифровой подписи с использованием современных средств аутентификации и криптографических протоколов;

е) разграничение доступа субъектов к различным объектам и/или целевым функциям центра сертификации на основе идентификации субъектов и их функционального разграничения;

ф) безопасность хранения, обработки и передачи по каналам связи конфиденциальной информации.

22. Центр сертификации должен обеспечить управление доступом субъектов к различным объектам и/или целевым функциям центра сертификации на основе идентификации субъектов и их функционального разграничения.

23. Центр сертификации должен обеспечить резервное копирование, сохранение и восстановление критически важной для своей деятельности информации, а также установление, в случае необходимости, дополнительных или резервных технических ресурсов.

24. Центр сертификации должен располагать достаточным персоналом, обладающим необходимой квалификацией, для функционирования и обеспечения безопасности центра сертификации.

25. Центр сертификации должен выполнять свои функции на основе принципа разделения привилегий (обязанностей) должностных лиц: администратора регистрации, администратора сертификации, администратора безопасности и системного администратора.

26. Администратор регистрации отвечает за правильность (достоверность) информационного наполнения сертификата открытого ключа и регистрацию владельцев сертификатов открытых ключей в процессе создания, приостановления или возобновления действия, а также отзыва сертификатов открытых ключей.

27. Администратор сертификации (уполномоченное лицо центра сертификации) отвечает за создание, приостановление или возобновление действия и отзыв сертификатов открытых ключей, ведение реестра

сертификатов открытых ключей, безопасное хранение и использование своего закрытого ключа.

28. Администратор безопасности отвечает за надлежащее функционирование комплексной системы защиты информации, а также разработку и реализацию политики безопасности центра сертификации.

29. Системный администратор отвечает за администрирование, надлежащее функционирование и обеспечение безопасности программно-технического комплекса центра сертификации.

30. В случае необходимости в центре сертификации могут быть введены дополнительные должности, в частности, операторов.

31. Операторы выполняют работу по ежедневному обслуживанию программно-технического комплекса центра сертификации (копирование и восстановление системы, ведение архивов, ввод информации и пр.).

32. Центр сертификации должен исключить совмещение функций администратора регистрации, администратора сертификации, администратора безопасности, системного администратора и оператора.

33. Центр сертификации должен синхронизировать работу своих служб, в том числе программных и технических средств по назначению, с Всемирным координированным временем (UTC). Рекомендуется использовать два независимых источника UTC. Допускается синхронизация по Гринвичскому среднему времени (Greenwich Mean Time – GMT).

#### **IV. Требования к основным процедурам центра сертификации**

##### ***Раздел 1. Требования к процедуре регистрации физического лица***

34. Регистрацию физических лиц выполняет администратор регистрации, управляющий данными о владельце сертификата открытого ключа.

35. Администратор регистрации проводит идентификацию физического лица, подавшего заявление на сертификацию своего открытого ключа в соответствии с утвержденными центром сертификации процедурами.

36. Администратор регистрации должен установить:

а) соответствие процесса составления и подачи заявления положениям Закона об электронном документе и цифровой подписи, Регламента центра сертификации и других нормативных документов в сфере применения цифровой подписи;

б) подлинность и действительность представленной в заявлении информации;

с) соответствие информации, представленной в заявлении в форме электронного документа, информации, представленной в заявлении в виде документа на бумажном носителе;

д) соблюдение прав третьих лиц.

37. Администратор регистрации должен удостовериться, что физическое лицо, подавшее заявление на сертификацию открытого ключа, является владельцем соответствующего закрытого ключа.

38. Электронные документы администратора регистрации должны быть подписаны цифровой подписью, содержать метки времени, определяющие момент создания электронных документов, и передаваться с использованием систем, обеспечивающих конфиденциальность сообщений.

39. Центр сертификации должен обеспечить защиту конфиденциальной информации о владельцах сертификатов открытых ключей.

## ***Раздел 2. Требования к процедуре сертификации открытого ключа***

40. Центр сертификации создает и выдает сертификаты открытых ключей в соответствии с утвержденными центром сертификации процедурами.

41. Центр сертификации должен разработать и утвердить политику и процедуры сертификации открытых ключей в соответствии с установленными техническими нормами в сфере цифровой подписи.

42. Создание сертификата открытого ключа физического лица осуществляется администратором сертификации (уполномоченным лицом центра сертификации).

43. Администратор сертификации должен проверить целостность и достоверность данных, поступивших от администратора регистрации, а также их соответствие установленному стандарту сертификатов открытых ключей.

44. Центр сертификации должен обеспечить достоверность информации, содержащуюся в сертификате открытого ключа, а также целостность сертификата.

45. Сертификат открытого ключа должен соответствовать утвержденным в центре сертификации профилям, соответствующим политике сертификации.

46. Центр сертификации должен внести сертификат открытого ключа в реестр сертификатов не позднее даты и времени начала действия сертификата.

47. Закрытый ключ администратора сертификации должен использоваться только для подписания выдаваемых им сертификатов открытых ключей и списков отозванных сертификатов (CRL).

## ***Раздел 3. Требования к процедурам приостановления, возобновления действия и отзыва сертификата открытого ключа***

48. Центр сертификации приостанавливает, возобновляет действие или отзывает сертификат открытого ключа в случаях, установленных нормативными документами в сфере цифровой подписи.

49. Центр сертификации должен разработать и утвердить процедуры приостановления, возобновления действия и отзыва сертификатов открытых ключей в соответствии с техническими нормами, установленными в сфере цифровой подписи.

50. Центр сертификации должен разработать и утвердить безопасные процедуры аутентификации лица, заявившего о намерении приостановить, возобновить действие или отозвать свой сертификат открытого ключа, а также

процедуры подтверждения действительности заявления о приостановлении, возобновлении действия или отзыве сертификата открытого ключа.

51. Центр сертификации незамедлительно приостанавливает действие сертификата открытого ключа при наличии оснований полагать, что нарушена конфиденциальность закрытого ключа владельца сертификата или содержащаяся в сертификате открытого ключа информация не соответствует действительности.

52. Центр сертификации отзывает сертификат открытого ключа в случае установления факта нарушения конфиденциальности закрытого ключа владельца сертификата или несоответствия действительности информации, содержащейся в сертификате открытого ключа.

53. Приостановление, возобновление действия и отзыв сертификата открытого ключа осуществляется администратором сертификации под обязательным контролем со стороны администратора безопасности или другого должностного лица, назначенного руководителем центра сертификации.

54. Центр сертификации должен занести сведения об отозванном или приостановленном сертификате в список отозванных сертификатов в течение 3 рабочих часов с указанием даты и времени занесения и причины отзыва или приостановления действия сертификата.

55. Центр сертификации должен исключить возможность возобновления действия отозванного сертификата открытого ключа.

56. Сертификат открытого ключа, действие которого было возобновлено, в течение 3 рабочих часов удаляется из списка отозванных сертификатов.

57. Центр сертификации должен обеспечить процедуру своевременного выпуска обновленного списка отозванных сертификатов.

58. Центр сертификации должен разработать и утвердить процедуру уведомления владельца сертификата открытого ключа о приостановлении, возобновлении действия или отзыве сертификата.

#### ***Раздел 4. Требования к процедурам публикации сертификатов открытых ключей и распространения информации о приостановленных и отозванных сертификатах открытых ключей***

59. Распространение (публикация) сертификатов открытых ключей осуществляется в соответствии с установленными центром сертификации процедурами, а доступ третьих лиц может ограничиваться, если того требует владелец сертификата.

60. Центр сертификации должен разработать и утвердить политику контроля доступа к сертификатам открытых ключей, выданных центром сертификации.

61. Доступ к сертификатам открытых ключей должен предоставляться только лицам, имеющим на это право в соответствии с правилами, установленными политикой безопасности центра сертификации или владельцами сертификатов.

62. Центр сертификации должен предоставлять любому лицу информацию о состоянии сертификатов открытых ключей.

63. Центр сертификации должен предоставлять информацию о состоянии сертификатов открытых ключей в режиме реального времени (on-line), а также в других режимах, установленных центром сертификации, включая абонентскую рассылку списков отозванных сертификатов (off-line).

64. Центр сертификации должен обеспечить целостность и подлинность отправляемых сообщений в процессе проверки состояния сертификатов открытых ключей. Все ответы, касающиеся состояния сертификатов, должны быть подписаны цифровой подписью уполномоченного лица центра сертификации.

65. Центр сертификации может требовать, чтобы третьи лица подписывали цифровой подписью свои запросы относительно состояния сертификатов открытых ключей.

66. Центр сертификации может предоставлять ответ на запросы о состоянии сертификата открытого ключа, используя данные, которые были обновлены во время последнего периодического оповещения пользователей.

67. Центр сертификации должен опубликовывать сертификаты открытых ключей своих уполномоченных лиц.

68. Информация, содержащаяся в реестре сертификатов открытых ключей, должна быть защищена от несанкционированного доступа, изменения или уничтожения.

69. Центр сертификации должен установить порядок доступа с правом внесения записи или изменения в реестр сертификатов открытых ключей для лиц, имеющих такое право в соответствии с их функциональными обязанностями.

70. Центр сертификации должен использовать механизмы аутентификации субъектов, имеющих доступ к соответствующей информации в реестре сертификатов открытых ключей.

## **V. Требования к инфраструктуре центра сертификации**

### ***Раздел 1. Требования к помещениям***

71. Помещения центра сертификации должны обеспечивать стабильную работу программно-технического комплекса, систем связи и других технических компонентов, систем энерго-, водо- и теплоснабжения, кондиционирования воздуха, противопожарных систем, обеспечивать защищенность персонала и способствовать предотвращению хищений, утери и несанкционированной модификации, уничтожения данных и программно-технических средств.

72. Помещения центра сертификации должны соответствовать требованиям санитарных норм, по безопасности труда и охраны окружающей среды, установленным действующим законодательством.

73. Помещения центра сертификации должны находиться в зоне безопасности (зона, в которой имеют право находиться только сотрудники организации, в составе которой действует центр сертификации) и быть оборудованы в соответствии с требованиями по обеспечению безопасности.

74. К помещениям специального режима (далее – специальные помещения) центра сертификации относятся помещения, в которых установлены основные технические средства программно-технического комплекса (серверные помещения), хранятся материальные носители, содержащие: резервные копии реестра сертификатов открытых ключей, резервные копии системного и прикладного программного обеспечения, закрытые ключи сотрудников центра сертификации или секретные ключи других криптографических систем центра сертификации.

75. Специальные помещения центра сертификации должны:

а) соответствовать условиям максимальной безопасности, установленным настоящими специальными условиями, для обеспечения физической безопасности и технической защиты информации;

б) быть оборудованными автономными средствами и системами пожарной сигнализации, автоматического пожаротушения и удаления дыма согласно нормативам NCM.E.03.03-2003 "Dotarea clădirilor și instalațiilor cu sisteme autonome de semnalizare și stingere a incendiilor" и NCM.E.03.05-2004 "Instalații autonome de stingere și semnalizare a incendiilor. Normativ pentru proiectare";

с) отвечать требованиям, действующим в Республике Молдова, по проектированию и эксплуатации электрической сети, согласно нормам, предусмотренным в Правилах устройства электроустановок, Правилах технической эксплуатации электроустановок потребителей и Правилах техники безопасности при эксплуатации электроустановок потребителей;

д) обеспечивать работу основных технических средств в течение не менее 30 минут после прекращения основного электроснабжения;

е) оборудоваться средствами вентиляции и кондиционирования воздуха, имеющими сертификат соответствия, выданный в соответствии с действующим законодательством.

76. В помещениях, предназначенных для хранения документации и резервных копий реестра сертификатов открытых ключей, должны устанавливаться металлические хранилища.

## ***Раздел 2. Требования к программно-техническому комплексу***

77. Программно-технический комплекс центра сертификации должен обеспечивать выполнение центром функций по сертификации открытых ключей и соответствовать техническим нормам в сфере цифровой подписи.

78. Эксплуатация программно-технического комплекса центра сертификации должна осуществляться в соответствии с установленными требованиями по обеспечению безопасности.

79. Технические средства программно-технического комплекса, используемые центром сертификации, должны быть собственностью центра, либо быть арендованными или полученными в пользование на основании письменного договора.

80. Каждое техническое средство должно быть зарегистрировано и проверено на возможность его эксплуатации, каждое техническое и программное средство должно быть снабжено технической документацией.

81. Работоспособность технических средств должна периодически проверяться на протяжении всего цикла функционирования, а результаты проверок должны документироваться.

82. Все технические средства должны быть обеспечены возможностью ремонта. Для аппаратуры, требующей периодического технического обслуживания, должны быть разработаны соответствующие инструкции и графики технического обслуживания. Все оборудование и контрольно-измерительная аппаратура должны содержаться в условиях, обеспечивающих их сохранность.

83. Программно-технический комплекс центра сертификации должен обеспечивать возможность резервного копирования и сохранения критически важной для деятельности центра сертификации информации, ее быстрого и целостного восстановления в случае отказов, сбоев и ошибок в системе, а также установки, при необходимости, дополнительных или резервных технических ресурсов.

84. В своей деятельности центр сертификации должен использовать только свободно распространяемое или лицензионное программное обеспечение.

85. Центр сертификации обязан обеспечить управление программно-техническим комплексом или его отдельными подсистемами только лицами, наделенными полномочиями администрирования, а также исключить несанкционированное изменение конфигурации оборудования, системных настроек, алгоритмов работы программных средств, изменение поддерживаемых информационных потоков или процессов.

### ***Раздел 3. Требования к персоналу***

86. Центр сертификации должен располагать штатом сотрудников, количественный состав, профессиональная подготовка, опыт работы и квалификация которых должны быть на уровне, позволяющем решать весь комплекс задач по предоставлению услуг в области цифровой подписи.

87. Расстановка кадров центра сертификации должна быть отражена в соответствующей организационной структуре и номенклатуре должностей, утвержденных руководителем юридического лица. Уровень квалификации каждого специалиста должен быть подтвержден документально.

88. Для каждого специалиста центра сертификации должны быть установлены конкретные требования по образованию, техническим знаниям и опыту работы. Должны быть также определены должностные обязанности,

функции, права, ответственность и требования по режиму конфиденциальности.

89. Каждый сотрудник центра сертификации обязан знать и выполнять свои должностные обязанности, периодически повышать свою квалификацию, осваивать смежные профессии по профилю своей деятельности.

90. Центр сертификации должен периодически проводить проверку и оценку уровня квалификации специалистов и обеспечивать повышение этого уровня.

91. При отсутствии специалистов для выполнения специальных работ центр сертификации может привлекать сотрудников других организаций с обеспечением установленных требований по безопасности.

92. Сотрудники центра сертификации должны подписывать обязательства о конфиденциальности, в соответствии со статьей 53 Трудового кодекса Республики Молдова, а также, при необходимости, обязательства о неразглашении коммерческой тайны, распространяющиеся как на период действия заключенного индивидуального трудового договора, так и на период после его истечения, установленный договором.

## **VI. Требования по управлению информационными ресурсами центра сертификации**

### ***Раздел 1. Требования к информационным ресурсам***

93. Информационными ресурсами центра сертификации являются реестр сертификатов открытых ключей и служебные документы центра сертификации.

94. Информационные ресурсы центра сертификации ведутся в виде документов на бумажном носителе и в форме электронных документов, которые хранятся на материальных носителях.

95. Основным информационным ресурсом центра сертификации является реестр сертификатов открытых ключей, представляющий собой набор электронных документов и документов на бумажном носителе, включающий:

- a) заявления на сертификацию открытых ключей пользователей цифровой подписи;
- b) сертификаты открытых ключей пользователей цифровой подписи;
- c) решения о приостановлении, возобновлении действия или отзыве сертификатов открытых ключей пользователей цифровой подписи;
- d) сертификаты открытых ключей уполномоченных лиц центров сертификации третьего уровня (только для центров сертификации второго уровня);
- e) заявления на приостановление, возобновление действия или отзыв сертификатов открытых ключей уполномоченных лиц центров сертификации третьего уровня (только для центров сертификации второго уровня);
- f) списки отозванных сертификатов.

96. Документация центра сертификации должна соответствовать международному стандарту ISO 15489 "Информация и документация – управление документацией".

## ***Раздел 2. Требования к архивному хранению информационных ресурсов***

97. Архивному хранению подлежат следующие информационные ресурсы центра сертификации:

- a) реестр сертификатов открытых ключей;
- b) журналы аудита программно-аппаратного комплекса;
- c) другие виды документов, установленные центром сертификации.

98. Срок архивного хранения реестра сертификатов открытых ключей составляет не менее 10 лет с момента отзыва последнего занесенного в реестр сертификата.

99. Подготовка к уничтожению и уничтожение архивных документов осуществляется комиссией, формируемой из числа сотрудников центра сертификации, в соответствии с действующим законодательством.

100. Работы по подготовке к уничтожению и уничтожению документов, не подлежащих архивному хранению, осуществляются сотрудниками центра сертификации, обеспечивающими документирование, в порядке, установленном руководителем центра сертификации.

## ***Раздел 3. Требования по обеспечению доступа к информационным ресурсам***

101. Центр сертификации обеспечивает доступ пользователей цифровой подписи к реестру сертификатов открытых ключей посредством:

- a) официального электронного информационного ресурса центра сертификации (web-портала);
- b) электронной почты;
- c) исполнения запросов пользователей цифровой подписи в соответствии с утвержденными центром сертификации процедурами.

102. Доступ к архивным документам центра сертификации осуществляется в соответствии с действующим законодательством.

## **VII. Требования по обеспечению безопасности центра сертификации**

### ***Раздел 1. Требования к системе безопасности***

103. Основными задачами по обеспечению безопасности центра сертификации являются:

- a) защита конфиденциальной информации при ее хранении, обработке и передаче (криптографические ключи, средства криптографической защиты информации, персональные сведения, охраняемые в соответствии с действующим законодательством, парольная информация и т.п.);

b) контроль целостности конфиденциальной и открытой информации (информация о владельцах, входящая в состав сертификатов открытых ключей, информация о приостановленных и отозванных сертификатах открытых ключей, свободно распространяемые программные компоненты и документация к ним и т.п.);

c) контроль целостности программных и аппаратных компонентов программно-технического комплекса;

d) обеспечение безотказной работы;

e) обеспечение физической безопасности центра сертификации.

104. Система безопасности центра сертификации должна:

a) защищать информацию о владельцах сертификатов открытых ключей посредством обеспечения конфиденциальности, целостности и безопасного доступа к реестру сертификатов открытых ключей;

b) обеспечивать безопасность инфраструктуры и информационных ресурсов центра сертификации;

c) устанавливать ответственность за информационную безопасность в центре сертификации;

d) минимизировать риски, связанные с использованием информационных технологий;

e) обеспечить способность центра сертификации продолжать деятельность в чрезвычайных и других критических ситуациях (обеспечение непрерывности деятельности центра сертификации).

105. Комплекс мер и средств защиты информации в центре сертификации должен включать следующие подсистемы:

a) подсистема криптографической защиты информации, включающая средства криптографической защиты информации;

b) подсистема защиты информации от несанкционированного доступа;

c) подсистема активного аудита информационной безопасности центра;

d) подсистема обнаружения вторжений;

e) подсистема защиты информации от непреднамеренного воздействия, включая подсистему резервного копирования и архивирования данных;

f) подсистема обеспечения целостности информации, программных и аппаратных компонентов программно-технического комплекса центра сертификации, в том числе криптографическими методами;

g) подсистема обеспечения доступности, включая подсистему безотказной работы программно-технического комплекса центра сертификации;

h) подсистема защиты оборудования программно-технического комплекса центра сертификации от утечки информации по техническим и побочным каналам;

i) подсистема физической безопасности.

106. Центр сертификации должен разработать требования по обеспечению своей безопасности, критерии и показатели оценки уровня безопасности, в соответствии с которыми осуществлять те или иные мероприятия и внедрять конкретные средства защиты информации.

107. Любая функция центра сертификации может быть делегирована третьим лицам только с учетом требований по безопасности центра сертификации.

108. Центр сертификации должен разработать и утвердить внутренние бизнес-процессы, обеспечивающие безопасную деятельность центра сертификации.

109. Любая форс-мажорная ситуация, которая может негативно повлиять на выполнение обязательных процедур центра сертификации, должна быть доведена до сведения владельцев сертификатов открытых ключей.

110. Центр сертификации должен разработать и утвердить политику безопасности центра сертификации, которая должна отражать видение проблемы информационной безопасности центра сертификации, систему мер по ее обеспечению, ответственность сотрудников и механизмы контроля состояния информационной безопасности.

111. Политика безопасности должна обеспечивать соблюдение общепринятых правил, норм и стандартов в сфере информационной безопасности и должна содержать:

а) категории ресурсов центра сертификации с указанием необходимого уровня защиты для каждой категории;

б) анализ рисков центра сертификации, возникающих в связи с применением информационных и телекоммуникационных технологий;

с) модель безопасности центра сертификации;

д) выбор комплексной системы обеспечения безопасности центра сертификации;

е) основные организационно-технические мероприятия, необходимые для обеспечения безопасности центра сертификации;

ф) требования к техническим средствам защиты информации;

г) перечень технических средств защиты информации;

h) план действий по поддержанию режима безопасности центра сертификации, включая планы обеспечения бесперебойной работы;

и) обязанности персонала центра сертификации по обеспечению безопасности;

ж) процедуры проверки центра сертификации на соответствие требованиям безопасности;

к) процедуры ознакомления пользователей цифровой подписи с Регламентом и политикой безопасности центра сертификации и получение от них обязательств по соблюдению положений Регламента и политики безопасности;

л) ознакомление пользователей цифровой подписи с информацией об уровне защищенности центра сертификации.

112. Центр сертификации должен разработать и утвердить систему предоставления прав доступа к ресурсам центра сертификации согласно установленным процедурам доступа.

113. Центр сертификации должен анализировать все компоненты своей инфраструктуры (аппаратное и программное обеспечение, средства защиты

информации и т.д.) с точки зрения рисков, планировать и осуществлять мероприятия по минимизации и устранению выявленных рисков.

114. Центр сертификации должен внедрять автоматизированные инструменты анализа информационных и телекоммуникационных систем, бизнес-процессов центра сертификации для выявления, определения уязвимых мест в системе безопасности.

115. Центр сертификации должен разработать и утвердить план мероприятий по обеспечению непрерывности своей деятельности, который периодически корректируется на основании анализа текущей деятельности и тестирования различных возможных чрезвычайных ситуаций.

## ***Раздел 2. Требования по обеспечению физической безопасности***

116. Центр сертификации должен создать и поддерживать систему физической безопасности, обеспечивающую защиту инфраструктуры, информационных ресурсов и персонала центра, обладающую гибкостью при изменении предъявляемых к ней требований, возможностью наращивания функций, и быть простой в эксплуатации.

117. Система физической безопасности центра сертификации должна включать следующие подсистемы:

- a) управления доступом к различным физическим объектам;
- b) обнаружения несанкционированного проникновения на физические объекты;
- c) управления, анализа и регистрации информации;
- d) инженерно-технической защиты (пассивной защиты);
- e) оповещения и обеспечения связи в чрезвычайных ситуациях.

118. Центр сертификации должен установить и распределить обязанности сотрудников по обеспечению физической безопасности.

119. Информация о размещении подсистем программно-технического комплекса центра сертификации является конфиденциальной.

120. Инженерно-техническое и специальное оборудование, охрана и режим доступа в специальные помещения центра сертификации должны обеспечивать безопасность конфиденциальной информации и криптографических ключей, контролируемый доступ в эти помещения, а также доступ к техническим средствам и криптографическим ключам.

121. Центр сертификации должен категорировать специальные помещения, определить порядок доступа и утвердить перечень лиц, которым разрешен доступ в эти помещения.

122. Доступ сотрудников центра сертификации в специальные помещения осуществляется на основании действующих в центре сертификации инструкций и приказов.

123. Физический доступ в специальные помещения центра сертификации должен быть возможен только после двойного контроля и в соответствии с установленными правами доступа.

124. Сотрудники центра сертификации, имеющие доступ в специальные помещения, несут персональную ответственность за несанкционированный допуск в эти помещения посторонних лиц.

125. Специальные помещения в обязательном порядке оборудуются системами контроля доступа и видеонаблюдения, позволяющими отслеживать доступ лиц в данные помещения.

126. Специальные помещения в обязательном порядке оборудуются многорубежными системами охранной и тревожной сигнализации в соответствии с методологическими и техническими нормами проектирования и монтажа систем охранной сигнализации, утвержденными Постановлением Правительства № 667 от 8 июля 2005 г. "О мерах по реализации Закона № 283-ХV от 4 июля 2003 г. о частной детективной и охранной деятельности".

127. При размещении технических средств центр сертификации должен обеспечить их защиту от несанкционированного доступа, кражи, пожаров, наводнений, сильных электромагнитных полей и других возможных рисков.

128. Помещения, предназначенные для размещения персонала центра сертификации, а также иные служебные помещения должны оборудоваться:

- а) системами охранной, тревожной и пожарной сигнализации;
- б) системой контроля доступа, позволяющей отслеживать доступ персонала центра сертификации в определенные помещения.

129. При расположении служебных и иных помещений центра сертификации на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п. окна помещений оборудуются внутренними решетками.

### ***Раздел 3. Требования по обеспечению безопасности информационных и телекоммуникационных систем***

130. Для минимизации рисков, связанных с применением информационных и телекоммуникационных технологий, центр сертификации разрабатывает и внедряет комплекс мер по обеспечению безопасности своих информационных и телекоммуникационных систем (программных и технических средств, каналов связи, сетевого оборудования, обрабатываемой, хранимой и передаваемой информации) функционированием следующих подсистем безопасности:

- а) подсистема управления доступом;
- б) подсистема регистрации и учета (аудита);
- с) подсистема обеспечения целостности;
- д) подсистема обеспечения доступности;
- е) подсистема криптографической защиты.

131. Подсистема управления доступом:

- а) разделяет доступ к информационным объектам и функциям информационных систем в соответствии с правилами доступа, основанными на атрибутах доступа;

b) осуществляет проверку подлинности субъектов, получающих доступ к компонентам информационных систем;

c) осуществляет контроль доступа субъектов к защищаемым ресурсам в соответствии с установленными уровнями доступа;

d) управляет информационными потоками с применением меток конфиденциальности;

e) фиксирует случаи успешного и безуспешного доступа.

132. Подсистема регистрации и учета:

a) регистрирует попытки входа (выхода) субъекта доступа в систему по следующим параметрам:

дата и время попытки входа (выхода);

идентификатор субъекта доступа;

результат попытки входа (выхода) – успешная или безуспешная;

b) регистрирует попытки запуска (завершения работы) приложений и процессов, предназначенных для обработки защищаемых ресурсов по следующим параметрам:

дата и время попытки запуска;

наименование (идентификатор) приложения или процесса;

идентификатор субъекта доступа;

результат попытки запуска – успешная или безуспешная;

c) регистрирует попытки получения доступа (выполнения операций) приложений и процессов к защищаемым ресурсам по следующим параметрам:

дата и время попытки получения доступа (выполнения операции);

наименование (идентификатор) приложения или процесса;

идентификатор субъекта доступа;

спецификация защищаемого ресурса (идентификатор, логическое имя, имя файла, номер и т.п.);

вид запрашиваемой операции (чтение, запись, удаление, монтирование и т.п.);

результат попытки получения доступа (выполнения операции) – успешная или безуспешная;

d) регистрирует попытки несанкционированного входа субъектов доступа в систему, попытки несанкционированного запуска приложений (процессов) или выполнения операций, а также блокирует все несанкционированные операции и оповещает об этом администратора безопасности;

e) регистрирует изменения полномочий субъектов доступа и статуса объектов доступа по следующим параметрам:

дата и время изменения полномочий;

идентификатор администратора, осуществившего изменения;

идентификатор субъекта доступа и его новые полномочия или спецификация объекта доступа и его новый статус;

f) регистрирует выдачу из системы информации (электронного документа, данных и т.д.) по следующим параметрам:

дата и время выдачи;

наименование информации и путь к ней;  
 спецификация устройства выдачи (логическое имя);  
 идентификатор субъекта доступа, запросившего информацию;  
 объем выданного документа (количество страниц, листов, копий) и  
 результат выдачи (успешный, безуспешный);

g) ведет учет защищаемых ресурсов центра сертификации, проводит регистрацию выдачи/приема материальных носителей с конфиденциальной информацией;

h) защищает "протокольные" данные (регистрационный журнал, log-файл и т.п.) от изменения;

i) идентифицирует и показывает текущие события.

133. Подсистема обеспечения целостности обеспечивает неизменность программной среды, целостность обрабатываемой информации, программно-технических средств и средств защиты информации.

134. Подсистема обеспечения доступности:

a) обеспечивает отказоустойчивую работу информационных и телекоммуникационных систем центра сертификации;

b) обеспечивает гарантированное сохранение информационных ресурсов центра сертификации, а также возможность их восстановления в случае необходимости или в форс-мажорных обстоятельствах;

c) обеспечивает постоянный доступ пользователей системы к информационным ресурсам центра сертификации в соответствии с установленными правилами доступа к информации.

135. Подсистема криптографической защиты:

a) осуществляет шифрование всей конфиденциальной информации в информационной системе и в каналах связи;

b) обеспечивает контроль доступа субъектов к операциям шифрования и криптографическим ключам в соответствии с установленными правилами доступа.

136. Архитектура информационных и телекоммуникационных систем центра сертификации и их подсистем безопасности должна быть достаточно гибкой, допускать простое, без структурных изменений, развитие конфигурации используемых средств, наращивание функций и ресурсов.

137. Информационные и телекоммуникационные системы центра сертификации должны сопровождаться документацией, обеспечивающей квалифицированную их эксплуатацию.

138. Отдельные критические компоненты информационных и телекоммуникационных систем центра сертификации должны иметь системы резервирования и восстановления после нарушения режима безопасности или отказов (сбоев).

139. Информационные и телекоммуникационные системы, их компоненты, программные и технические средства центра сертификации должны соответствовать установленным нормам политики информационной безопасности, а со стороны их разработчиков (производителей, поставщиков и т.д.) должна осуществляться необходимая техническая поддержка.

140. Центр сертификации должен обеспечить защиту своих информационных и телекоммуникационных систем от воздействия вредоносного программного обеспечения (систему антивирусной защиты).

141. Центр сертификации должен категорировать ресурсы информационных систем, определить порядок доступа и утвердить перечень лиц, которым разрешен доступ к отдельным ресурсам информационных и телекоммуникационных систем.

142. Центр сертификации должен разработать, утвердить и внедрить необходимые механизмы и процедуры разграничения и контроля логического и физического доступа к оборудованию информационных систем и телекоммуникационным ресурсам.

143. Доступ сотрудников центра сертификации к ресурсам информационных и телекоммуникационных систем должен осуществляться на основании действующих в центре сертификации инструкций и приказов в соответствии с утвержденными правами доступа.

144. Центр сертификации должен установить и документировать процедуры администрирования и использования системного и прикладного программного обеспечения.

145. Внедрение новых или усовершенствованных информационных и телекоммуникационных систем, их компонентов, программных и технических средств должно производиться только в установленном порядке, с соблюдением требований по обеспечению информационной безопасности.

146. Центр сертификации должен разработать и утвердить соответствующие инструкции по применению новых или модификации существующих информационных и телекоммуникационных систем, их компонентов, программных и технических средств.

147. Ответственный персонал центра сертификации должен быть инструктирован о функциональности и правилах администрирования (эксплуатации) новых или усовершенствованных информационных телекоммуникационных систем, их компонентов, программных и технических средств.

148. Все возможные изменения в конфигурации информационных и телекоммуникационных систем, их компонентов, программных и технических средств должны быть протестированы до их внедрения в операционную среду. Решение о модификации принимается только после оценки рисков, связанных с внедрением данных изменений.

149. Центр сертификации должен разработать и утвердить формальные процедуры контроля модификаций информационных и телекоммуникационных систем, их компонентов, программных и технических средств.

150. Центр сертификации должен использовать безопасные, контролируемые сетевые подключения и механизмы, обеспечивающие целостность и конфиденциальность информации при ее передаче через публичные сети.

151. Центр сертификации должен внедрять системы межсетевое экранирования, обеспечивающие защиту внутренних информационных и телекоммуникационных систем и ресурсов центра сертификации.

152. Ответственный персонал центра сертификации (системные администраторы) обязаны осуществлять ежедневный контроль состояния информационных и телекоммуникационных систем, их компонентов, операционных и прикладных систем, а также инструментов безопасности.

#### ***Раздел 4. Требования по использованию средств криптографической защиты информации***

153. Центр сертификации обеспечивает безопасность конфиденциальной информации при ее хранении, обработке и передаче по каналам связи, применяя технологии шифрования информации с использованием средств криптографической защиты информации (СКЗИ).

154. Для разработки и осуществления мероприятий по обеспечению безопасности информации и использованию СКЗИ в центре сертификации должно быть создано подразделение криптографической защиты информации (выделен сотрудник), разработаны и утверждены инструкции, регламентирующие процессы подготовки, ввода, обработки, хранения и передачи конфиденциальной информации, защищаемой с использованием СКЗИ.

155. Подразделение криптографической защиты:

а) разрабатывает и внедряет систему криптографической защиты конфиденциальной информации центра сертификации;

б) разрабатывает инструкции и мероприятия по обеспечению функционирования и безопасности применяемых СКЗИ;

с) обеспечивает хранение и учет материальных носителей конфиденциальной информации, СКЗИ и документации к ним, материальных носителей ключевой информации, а также учет пользователей, непосредственно эксплуатирующих СКЗИ;

д) обучает пользователей СКЗИ правилам работы с СКЗИ;

е) осуществляет контроль соблюдения пользователями установленных норм использования СКЗИ, эксплуатационной и технической документации к ним;

ф) осуществляет контроль целостности системного и прикладного программного обеспечения технических средств, на которых установлены СКЗИ, а также контроль целостности СКЗИ;

г) выявляет факты нарушения установленных норм использования СКЗИ и принимает необходимые меры по предотвращению возможных последствий подобных нарушений.

156. Сотрудники подразделения криптографической защиты обязаны:

а) соблюдать режим конфиденциальности в процессе выполнения своих служебных обязанностей;

b) своевременно выявлять попытки посторонних лиц получить сведения о конфиденциальной информации, об используемых СКЗИ и ключевых носителях;

c) незамедлительно принимать меры по предупреждению разглашения конфиденциальной информации, возможной утечки такой информации при использовании СКЗИ.

157. Сотрудники подразделения криптографической защиты должны иметь соответствующий уровень квалификации и осуществлять свою деятельность согласно должностным обязанностям.

158. Центр сертификации осуществляет внедрение и эксплуатацию СКЗИ в соответствии с эксплуатационной и технической документацией к этим средствам, утвержденными инструкциями, а также настоящими специальными условиями.

159. Инструкции, регламентирующие безопасную эксплуатацию СКЗИ, должны предусматривать:

a) права и обязанности сотрудников центра сертификации, эксплуатирующих СКЗИ;

b) порядок размещения, установки, хранения и использования СКЗИ и эксплуатационной документации к ним;

c) порядок создания, учета, распространения, хранения и уничтожения криптографических ключей;

d) порядок расследования фактов нарушения установленных правил использования СКЗИ, криптографических ключей, а также меры по устранению последствий выявленных нарушений;

e) порядок осуществления контроля выполнения требований по обеспечению защиты информации с применением СКЗИ.

160. Условия внедрения и эксплуатации СКЗИ должны исключать возможность несанкционированного доступа к ним, внесения изменений, хищения и бесконтрольного распространения.

161. Эксплуатирующиеся центром сертификации СКЗИ должны периодически подвергаться контрольным проверкам на протяжении всего цикла функционирования.

162. СКЗИ подлежат учету. Программные СКЗИ учитываются совместно с аппаратными средствами, с которыми осуществляется их функционирование.

163. При необходимости, для обеспечения целостности криптографических ключей могут создаваться резервные копии, которые хранятся в соответствии с установленными нормами по обеспечению их защиты от несанкционированного доступа и непреднамеренного воздействия.

164. Сотрудники центра сертификации несут персональную ответственность за сохранность и безопасность криптографических ключей.

165. Материальные носители с криптографическими ключами учитываются подразделением криптографической защиты.

166. Неиспользованные или выведенные из обращения материальные носители с криптографическими ключами уничтожаются подразделением криптографической защиты.

167. Уничтожение криптографических ключей производится путем физического уничтожения материального носителя или гарантированного уничтожения ключевой информации без повреждения носителя (для его повторного использования).

168. Криптографические ключи СКЗИ должны периодически меняться. Процедура смены ключей устанавливается центром сертификации.

169. Криптографические ключи или СКЗИ, в отношении которых имеются основания полагать, что они скомпрометированы, немедленно выводятся из обращения, а подразделение криптографической защиты осуществляет комплекс необходимых мер для проверки факта и устранения последствий.

### ***Раздел 5. Требования по технической защите информации***

170. Центр сертификации обеспечивает защиту конфиденциальной информации, применяя технологии и специальные средства защиты информации от утечки по техническим каналам.

171. Центр сертификации должен исключить неконтролируемое пребывание посторонних лиц или автотранспортных средств, а также размещение случайных антенн в зоне радиусом не менее 15 метров от места размещения основных технических средств программно-технического комплекса (далее – контролируемая зона).

172. Серверные помещения центра сертификации должны быть защищены от утечки информации за счет побочных электромагнитных излучений и наводок путем экранирования помещений или установки систем электромагнитного зашумления.

173. В случае экранирования помещений должна обеспечиваться непрерывность электрического соединения материала всех частей экрана: стен, потолка, пола, оконных и дверных проемов. Дверное полотно должно иметь надежный электрический контакт с экраном помещения по всей поверхности, экранирующие конструкции должны быть заземлены через контур заземления, расположенный в контролируемой зоне.

174. Центр сертификации должен обеспечить защиту информации от утечки по цепям электропитания [развязка цепей электропитания объекта с применением защитных фильтров, блокирующих (подавляющих) сигнал].

175. В помещениях центра сертификации, в которых размещены технические средства, обрабатывающие конфиденциальную информацию, размещение посторонней электро-, радио- и другой аппаратуры должно быть исключено или ограничено.

176. Оборудование на линиях, которых имеют выход за пределы контролируемой зоны, должно устанавливаться на расстоянии не менее 3 метров от основных технических средств программно-технического комплекса центра сертификации.

177. Достаточность применяемых технических мер защиты, а также необходимость установки дополнительных специальных технических средств

определяются по результатам специальных исследований и оценки защищенности объекта.

### ***Раздел 6. Требования по обеспечению безопасности информационных ресурсов***

178. Информационные ресурсы центра сертификации должны быть классифицированы и категорированы в соответствии с уровнем их безопасности.

179. Вся информация, данные и документы должны обрабатываться и храниться согласно уровню классификации и категории данной информации.

180. Вся информация, данные и документы, классифицированные как конфиденциальные, должны храниться в отдельной безопасной среде.

181. Центр сертификации должен осуществлять меры по защите персональных данных в соответствии с законодательством Республики Молдова.

182. Реестр сертификатов открытых ключей должен храниться и обрабатываться в условиях, обеспечивающих его целостность, доступность и конфиденциальность.

183. Центр сертификации должен создавать резервные копии реестра сертификатов открытых ключей, другой критически важной информации.

184. Хранение резервных копий должно осуществляться в специальных помещениях центра сертификации.

185. Документы центра сертификации должны быть защищены от утери, уничтожения и фальсификации.

186. Центр сертификации должен установить сроки использования и хранения документов и информации, разработать номенклатуру дел, в которую вносятся основные типы документов и установленные для них сроки хранения.

187. Сотрудникам центра сертификации запрещается использование информационных ресурсов центра в личных целях.

188. Персонал центра сертификации обязан знать риски, связанные с нарушением безопасности информации, с которой они работают.

### ***Раздел 7. Требования по управлению информационной безопасностью центра сертификации***

189. Центр сертификации должен создать систему управления информационной безопасностью, проводить постоянный мониторинг системы информационной безопасности, выявлять угрозы информационной безопасности и управлять рисками.

190. Для управления информационной безопасностью рекомендуется руководствоваться международным стандартом ISO/IEC 17799-2005 "Информационные технологии. Свод правил по управлению безопасностью информации".

## **VIII. Проверка деятельности центра сертификации**

191. Центр сертификации обязан проводить, один раз в два года, комплексную проверку своей деятельности.

192. Комплексная проверка деятельности центра сертификации осуществляется уполномоченным органом по разработке и реализации государственной политики и контролю в сфере применения цифровой подписи – Службой информации и безопасности Республики Молдова (далее – уполномоченный орган), с привлечением, в случае необходимости, специалистов в данной сфере.

193. По инициативе центра сертификации комплексная проверка его деятельности может осуществляться организациями, специализирующимися в аудиторской и консультационной деятельности в сфере информационных технологий, с привлечением представителя уполномоченного органа, за счет центра сертификации.

194. Рекомендуются, чтобы организация, осуществляющая комплексную проверку деятельности центра сертификации, соответствовала следующим требованиям:

а) обладать персоналом, квалификация которых подтверждена сертификатами аудиторов в сфере информационных систем (международные сертификаты CISA или CISM);

б) иметь опыт аудита в сфере информационных технологий не менее 2 лет.

195. Организация, осуществляющая комплексную проверку деятельности центра сертификации, должна:

а) обеспечить независимость осуществляемой проверки;

б) осуществлять проверку в соответствии с нормами и стандартами аудита в сфере информационных технологий и безопасности информационных систем;

в) использовать методологию проверки, основанную на оценке рисков и соответствующих процедурах оценки адекватности мероприятий по управлению рисками;

г) обеспечить конфиденциальность полученной в результате проверки информации.

196. Организация, осуществляющая комплексную проверку деятельности центра сертификации, составляет акт проверки и заключение.

197. Акт проверки подписывается ответственным лицом, осуществившим проверку деятельности центра сертификации, представителем уполномоченного органа и руководителем юридического лица, в составе которого осуществляет свою деятельность центр сертификации.

198. Заключение составляется на основании акта проверки и является документом, подтверждающим (не подтверждающим) соответствие деятельности центра сертификации установленным нормам в сфере цифровой подписи.

199. Заключение должно содержать:

- a) оценку качества и непрерывности услуг в сфере цифровой подписи, предоставляемых центром сертификации;
- b) соответствие деятельности центра сертификации стандартам, техническим нормам и другим нормативным документам в сфере цифровой подписи;
- c) соответствие деятельности центра сертификации положениям Регламента центра сертификации, политике сертификации и политике безопасности;
- d) соответствие деятельности центра сертификации установленным функциям и обязанностям;
- e) соответствие основных процедур центра сертификации предъявляемым требованиям;
- f) соответствие деятельности центра сертификации требованиям по обеспечению безопасности центра сертификации;
- g) выводы о достаточности мер по обеспечению конфиденциальности, целостности и доступности информации и информационных услуг;
- h) оценку качества и комплексности внутренних процедур центра сертификации;
- i) анализ функции управления рисками центра сертификации;
- j) соблюдение процедур обеспечения непрерывности деятельности центра сертификации;
- k) соответствие программно-технического комплекса центра сертификации предъявляемым требованиям;
- l) проверку принятых мер по результатам предыдущего аудита.

200. Результаты комплексной проверки деятельности центра сертификации (копия акта и заключения), проведенной организацией, специализирующейся в аудиторской и консультационной деятельности в сфере информационных технологий, предоставляются уполномоченному органу.

201. Центр сертификации периодически должен проводить внутренний аудит своей деятельности в соответствии с Регламентом проведения внутреннего аудита, утвержденного данным центром.

## **IX. Создание, реорганизация и ликвидация центра сертификации**

### ***Раздел 1. Требования по созданию центра сертификации***

202. Для предоставления услуг по сертификации открытых ключей центр сертификации должен пройти процедуру регистрации в соответствии с установленными нормами и сертифицировать открытый ключ уполномоченного лица центра сертификации в вышестоящем центре сертификации.

203. Для регистрации центра сертификации юридическое лицо, создающее центр сертификации, обязано обеспечить выполнение следующих условий:

а) создать (назначить) подразделение для осуществления функций центра сертификации;

б) создать штат сотрудников, обладающих квалификацией, необходимой для предоставления услуг по сертификации открытых ключей и других услуг в сфере цифровой подписи;

с) обустроить специальные помещения, а также другие рабочие помещения центра сертификации в соответствии с требованиями к помещениям центра сертификации, установленными настоящими специальными условиями;

д) создать программно-технический комплекс центра сертификации, соответствующий техническим нормам в сфере цифровой подписи и требованиям настоящих специальных условий;

е) назначить уполномоченное лицо центра сертификации (администратора сертификации), администратора регистрации, администратора безопасности и системного администратора;

ф) создать систему безопасности центра сертификации в соответствии с настоящими специальными условиями;

г) создать подразделение (назначить сотрудника), ответственное за криптографическую защиту информации в центре сертификации;

h) разработать и утвердить нормативную базу центра сертификации, необходимую для предоставления услуг по сертификации открытых ключей, включающую следующие обязательные документы:

политика сертификации центра сертификации;

Регламент центра сертификации;

политика безопасности центра сертификации;

политика предоставления и контроля доступа к ресурсам центра сертификации;

план управления рисками;

план обеспечения непрерывности деятельности центра сертификации;

процедуры восстановления работы центра сертификации;

инструкции, регламентирующие безопасность и эксплуатацию СКЗИ;

регламент проведения внутреннего аудита центра сертификации;

і) получить банковскую гарантию в банке, зарегистрированном на территории Республики Молдова, или страховой полис в страховой компании, зарегистрированной на территории Республики Молдова, в пользу уполномоченного органа на сумму в молдавских леях, эквивалентную 20.000 евро.

204. При регистрации, центр сертификации должен пройти процедуру комплексной проверки в соответствии с установленными настоящими специальными условиями требованиями по проверке деятельности центра сертификации.

## ***Раздел 2. Требования по реорганизации центра сертификации***

205. Реорганизация центра сертификации осуществляется в установленных законодательством формах путем его передачи его функций другому юридическому лицу.

206. Передача центра сертификации осуществляется:

- a) на основании договора о передаче центра сертификации;
- b) на основании решения о реорганизации юридического лица.

207. Юридическое лицо в срок не менее чем за 30 дней до момента передачи должно уведомить уполномоченный орган и вышестоящий центр сертификации о решении о передаче центра сертификации.

208. Юридическое лицо в срок не менее чем за 30 дней до момента передачи должно уведомить все нижестоящие центры сертификации и пользователей цифровой подписи о решении о передаче центра сертификации и о необходимости перезаключения контрактов на обслуживание с новым центром сертификации.

209. Решением заинтересованных юридических лиц создается комиссия по передаче центра сертификации.

210. В состав комиссии по передаче центра сертификации должны входить:

- a) представители юридических лиц;
- b) представитель уполномоченного органа;
- c) другие лица, назначенные сторонами.

211. В ходе процедуры передачи центр сертификации должен:

a) уничтожить закрытые ключи уполномоченных лиц центра сертификации без нарушения их конфиденциальности в соответствии с требованиями, установленными уполномоченным органом;

b) передать реестр сертификатов открытых ключей.

212. Реестр сертификатов открытых ключей в форме электронных документов передается на материальных носителях, а реестр сертификатов открытых ключей на бумажных носителях передается в виде архива документов на бумажных носителях.

213. Сертификаты открытых ключей, выданные центром сертификации, продолжают действовать до истечения срока их действия.

214. По окончании работы комиссии составляется акт приема-передачи, в соответствии с которым юридическое лицо, которому был передан центр сертификации, становится правопреемником центра. Акт подписывается членами комиссии и утверждается руководителями заинтересованных юридических лиц.

### ***Раздел 3. Требования по ликвидации центра сертификации***

215. Центр сертификации может быть ликвидирован:

- a) по инициативе юридического лица, создавшего центр сертификации;
- b) по инициативе уполномоченного органа при нарушении установленных норм в сфере цифровой подписи;
- c) при ликвидации юридического лица, создавшего центр сертификации.

216. Юридическое лицо в срок не менее чем за 30 дней до момента ликвидации должно уведомить уполномоченный орган и вышестоящий центр сертификации о решении о ликвидации центра сертификации.

217. Пользователи цифровой подписи в срок не менее чем за 30 дней до момента ликвидации должны быть оповещены о ликвидации центра сертификации.

218. Процедура ликвидации центра сертификации по инициативе юридического лица, создавшего центр сертификации, инициируется приказом руководителя юридического лица.

219. Приказом руководителя юридического лица, ликвидирующего центр сертификации, создается ликвидационная комиссия, в задачи которой входит проведение процедуры ликвидации.

220. Ликвидация центра сертификации по инициативе уполномоченного органа осуществляется в судебном порядке на основании заключения уполномоченного органа о нарушении законодательства в сфере цифровой подписи. После вынесения судебного решения приказом руководителя уполномоченного органа создается ликвидационная комиссия.

221. В состав ликвидационной комиссии должны входить:

- a) руководитель юридического лица, создавшего центр сертификации;
- b) представитель уполномоченного органа;
- c) другие лица, назначенные приказом.

222. В ходе процедуры ликвидации центр сертификации должен:

- a) уничтожить закрытые ключи уполномоченных лиц центра сертификации без нарушения их конфиденциальности в соответствии с требованиями, установленными уполномоченным органом;
- b) отозвать сертификаты открытых ключей пользователей цифровой подписи, выданные ликвидированным центром сертификации;
- c) опубликовать статус сертификатов открытых ключей;
- d) передать на хранение уполномоченному органу реестр сертификатов открытых ключей.

223. Реестр сертификатов открытых ключей в форме электронных документов передается на материальных носителях, а реестр сертификатов открытых ключей на бумажных носителях передается в виде архива документов на бумажных носителях, о чем составляется акт приема-передачи, который подписывается руководителем юридического лица, создавшего центр сертификации, и представителем уполномоченного органа, ответственным за хранение. Реестр сертификатов открытых ключей подлежит архивному хранению в соответствии с действующим законодательством.

224. Ликвидационной комиссией составляется акт, в соответствии с которым центр сертификации прекращает свое существование.