ПРИЛОЖЕНИЕ № 6

к Требованиям к созданию, развитию
и функционированию трансграничного
пространства доверия

Т Р Е Б О В А Н И Я
к мерам и способам обеспечения защиты информации

I. Общие положения

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

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

3. Защита элементов и сервисов государственных компонентов общей инфраструктуры документирования информации в электронном виде осуществляется в соответствии с законодательством государств – членов Евразийского экономического союза или международными стандартами с учетом настоящих Требований.

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

а) требования к обеспечению физической защиты;

б) требования к обеспечению защиты от вредоносного программного обеспечения;

в) требования к обеспечению резервного копирования;

г) требования к учету событий и инцидентов информационной безопасности;

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

е) требования к работе со средствами криптографической защиты;

ж) требования к управлению доступом.

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

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

II. Требования к обеспечению физической защиты

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

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

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

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

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

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

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

а) порядок обустройства контролируемых зон ограниченного доступа;

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

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

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

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

е) описание политики управления доступом, которая устанавливает набор допустимых операций пользователей различных

ролей с сервисами и сервисов, выступающих от имени пользователей, с элементами и сервисами объекта защиты.

III. Требования к обеспечению защиты от вредоносного программного обеспечения

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

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

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

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

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

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

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

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

в) порядок действий персонала при выявлении вредоносного программного обеспечения;

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

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

IV. Требования к обеспечению резервного копирования

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

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

22. Должно проводиться регулярное тестирование работоспособности средств резервного копирования.

23. Документация о проведении резервного копирования данных должна содержать:

а) требования к составу средств копирования и восстановления данных;

б) регламент проведения работ по резервному копированию информации;

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

г) порядок регистрации событий резервного копирования и восстановления данных;

д) порядок тестирования работоспособности средств резервного копирования.

V. Требования к учету событий и инцидентов информационной безопасности

24. Должен вестись учет событий и инцидентов информационной безопасности.

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

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

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

а) порядок учета событий и инцидентов информационной безопасности;

б) политику обработки событий и инцидентов;

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

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

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

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

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

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

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

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

в) описание защитных мер.

VII. Требования к работе со средствами криптографической защиты информации

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

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

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

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

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

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

37. Должны использоваться только сертифицированные средства криптографической защиты информации.

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

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

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

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

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

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

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

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

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

г) перечень сертифицированных средств криптографической защиты информации;

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

е) порядок учета хранящихся средств криптографической защиты информации;

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

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

VIII. Требования к управлению доступом

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

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