Экз. № ____

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 51624
(проект, окончательная редакция)

Защита информации

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Общие требования

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Стандартинформ
20XX

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России») и Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»)

2 ВНЕСЕН Техническим комитетом по стандартизации «Защита информации» (ТК 362)

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от « » 20 г. №

4 ВЗАМЕН ГОСТ Р 51624-2000

Правила применения настоящего стандарта установлены в статье 26 Федерального закона «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте федерального органа исполнительной власти в сфере стандартизации в сети Интернет (gost.ru).

Содержание

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Общие требования

Protection of information. Protected automated systems.
General requirements

Дата введения _____

1 Область применения

Настоящий стандарт устанавливает общие требования к защите информации в автоматизированных системах от утечки по техническим каналам, несанкционированного доступа, преднамеренных и непреднамеренных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней.

Положения настоящего стандарта распространяются на создаваемые (модернизируемые) автоматизированные системы, в отношении которых законодательством Российской Федерации или заказчиком установлены требования к защите информации.

Положения настоящего стандарта дополняют положения комплекса стандартов «Информационная технология. Комплекс стандартов на автоматизированные системы» в части общих требований к защите информации от утечки по техническим каналам, несанкционированного доступа, непреднамеренных и преднамеренных воздействий на информацию.

Примечание – Настоящий стандарт может применяться к автоматизированным системам, относящимся к ключевым системам информационной инфраструктуры, в части, не противоречащей нормативным документам и стандартам на данные виды систем.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем

ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы

ГОСТ 16325-88 Машины вычислительные электронные цифровые общего назначения. Общие технические требования

ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения

ГОСТ 20397-82 Средства технические малых электронных вычислительных машин. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение, гарантия изготовителя

ГОСТ 21552-84 Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение

ГОСТ 23773-88 Машины вычислительные электронные цифровые общего назначения. Методы испытаний

ГОСТ 27201-87 Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования

ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

ГОСТ 28195-89 Оценка качества программных средств. Общие положения

ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры

ГОСТ Р 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний

ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации

ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения

ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов

ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования

ГОСТ Р 56938-2016 Защита информации. Защита информации при использовании технологий виртуализации. Общие положения

ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования

ГОСТ Р ИСО/МЭК 9126-93 Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению

ГОСТ Р ИСО/МЭК 12119-2000 Информационная технология. Пакеты программ. Требования к качеству и тестирование

П р и м е ч а н и е – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования – на официальном сайте Федерального органа исполнительной власти в сфере стандартизации в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячно издаваемого информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный документ, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого документа с учетом всех внесенных в данную версию изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то рекомендуется использовать версию этого документа с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ 34.003, ГОСТ 16504, ГОСТ Р 50922, ГОСТ Р 53114, а также следующие термины с соответствующими определениями:

3.1 **автоматизированная система:** Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

[ГОСТ 34.003-90, статья 1.1]

Примечание – Термин «автоматизированная система», установленный ГОСТ 34.003, следует считать эквивалентным термину «информационная система», установленному в соответствии с [1].

3.2 **автоматизированная система в защищенном исполнении:** Автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации.

[ГОСТ Р 51624-2000, статья 3.1.7]

3.3 **система защиты информации автоматизированной системы:** Совокупность организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации.

[ГОСТ Р 51583-2014, статья 3.3]

4 Обозначения и сокращения

В настоящем стандарте приняты следующие сокращения:

АСЗИ – автоматизированная система в защищенном исполнении;

КЗ – контролируемая зона;

НСД – несанкционированный доступ;

ПО – программное обеспечение;

ПЭМИН – побочные электромагнитные излучения и наводки;

СВТ – средство вычислительной техники;

ТЗ – техническое задание.

5 Общие положения

5.1 При создании (модернизации), эксплуатации и выводе из эксплуатации АСЗИ должны выполняться требования законодательства Российской Федерации в области защиты информации.

5.2 Требования к защите информации в АСЗИ реализуются системой защиты информации, которая является неотъемлемой частью АСЗИ.

5.3 Требования к защите информации, предъявляемые к АСЗИ, задаются в рамках ТЗ на создание (развитие или модернизацию) автоматизированной системы или в рамках ТЗ (частного ТЗ) на создание (развитие или модернизацию) системы защиты информации автоматизированной системы, разрабатываемого с учетом ГОСТ 34.602 и ГОСТ Р 51583.

5.4 Создание АСЗИ осуществляется с учетом ГОСТ Р 51583.

5.5 Защита информации в АСЗИ должна быть:

- целенаправленной, осуществляемой в интересах реализации конкретных целей защиты информации в АСЗИ;

- комплексной, осуществляемой в интересах защиты всего многообразия структурных элементов АСЗИ от всех актуальных для АСЗИ угроз безопасности информации;

- управляемой и осуществляемой на всех стадиях жизненного цикла АСЗИ, в зависимости от степени секретности обрабатываемой информации, состояния ресурсов АСЗИ, условий эксплуатации АСЗИ, результатов отслеживания угроз безопасности информации;

- адекватной; меры и средства защиты информации должны обеспечивать безопасность информации, независимо от форм ее представления.

6 Общие требования

6.1 Требования к защите информации в автоматизированной системе в защищенном исполнении

Требования к защите информации в АСЗИ включают:

- цели и задачи защиты информации в АСЗИ;
- требования к организации защиты информации в АСЗИ;
- требования к мерам защиты информации в АСЗИ;
- требования к основным видам обеспечения АСЗИ.

6.2 Цели и задачи защиты информации в автоматизированной системе в защищенном исполнении

6.2.1 Общей целью защиты информации в АСЗИ является предотвращение или снижение величины ущерба, наносимого обладателю и/или пользователю этой системы или обладателю информации, вследствие реализации угроз безопасности информации.

Система защиты информации в АСЗИ не должна препятствовать достижению целей создания АСЗИ и ее функционированию по прямому назначению.

Частными целями защиты информации, обеспечивающими достижение общей цели АСЗИ, могут являться:

- предотвращение неправомерного доступа, уничтожения, искажения, копирования, блокирования информации, иных неправомерных действий в ее отношении;

- соблюдение информационной технологии выполнения установленных функций;

- соблюдение правового режима использования информационных массивов и программ обработки информации;

- сохранение возможности управления процессом обработки и использования информации в условиях воздействия всех актуальных для АСЗИ угроз безопасности информации.

Цели защиты информации в АСЗИ должны включать:

- содержательную формулировку цели защиты;

- показатель эффективности достижения цели и требуемое его значение.

6.2.2 Задачи защиты информации в АСЗИ включают:

- защиту технических средств АСЗИ;

- защиту информации, содержащейся в АСЗИ, от НСД;

- защиту каналов передачи информации;

- защиту информации при информационном взаимодействии с иными автоматизированными системами и информационно-телекоммуникационными сетями.

Формулировка каждой задачи защиты информации в АСЗИ должна включать:

- цель защиты информации в АСЗИ, которая достигается при решении данной задачи защиты информации;

- угрозы безопасности информации для АСЗИ, которые необходимо предотвратить (устранить) при решении задачи;

- способ решения задачи;

- перечень мер защиты информации, которые должны быть реализованы для решения задачи.

6.3 Требования к организации защиты информации в автоматизированной системе в защищенном исполнении

6.3.1 Защита информации в АСЗИ непрерывно обеспечивается на всех стадиях (этапах) жизненного цикла АСЗИ с учетом ГОСТ Р 51583 путем реализации следующих мероприятий:

- формирование требований к защите информации в АСЗИ;

- разработка, модернизация, внедрение, оценка соответствия, ввод в действие системы защиты информации в АСЗИ;

- обеспечение защиты информации в ходе эксплуатации и выводе из эксплуатации АСЗИ;

- контроль эффективности защиты информации в ходе эксплуатации АСЗИ.

6.3.2 При формировании требований к АСЗИ определяется перечень объектов защиты в АСЗИ.

В АСЗИ объектами защиты могут являться: защищаемая информация, содержащаяся в АСЗИ (буквенно-цифровая, графическая, видео- и речевая информация), технические средства (в том числе СВТ, машинные носители информации, средства и системы передачи информации, технические средства обработки информации), общее и специальное (прикладное) ПО, информационные технологии, а также средства защиты информации.

Определение конкретного перечня объектов защиты в АСЗИ должно осуществляться исходя из назначения АСЗИ, целей защиты информации, состава и структуры АСЗИ.

6.3.3 В случаях, предусмотренных законодательством Российской Федерации, при формировании требований к АСЗИ определяются угрозы безопасности информации, актуальные для АСЗИ с учетом структурно-функциональных характеристик АСЗИ, и разрабатывается модель угроз безопасности информации, обрабатываемой в АСЗИ (при необходимости).

Угрозы безопасности информации определяются по результатам оценки возможностей (типа, вида, потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей АСЗИ, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики АСЗИ, включающие структуру и состав системы, физические, логические, функциональные и технологические взаимосвязи между сегментами АСЗИ, с иными автоматизированными системами и информационно-телекоммуникационными сетями, режимы обработки информации в АСЗИ и в ее сегментах, а также иные характеристики АСЗИ, применяемые информационные технологии и особенности ее функционирования.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик АСЗИ, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание АСЗИ и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей АСЗИ, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Определение угроз безопасности информации и разработка модели угроз безопасности информации проводятся в установленном законодательством Российской Федерации порядке.

6.3.4 При формировании требований к АСЗИ проводится классификация АСЗИ по требованиям защиты информации.

Классификация АСЗИ по требованиям защиты информации проводится заказчиком в соответствии с законодательством Российской Федерации.

Результаты классификации АСЗИ по требованиям защиты информации оформляются актом классификации.

6.3.5 При вводе в действие АСЗИ назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации в АСЗИ.

6.3.6 При модернизации и эксплуатации (выводе из эксплуатации) АСЗИ пользователям предоставляется право работать только с теми техническими средствами, ПО, информационными ресурсами и документацией, которые необходимы им для выполнения установленных функциональных обязанностей.

Эксплуатирующему персоналу, в том числе сотрудникам сторонних организаций (поставщиков технических средств, ПО и услуг гарантийного, послегарантийного обслуживания), предоставляется право работы только с необходимыми техническими средствами и ПО.

6.3.7 При создании (модернизации) и эксплуатации АСЗИ осуществляется выявление (поиск), анализ и устранение уязвимостей АСЗИ.

При эксплуатации АСЗИ осуществляется обновление ПО в АСЗИ, а также выявление инцидентов безопасности информации в АСЗИ и реагирование на них.

Работы по анализу уязвимостей в АСЗИ, обновлению ПО, а также выявлению инцидентов безопасности информации и реагированию на них проводятся в установленном законодательством Российской Федерации порядке.

6.3.8 При эксплуатации АСЗИ проводится периодический контроль эффективности защиты информации.

Контроль проводится с периодичностью, установленной законодательством Российской Федерации. Обязательным является контроль после про-

ведения ремонта средств защиты информации или при изменениях условий их эксплуатации.

Периодический контроль проводится с целью своевременного выявления недостатков в системе защиты информации АСЗИ и мониторинга стабильности характеристик системы защиты информации, влияющих на эффективность защиты информации, и заключается в оценке:

- работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

- выполнения требований к защите информации в АСЗИ;

- знаний и навыков выполнения эксплуатирующим персоналом своих функциональных обязанностей в части защиты информации.

Для проведения контроля могут привлекаться организации - обладатели лицензий на деятельность (оказание услуг) по технической защите информации, полученных в установленном в Российской Федерации порядке.

6.4 Требования к мерам защиты информации в автоматизированной системе в защищенном исполнении

6.4.1 Для решения задач защиты информации в АСЗИ принимаются организационные и технические меры защиты информации в АСЗИ, направленные на нейтрализацию угроз безопасности информации в АСЗИ.

6.4.2 Организационные и технические меры защиты технических средств АСЗИ включают:

- организацию КЗ;

- контроль и управление физическим доступом;

- защиту информации, выводимой техническими средствами, от несанкционированного просмотра;

- защиту информации, обрабатываемой и воспроизводимой техническими средствами, от утечки по техническим каналам;

- выявление возможно внедренных в технические средства АСЗИ электронных устройств негласного получения информации (закладочных устройств);

- защиту от преднамеренных силовых электромагнитных воздействий, вызывающих нарушение нормального функционирования (сбои в работе) электронных технических средств АСЗИ;

- защиту от непреднамеренных воздействий, вызывающих уничтожение, искажение, копирование, блокирование доступа к защищаемой информации, утрату, уничтожение, сбои в функционировании носителей информации или сбои в работе технических средств АСЗИ.

Организация КЗ осуществляется путем исключения неконтролируемого пребывания в ней лиц, не имеющих допуска к АСЗИ, а также посторонних транспортных средств. В пределах КЗ должны быть размещены защищаемые технические средства АСЗИ, средства защиты информации, а также средства обеспечения функционирования АСЗИ.

Контроль и управление физическим доступом осуществляются с целью исключения несанкционированного физического доступа к техническим средствам АСЗИ, средствам защиты информации в АСЗИ, средствам обеспечения функционирования АСЗИ, а также в помещения и сооружения, в которых они установлены. Требования к средствам контроля и управления физическим доступом устанавливают с учетом ГОСТ Р 51241.

Размещение технических средств вывода (визуального отображения, печати) буквенно-цифровой, видео- и графической информации, также технических средств вывода (визуального отображения) артикуляционной речевой информации должно исключать возможность несанкционированного просмотра выводимой (отображаемой) информации, как из-за пределов КЗ, так и в пределах КЗ.

Выявление возможно внедренных в технические средства АСЗИ электронных устройств негласного получения информации (закладочных устройств) осуществляется путем проведения специальных проверок технических средств АСЗИ в соответствии с законодательством Российской Федерации.

Защита информации, обрабатываемой и воспроизводимой техническими средствами АСЗИ, от утечки по техническим каналам включает:

- защиту информации, обрабатываемой техническими средствами АСЗИ, от утечки по каналам ПЭМИН;

- защиту речевой информации, обрабатываемой и воспроизводимой техническими средствами АСЗИ, от утечки по техническим каналам.

Меры защиты информации, обрабатываемой техническими средствами АСЗИ, от утечки информации по каналам ПЭМИН могут включать:

- размещение технических средств в пределах КЗ на максимально возможном удалении от ее границ;

- использование в АСЗИ технических средств в защищенном исполнении от утечки информации по каналам ПЭМИН;

- экранирование помещений, технических средств, линий электропитания и линий передачи данных;

- развязку цепей электропитания технических средств с помощью помехоподавляющих фильтров;

- электромагнитную развязку (исключение совместного пробега, экранирование) между линиями вспомогательных технических средств и систем, выходящими за пределы КЗ, и линиями, по которым циркулирует защищаемая информация;

- пространственное электромагнитное зашумление и (или) зашумление линий с помощью средств активной защиты информации от утечки по каналам ПЭМИН.

Организационные и технические меры защиты речевой информации, обрабатываемой и воспроизводимой техническими средствами АСЗИ, от утечки по техническим каналам включают:

- воспроизведение защищаемой речевой информации техническими средствами АСЗИ, а также ее обсуждение персоналом только в специально предназначенных помещениях, размещаемых в пределах КЗ на максимальном удалении от границ КЗ (далее – помещения);

- проведение специальных обследований помещений по выявлению возможно внедренных электронных устройств негласного получения информации;

- исключение размещения в помещениях индивидуальных видео- и звукозаписывающих устройств, средств связи и коммуникации, в том числе средств беспроводной связи;

- использование в АСЗИ защищенных технических средств обработки и воспроизведения речевой информации от утечки по техническим каналам;

- размещение в помещениях вспомогательных технических средств, прошедших специальные исследования по выявлению технических каналов утечки речевой информации;

- развязку (фильтрацию, размыкание) выходящих за пределы КЗ линий вспомогательных технических средств и систем, размещаемых в помещениях;

- звуко- и виброизоляцию строительных конструкций и инженерно-технических коммуникаций помещений;

- виброакустическое зашумление строительных конструкций помещений и инженерно-технических коммуникаций, а также технических средств, размещаемых в помещениях.

Требования к устойчивости функционирования технических средств АСЗИ при преднамеренном силовом электромагнитном воздействии по цепям электропитания, линиям связи, металлоконструкциям и электромагнитному полю, вызывающем разрушение, уничтожение, искажение ин-

формации или сбои в работе средств АСЗИ, устанавливают с учетом ГОСТ Р 56115.

Требования к устойчивости функционирования компонентов АСЗИ к внешним факторам, воздействующим на информацию, устанавливают с учетом ГОСТ 16325, ГОСТ 20397, ГОСТ 21552, ГОСТ 27201.

Технические средства АСЗИ должны обеспечивать сохранность информации при снижении качества электроэнергии источника электроснабжения, отключении электропитания, при авариях, а также в условиях неблагоприятных природных явлений и стихийных бедствий.

Требования к устойчивости АСЗИ к внутренним воздействующим факторам на информацию (отказы, сбои, ошибки) устанавливают совместно с требованиями по надежности и устойчивости функционирования конкретной системы или ее компонентов и по ГОСТ 16325, ГОСТ 20397, ГОСТ 21552, ГОСТ 27201.

6.4.3 Организационные и технические меры защиты от НСД к информации могут включать:

- сегментирование АСЗИ;

- идентификацию и аутентификацию субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;

- защиту машинных носителей информации;

- регистрацию событий безопасности;

- антивирусную защиту;

- обнаружение (предотвращение) компьютерных вторжений;

- обеспечение целостности информации;

- контроль содержания информации, передаваемой из АСЗИ;

- обеспечение доступности информации;

- защиту от угроз безопасности информации, направленных на отказ в обслуживании АСЗИ;

- защиту среды виртуализации;
- создание ложных компонентов АСЗИ;
- защиту остаточной информации;
- и/или другие меры защиты информации.

Сегментирование АСЗИ проводится с целью построения многоуровневой (эшелонированной) системы защиты информации в АСЗИ путем построения сегментов на различных физических доменах или средах. Сегментирование АСЗИ может проводиться с целью ее разделения на сегменты, имеющие различные классы защищенности. Сегментирование должно осуществляться с учетом структурно-функциональных характеристик АСЗИ и актуальных угроз безопасности информации и обеспечивать снижение вероятности реализации угроз и (или) их локализации в рамках одного сегмента.

Идентификация и аутентификация субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникальных признаков (идентификаторов), сравнение предъявляемых субъектами (объектами) доступа идентификаторов с перечнем присвоенных идентификаторов, а также проверку принадлежности субъектам (объектам) доступа предъявленных ими идентификаторов (подтверждение подлинности).

Требования к используемым средствам высоконадежной биометрической аутентификации устанавливают с учетом ГОСТ Р 52633.0.

Управление доступом субъектов доступа к объектам доступа должно обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в АСЗИ правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

Ограничение программной среды должно обеспечивать установку и (или) запуск только ПО, разрешенного к использованию в АСЗИ, или исключать возможность установки и (или) запуска ПО, запрещенного к использованию в АСЗИ.

Защита машинных носителей информации (средств обработки (хранения) информации, съемных машинных носителей информации) должна исключать возможность НСД к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации. Утилизация машинных носителей информации после вывода их из эксплуатации должна проводиться в установленном законодательством Российской Федерации порядке.

Регистрация событий безопасности должна обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в автоматизированной системе, а также возможность просмотра и анализа информации о таких событиях и реагирования на них.

Антивирусная защита должна обеспечивать обнаружение в АСЗИ компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Обнаружение (предотвращение) компьютерных вторжений включает регистрацию событий безопасности информации в АСЗИ, их анализ на основе правил и признаков компьютерных атак, распознавание компьютерных атак и реагирование на них.

Обеспечение целостности информации включает обнаружение фактов несанкционированного нарушения целостности ПО АСЗИ и содержащейся в ней информации, а также возможность восстановления ПО АСЗИ и содержащейся в ней информации за счет резервирования ПО, технических средств и дублирования массивов и машинных носителей информации.

Контроль содержания информации, передаваемой из АСЗИ, включает выявление запрещенной к передаче информации на основе анализа свойств объектов доступа, в которых хранится передаваемая информация, на основе

сигнатур (масок) запрещенной к передаче информации или иных методов, а также исключение неправомерной передачи информации из АСЗИ.

Обеспечение доступности информации включает авторизованный доступ пользователей, имеющих права по такому доступу, к информации в штатном режиме функционирования АСЗИ, периодическое резервное копирование информации на резервные машинные носители информации и восстановление информации с резервных машинных носителей информации при нарушении штатного режима функционирования АСЗИ.

Защита от угроз безопасности информации, направленных на отказ в обслуживании АСЗИ, включает защиту периметра АСЗИ и использование в АСЗИ технических средств с повышенными характеристиками производительности совместно с резервированием информации, технических средств и ПО АСЗИ, а также каналов передачи информации.

Защита среды виртуализации АСЗИ должна предотвращать НСД к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Требования к защите среды виртуализации АСЗИ устанавливают с учетом ГОСТ Р 56938.

Создание (эмуляция) ложных компонентов АСЗИ осуществляется для навязывания нарушителю ложных целей при реализации им компьютерных атак и обеспечивает имитацию функционирования реальных компонентов АСЗИ с целью обнаружения, регистрации и анализа действий

нарушителей по реализации компьютерных атак, а также принятия мер по их предотвращению.

Защита остаточной информации должна исключать возможность доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через общие для пользователей ресурсы АСЗИ (реестры, ресурсы файловой системы, оперативную память, внешние запоминающие устройства и т.д.).

6.4.4 Организационные и технические меры защиты каналов передачи информации включают:

- резервирование каналов передачи информации;

- использование выделенных каналов передачи информации;

- защиту линий передачи информации от несанкционированного физического доступа за пределами КЗ;

- криптографическую защиту информации, передаваемой по каналам передачи информации;

- исключение возможности отрицания отправителем факта отправки информации;

- исключение возможности отрицания получателем факта получения информации;

- выявление и блокирование скрытых каналов передачи информации;

- защиту беспроводных каналов передачи информации.

Резервирование каналов передачи информации включает использование каналов передачи от основных и альтернативных поставщиков телекоммуникационных услуг (провайдеров), контроль (проверку) наличия у провайдеров планов по восстановлению связи при авариях и сбоях, с указанием времени восстановления, а также контроль состояния и качества предоставления провайдером вычислительных ресурсов (мощностей) по передаче данных.

Использование выделенных каналов передачи информации предполагает отсутствие у таких каналов подключений к другим каналам и сетям передачи данных.

Защита линий передачи информации от несанкционированного физического доступа включает оборудование системы передачи данных средствами сигнализации о несанкционированных подключениях к металлическим или волоконно-оптическим линиям передачи данных и прекращение передачи информации по ним при обнаружении подключений.

Криптографическая защита должна быть направлена на скрытие, модификацию и навязывание (ввод ложной) информации при ее передаче (подготовке к передаче) по каналам передачи информации, имеющим выход за пределы КЗ. Требования и порядок использования средств криптографической защиты информации определяются в установленном законодательством Российской Федерации порядке.

Исключение возможности отрицания отправителем факта отправки информации включает генерацию свидетельства отправления информации (например, электронную цифровую подпись) и его верификацию (проверку), а также запись и защищенное хранение в течение установленного времени информации при отправке. Требования к формированию и проверке электронной цифровой подписи устанавливаются с учетом ГОСТ Р 34.10, ГОСТ Р 34.11.

Исключение возможности отрицания получателем факта получения информации включает генерацию свидетельства получения информации (например, запрос подтверждения получения, электронная цифровая подпись) и его верификацию (проверку), а также запись и защищенное хранение в течение установленного времени полученной информации.

Выявление, анализ и блокирование скрытых каналов передачи информации осуществляется на этапах разработки и реализации системы защиты информации в АСЗИ с учетом ГОСТ Р 53113.1, ГОСТ Р 53113.2.

Защита беспроводных каналов передачи информации включает ограничение и контроль использования в АСЗИ беспроводных каналов передачи информации в строгом соответствии с задачами (функциями) АСЗИ, для решения которых такие каналы необходимы, а также использование программно-технических средств обнаружения и блокирования несанкционированных беспроводных каналов передачи информации.

6.4.5 Меры защиты информации при информационном взаимодействии с иными автоматизированными системами и информационно-телекоммуникационными сетями включают:

- ограничение числа точек доступа в АСЗИ из иных автоматизированных систем и информационно-телекоммуникационных сетей;

- управление взаимодействием с иными автоматизированными системами и информационно-телекоммуникационными сетями;

- защиту периметра АСЗИ.

Количество точек доступа в АСЗИ из иных автоматизированных систем и информационно-телекоммуникационных сетей должно быть ограничено до минимально необходимого числа для решения задач АСЗИ по прямому назначению. При этом для каждого внешнего телекоммуникационного сервиса должен применяться отдельный физический управляемый (контролируемый) сетевой интерфейс.

Управление взаимодействием с иными автоматизированными системами и информационно-телекоммуникационными сетями, информационное взаимодействие с которыми необходимо для функционирования АСЗИ, должно включать установление информационного взаимодействия на основании заключенного договора (соглашения) с оператором (обладателем) иной автоматизированной системы и (или) при наличии подтверждения выполнения в иной автоматизированной системе требований к защите информации, предоставление доступа к АСЗИ только авторизованным (уполномоченным) пользователям из иных автоматизированных систем, определение информационных ресурсов и типов ПО АСЗИ, к ко-

торым разрешен доступ авторизованным (уполномоченным) пользователям из иных автоматизированных систем, а также определение порядка обработки, хранения и передачи информации с использованием иных автоматизированных систем.

Защита периметра (физических и (или) логических границ) АСЗИ осуществляется за счет обеспечения взаимодействия АСЗИ и (или) ее сегментов с иными автоматизированными системами и информационно-телекоммуникационными сетями только через сетевые интерфейсы, которые обеспечивают управление (фильтрацию, маршрутизацию, контроль соединений, однонаправленную передачу и другие способы управления и контроля) информационными потоками из иных автоматизированных систем во внутренние сегменты АСЗИ.

6.4.6 Конкретные состав и содержание мер защиты информации в АСЗИ определяются в зависимости от актуальных угроз безопасности информации и класса защищенности АСЗИ, установленного в соответствии с законодательством Российской Федерации.

6.4.7 Технические меры защиты информации реализуются посредством применения средств защиты информации, реализующих необходимые функции безопасности.

В случаях, предусмотренных законодательством Российской Федерации, для обеспечения защиты информации в АСЗИ применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

6.5 Требования к основным видам обеспечения автоматизированной системы в защищенном исполнении

6.5.1 Требования к защите информации предъявляются к следующим основным видам обеспечения АСЗИ:

- техническое обеспечение АСЗИ (включая объекты капитального строительства, в которых устанавливаются АСЗИ, и их инженерно-технические системы);

- программное обеспечение АСЗИ;

- информационное обеспечение АСЗИ.

6.5.2 Требования к техническому обеспечению АСЗИ включают:

- резервирование технических средств и средств обеспечения функционирования АСЗИ;

- обеспечение безотказного функционирования технических средств и средств обеспечения функционирования АСЗИ;

- требования к системе электропитания и заземления АСЗИ.

Резервирование технических средств в зависимости от требуемых условий обеспечения непрерывности функционирования АСЗИ включает ненагруженное и (или) нагруженное резервирование.

Обеспечение безотказного функционирования технических средств и средств обеспечения функционирования АСЗИ включает обнаружение и локализацию отказов их функционирования, а также принятие мер по восстановлению отказавших средств, их тестирование и документирование отказов.

Методы контроля, испытаний и приемки технических средств АСЗИ устанавливают с учетом ГОСТ 23773.

Требования к системе электропитания и заземления АСЗИ включают:

- резервирование электропитания АСЗИ с использованием кратковременных резервных источников питания для корректного завершения

работы АСЗИ и (или) долговременных резервных источников питания для продолжения функционирования АСЗИ;

- устройство электрических установок и системы электропитания в соответствии с требованиями, установленными законодательством Российской Федерации;

- исключение использования в качестве заземляющего устройства нулевых рабочих проводников промышленной электросети, металлоконструкций зданий и металлических инженерно-технических систем, имеющих соединение с заземляющем устройством;

- размещение электрических установок (трансформаторных подстанций, автономных источников и т.п.), кабелей и устройств, предназначенных для электропитания и заземления технических средств АСЗИ, в пределах КЗ;

- использование заземляющих проводников, шин заземления и контактных соединений, обеспечивающих минимальное электрическое сопротивление, а также механическую прочность и устойчивость к коррозии;

- присоединение каждого заземляемого технического средства АСЗИ к заземляющему проводнику при помощи отдельного параллельного ответвления, исключение использования последовательного присоединения нескольких заземляемых технических средств;

- отсутствие в системе заземления замкнутых контуров.

Проектирование новых и реконструкцию действующих объектов капитального строительства (зданий, помещений), в которых устанавливаются АСЗИ, и их инженерно-технических систем рекомендуется осуществлять с учетом требований к защите информации. Задание требований и выбор проектных технических решений к защите информации осуществляются в установленным законодательством Российской Федерации порядке.

6.5.3 Требования к ПО АСЗИ включают:

- обеспечение безопасной разработки ПО АСЗИ;

- использование ПО, удовлетворяющего требованиям к качеству;

- резервирование ПО АСЗИ.

Требования к обеспечению безопасной разработки ПО АСЗИ устанавливаются с учетом ГОСТ Р 56939.

Требования к качеству ПО АСЗИ устанавливаются с учетом ГОСТ Р ИСО/МЭК 12119, ГОСТ Р ИСО/МЭК 9126, ГОСТ 28195.

При резервировании ПО осуществляется создание резервных копий общесистемного, специального и прикладного ПО, а также их настроек, относящихся к защите информации.

6.5.4 Конкретный состав и содержание требований к техническому и программному обеспечению АСЗИ определяется в зависимости от актуальных угроз безопасности информации и класса защищенности АСЗИ в установленным законодательством Российской Федерации порядке.

6.5.5 Требования к информационному обеспечению АСЗИ включают требования к документации на систему защиты информации в АСЗИ.

Проектная и эксплуатационная документация на систему защиты информации АСЗИ должна включать:

- цели и задачи защиты информации в АСЗИ;

- перечень объектов защиты информации в АСЗИ;

- результаты определения структуры, сегментов, степени распределенности АСЗИ, а также наличия подключения АСЗИ к иным автоматизированным системам и информационно-телекоммуникационным сетям;

- акт классификации АСЗИ по требованиям защиты информации;

- перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать АСЗИ;

- модель угроз безопасности информации в АСЗИ (при необходимости);

- состав и содержание организационных и технических мер защиты информации и блокирования (нейтрализации) угроз безопасности информации в АСЗИ;

- правила разграничения доступа, регламентирующие права доступа субъектов доступа к объектам доступа в АСЗИ;

- состав, порядок установки и настройки ПО АСЗИ;

- состав, порядок наладки и сопряжения технических средств АСЗИ;

- схему границы КЗ;

- состав и схемы размещения относительно границ КЗ основных и вспомогательных технических средств АСЗИ, схемы прокладки линий передачи данных и их выходы за пределы КЗ, схемы прокладки линий электропитания и заземления технических средств АСЗИ;

- состав и схемы размещения относительно границ КЗ технических средств управления и контроля физическим доступом, средств защиты технических средств АСЗИ (включая средства активной защиты, встраиваемые в линии средства пассивной защиты, размыкатели линий и др.), а также технических средств защиты линий связи и передачи данных;

- описание логических границ (периметра) АСЗИ;

- состав, места установки, параметры и порядок настройки программно-аппаратных средств защиты информации от НСД;

- перечень и реквизиты сертификатов соответствия на средства защиты информации;

- виды, объем и порядок проведения испытаний системы защиты информации АСЗИ.

Проектная и эксплуатационная документация на систему защиты информации АСЗИ должна определять правила и процедуры:

- контроля и управления физическим доступом;

- изменения условий эксплуатации, состава и конфигурации технических средств и ПО АСЗИ;

- управления конфигурацией ПО АСЗИ;

- установления правил разграничения доступа и введения ограничений на действия пользователей;

- отработки действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации;

- управления (администрирования) системой защиты информации АСЗИ;

- управления взаимодействием с иными автоматизированными системами;

- резервирования технических средств и каналов передачи информации;

- резервирования электропитания технических средств;

- резервирования ПО и информации;

- обновления ПО в АСЗИ;

- выявления инцидентов и реагирования на них;

- анализа и устранения уязвимостей АСЗИ;

- периодического контроля эффективности защиты информации в АСЗИ;

- документирования отказов функционирования технических средств и средств обеспечения функционирования АСЗИ;

- защиты информации при выводе из эксплуатации АСЗИ или после принятия решения об окончании обработки информации.

Библиография

[1] Федеральный закон от 27 июля 2006 г. № 149-ФЗ — Об информации, информационных технологиях и о защите информации

УДК ОКС 35.020

Ключевые слова: информация, защита информации, автоматизированная система в защищенном исполнении
