ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 51583— 2014

Защита информации

ПОРЯДОК СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Общие положения

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 января 2014 г. № 3-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ПЕРЕИЗДАНИЕ. Октябрь 2018 г.

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «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 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 агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Обозначения и сокращения 2
5 Общие положения 3
6 Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении 5
7 Содержание и порядок выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении 10
Приложение А (справочное) Примерный перечень и содержание нормативной информации национальных стандартов, рекомендуемых к применению при создании автоматизированных систем в защищенном исполнении 12
Библиография 13

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ПОРЯДОК СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Общие положения

Information protection. Sequence of protected operational systems formation. General provisions

Дата введения — 2014—09—01

1 Область применения

Настоящий стандарт распространяется на создаваемые (модернизируемые) информационные автоматизированные системы, в отношении которых законодательством или заказчиком установлены требования по их защите, и устанавливает содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении, содержание и порядок выполнения работ по защите информации о создаваемой (модернизируемой) автоматизированной системе в защищенном исполнении.

Примечание — В качестве основных видов автоматизированных систем рассматриваются автоматизированные рабочие места и информационные системы.

Положения настоящего стандарта дополняют положения комплекса стандартов «Информационная технология. Комплекс стандартов на автоматизированные системы» в части порядка создания автоматизированных систем в защищенном исполнении.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 34.003 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

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

ГОСТ 34.601 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

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

ГОСТ 34.603 Информационная технология. Виды испытаний автоматизированных систем

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

ГОСТ Р 50922 Защита информации. Основные термины и определения

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

ГОСТ Р 54869 Проектный менеджмент. Требования к управлению проектом

ГОСТ Р 57628 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности

Издание официальное

ГОСТ Р ИСО/МЭК 15408-1 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО/МЭК 15408-2 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

ГОСТ Р ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

ГОСТ Р ИСО/МЭК 18045 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий

ГОСТ Р ИСО/МЭК 21827 Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса

ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

ГОСТ Р ИСО/МЭК ТО 19791 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт 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 Р 50922, ГОСТ Р 53114, ГОСТ 34.003, ГОСТ 16504, а также следующие термины с соответствующими определениями:

3.1 **мероприятия по защите информации:** Совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации.

3.2 **обработка информации:** Выполнение любого действия (операции) или совокупности действий (операций) с информацией (например, сбор, накопление, ввод, вывод, прием, передача, запись, хранение, регистрация, преобразование, отображение и т. п.), совершаемых с заданной целью.

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

3.4 **информационная система:** Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения:

АС — автоматизированная система;

АСЗИ — автоматизированная система в защищенном исполнении;

ЗИ — защита информации;

НИР — научно-исследовательская работа;

НСД — несанкционированный доступ;

ОКР — опытно-конструкторская работа;

ПС — программное средство;
СЗИ — средство защиты информации;
ТЗ — техническое задание;
ТТЗ — тактико-техническое задание;
ТС — техническое средство.

5 Общие положения

5.1 Для обработки информации, необходимость защиты которой определяется законодательством Российской Федерации или решением ее обладателя, должны создаваться АСЗИ, в которых реализованы в соответствии с действующими нормативными правовыми актами требования о ЗИ. Реализация требований о ЗИ в АСЗИ осуществляется системой ЗИ, являющейся неотъемлемой составной частью АСЗИ.

5.2 Целью создания системы ЗИ АСЗИ является обеспечение ЗИ от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации, соблюдение конфиденциальности информации ограниченного доступа, реализация права на доступ к информации.

5.3 При создании (модернизации) АСЗИ необходимо руководствоваться следующими общими требованиями:

- система ЗИ АСЗИ должна обеспечивать комплексное решение задач по ЗИ от НСД, от утечки защищаемой информации по техническим каналам, от несанкционированных и непреднамеренных воздействий на информацию (на носители информации) применительно к конкретной АСЗИ. Состав решаемых задач по ЗИ определяется задачами обработки информации, решаемыми с использованием АСЗИ, ее программным и аппаратным составом, конфигурацией этой системы, условиями функционирования, требованиями, предъявляемыми к обрабатываемой информации, угрозами безопасности информации;
- система ЗИ АСЗИ должна разрабатываться (проектироваться) с учетом возможности реализации требований о защите обрабатываемой информации при использовании в АСЗИ методов и программно-аппаратных средств организации сетевого взаимодействия;
- система ЗИ АСЗИ должна создаваться с учетом обеспечения возможности формирования различных вариантов ее построения, а также расширения возможностей ее составных частей (сегментов) в зависимости от условий функционирования АСЗИ и требований о ЗИ;
- ЗИ должна обеспечиваться во всех составных частях (сегментах) АСЗИ, используемых в обработке защищаемой информации;
- входящие в состав АСЗИ средства ЗИ и контроля эффективности ЗИ не должны препятствовать нормальному функционированию АСЗИ;
- программное обеспечение системы ЗИ должно быть совместимым с программным обеспечением других составных частей (сегментов) АСЗИ и не должно снижать требуемый уровень защищенности информации в АСЗИ;
- программно-технические средства, используемые для построения системы ЗИ, должны быть совместимы между собой (корректно работать совместно) и не должны снижать уровень защищенности информации в АСЗИ.

ЗИ о создаваемой АСЗИ является составной частью работ по их созданию и осуществляется во всех организациях, участвующих в процессе создания (модернизации) этих систем.

5.4 Обеспечение ЗИ в АСЗИ достигается заданием, реализацией и контролем выполнения требований о защите информации:

- к процессу хранения, передачи и обработки защищаемой в АСЗИ информации;
- к системе ЗИ;
- к взаимодействию АСЗИ с другими АС;
- к условиям функционирования АСЗИ;
- к содержанию работ по созданию (модернизации) АСЗИ на различных стадиях и этапах ее создания (модернизации);
- к организациям (должностным лицам), участвующим в создании (модернизации) и эксплуатации АСЗИ;
- к документации на АСЗИ;
- к АСЗИ в целом.

5.5 АСЗИ должны создаваться в соответствии с ТЗ, являющимся основным документом, на основании которого выполняются работы, необходимые для создания (модернизации) АСЗИ в целом и ее системы ЗИ, и осуществляется приемка этих работ заказчиком.

5.6 Процесс создания АСЗИ должен представлять собой совокупность упорядоченных во времени, взаимосвязанных, объединенных в стадии и этапы работ, выполнение которых необходимо и достаточно для создания АСЗИ, соответствующей заданным к ней требованиям.

5.7 В работах по созданию (модернизации) АСЗИ и ее системы ЗИ участвуют:

- заказчик АСЗИ — в части задания в ТЗ на АСЗИ и систему ЗИ, включения в документацию на АСЗИ обоснованных требований о защите обрабатываемой АСЗИ информации и контроля их выполнения в процессе экспертизы документации, испытаний и приемки как АСЗИ в целом, так и системы ЗИ, а также в части организации аттестации АСЗИ на соответствие требованиям безопасности информации и сопровождения АСЗИ в ходе ее эксплуатации;
- разработчик АСЗИ — в части обеспечения соответствия разрабатываемой АСЗИ и ее системы ЗИ требованиям ТЗ, нормативных правовых актов, методических документов и национальных стандартов в области защиты информации;
- изготовитель ТС и ПС — в части осуществления технических мер по обеспечению соответствия изготавливаемых ТС и ПС заданным требованиям о защите обрабатываемой АСЗИ информации в соответствии с документацией на АСЗИ;
- поставщик ТС и ПС — в части поставки ТС и ПС для АСЗИ, соответствующих требованиям по ЗИ, по заказу изготовителя, разработчика или заказчика и их гарантийного и послегарантийного обслуживания.

5.8 Организации, участвующие в создании АСЗИ, в случае выполнения работ и оказания услуг в области ЗИ, деятельность по осуществлению которых подлежит лицензированию, должны иметь соответствующие лицензии [1]—[4].

5.9 Стадии и этапы работ по созданию АСЗИ устанавливаются в ТЗ на АСЗИ на основе ГОСТ 34.601 с учетом положений настоящего стандарта.

5.10 Типовое содержание работ в части создания системы ЗИ (на определенных в ГОСТ 34.601 стадиях и этапах создания АСЗИ) приведено в разделе 6. Типовое содержание и порядок выполнения работ по ЗИ о создаваемой АСЗИ приведены в разделе 7. Состав и содержание работ могут уточняться в соответствии с требованиями нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов по ЗИ, а также в соответствии с требованиями заказчика АСЗИ.

5.11 В ТЗ на создание АСЗИ для реализуемых в соответствии с ним стадий и этапов ее создания должны включаться требования к системе ЗИ АСЗИ, а также требования по ЗИ о создаваемой АСЗИ в соответствии с настоящим стандартом, нормативными правовыми актами и методическими документами уполномоченных федеральных органов исполнительной власти и другими национальными стандартами.

5.12 Мероприятия по ЗИ должны проводиться на всех стадиях и этапах создания АСЗИ с учетом применимых (исходя из предназначения АСЗИ) требований нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов в области ЗИ.

5.13 Для АСЗИ, создаваемой на базе действующей АС, разрабатывают ТЗ на создание системы ЗИ или дополнение к основному ТЗ на АС, в которое включают требования к системе ЗИ, а также к той части АС, которая подлежит доработке (модернизации) в связи с включением в состав АС системы ЗИ.

5.14 Разработка, утверждение и согласование ТЗ или дополнения к ТЗ на модернизируемую АС осуществляется в порядке, установленном ГОСТ 34.602.

5.15 Документация на АСЗИ должна разрабатываться с учетом требований ГОСТ 34.201 и [5], а также требований нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов по ЗИ.

5.16 Работы по созданию АСЗИ должны проводиться в соответствии с требованиями нормативных правовых актов и методических документов уполномоченного федерального органа исполнительной власти, настоящего стандарта и других национальных стандартов по ЗИ. Дополнительно при необходимости могут учитываться требования национальных стандартов, приведенных в приложении А.

5.17 Для создания АСЗИ могут применяться как серийно выпускаемые, так и специальные (разрабатываемые в ходе создания АСЗИ) ТС и ПС обработки информации, а также технические, программные, программно-аппаратные, криптографические СЗИ и средства контроля эффективности ЗИ.

Указанные средства должны иметь сертификаты соответствия, полученные в соответствующих системах сертификации по требованиям безопасности информации [6], [7]. Специальные средства должны быть сертифицированы в установленном порядке до начала опытной эксплуатации АСЗИ организациями (учреждениями), имеющими лицензии уполномоченных федеральных органов исполнительной власти на соответствующие виды деятельности.

5.18 Работы по созданию и эксплуатации АСЗИ с использованием криптографических средств организуются в соответствии с положениями нормативных актов Российской Федерации, определяющих порядок разработки, изготовления, сопровождения и эксплуатации криптографических средств.

5.19 Организационно-методическое руководство работами по созданию, изготовлению, обеспечению и эксплуатации средств криптографической ЗИ, по сертификации этих средств осуществляет федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности.

5.20 Перед вводом в эксплуатацию комплексов ТС АСЗИ (в случае отсутствия документа, подтверждающего уже проведенные исследования) и периодически в процессе их эксплуатации проводятся исследования по криптографической ЗИ в составе комплексов ТС АСЗИ организациями, имеющими лицензию на этот вид работ в соответствии с [4].

5.21 Порядок эксплуатации АСЗИ с использованием криптографических средств регламентируется законодательством Российской Федерации и нормативными правовыми актами федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности.

5.22 Организация надлежащего исполнения правил эксплуатации средств криптографической ЗИ (в том числе во время приемочных испытаний) возлагается на руководство организаций, эксплуатирующих данные средства.

Контроль выполнения требований инструкций по эксплуатации средств криптографической ЗИ возлагается на специальные подразделения (штатных специалистов) по ЗИ на предприятии (организации), эксплуатирующем данные средства.

5.23 Виды испытаний АСЗИ и общие требования к их проведению определяются ГОСТ 34.603, а также нормативными правовыми актами и методическими документами уполномоченного федерального органа исполнительной власти и национальными стандартами по ЗИ.

5.24 Испытания АСЗИ на соответствие требованиям безопасности информации от ее утечки по техническим каналам, несанкционированного доступа к ней, от несанкционированных и непреднамеренных воздействий на информацию, в том числе по криптографической и антивирусной защите, по обнаружению вторжений (атак) и др. осуществляются в соответствии с положениями нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов.

5.25 В случаях, установленных федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации, нормативными правовыми актами уполномоченных федеральных органов исполнительной власти, для подтверждения соответствия системы ЗИ АСЗИ в реальных условиях эксплуатации требованиям безопасности информации осуществляется аттестация АСЗИ на соответствие требованиям безопасности информации.

5.26 Аттестация АСЗИ проводится до ввода АСЗИ в постоянную эксплуатацию в соответствии с положениями нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов.

6 Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении

6.1 Защита информации в АСЗИ обеспечивается системой ЗИ АСЗИ. Создание системы ЗИ АСЗИ обеспечивается следующим комплексом работ:

- формирование требований к системе ЗИ АСЗИ;
- разработка (проектирование) системы ЗИ АСЗИ;
- внедрение системы ЗИ АСЗИ;
- аттестация АСЗИ на соответствие требованиям безопасности информации и ввод ее в действие;
- сопровождение системы ЗИ в ходе эксплуатации АСЗИ.

6.2 Формирование требований к системе ЗИ АСЗИ организуется заказчиком и осуществляется разработчиком на основе требований по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, несанкционированных и непреднамеренных воздействий

на информацию, в том числе требований по криптографической и антивирусной защите, по обнаружению вторжений (атак), обеспечению устойчивости и непрерывности функционирования АСЗИ и др., закрепленных в нормативных правовых актах уполномоченных федеральных органов исполнительной власти и национальных стандартах в области ЗИ, с учетом целей и задач АСЗИ, свойственных ей угроз безопасности информации и возможных последствий реализации этих угроз.

Формирование требований к системе ЗИ АСЗИ осуществляется на следующих стадиях создания АСЗИ, определенных ГОСТ 34.601:

- «Формирование требований к АС»;
- «Разработка концепции АС»;
- «Техническое задание».

Требования к системе ЗИ АСЗИ уточняются (при необходимости) на последующих стадиях создания АСЗИ, с конкретизацией требований к ее построению, используемым информационным технологиям, методам и программно-аппаратным средствам организации сетевого взаимодействия, в том числе с другими системами, к процессу обработки защищаемой информации, условиям функционирования АСЗИ.

6.3 На стадии «Формирование требований к АС» в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ выполняют следующие работы.

6.3.1 На этапе «Обследование объекта и обоснование необходимости создания АС» проводят:

- анализ данных о назначении, функциях, условиях функционирования создаваемой (модернизируемой) АСЗИ и характере обрабатываемой информации;
- определение перечня информации, подлежащей защите;
- определение актуальных угроз безопасности информации, связанных с НСД к защищаемой информации, с утечкой информации по техническим каналам и с несанкционированным воздействием на информацию;
- разработку модели угроз безопасности информации применительно к конкретным вариантам функционирования АСЗИ;
- оценку (технико-экономической и т. п.) целесообразности создания АС в защищенном исполнении.

6.3.2 На этапе «Формирование требований пользователя к АС» проводят:

а) подготовку исходных данных для формирования требований в части системы ЗИ к создаваемой (модернизируемой) АСЗИ (исходя из ее предназначения и условий использования), включая:

- определение порядка обработки информации в АСЗИ в целом и в отдельных компонентах;
- оценку степени участия персонала в обработке (обсуждении, передаче, хранении) защищаемой в АСЗИ информации;
- определение требуемого класса (уровня) защищенности АСЗИ от НСД;
- выбор целесообразных (исходя из экономических, научно-технических, временных и других ограничений, а также технологии обработки информации) способов ЗИ и контроля состояния ЗИ в АСЗИ;
- обоснование архитектуры и конфигурации системы ЗИ АСЗИ и ее отдельных составных частей, физических, функциональных и технологических связей как внутри АСЗИ, так и с другими взаимодействующими системами;
- выбор ТС, которые могут быть использованы при разработке системы ЗИ АСЗИ;
- оценку возможности создания АСЗИ, исходя из ресурсных ограничений;

б) формирование требований к системе ЗИ создаваемой (модернизируемой) АСЗИ в части требований о защите информации.

6.3.3 На этапе «Оформление отчета о выполненной работе и заявки на разработку АС (ТТЗ)» проводят:

- систематизацию результатов, полученных на предыдущих этапах;
- формирование разделов отчета о выполненных работах на данной стадии в части создания системы ЗИ для создаваемой (модернизируемой) АСЗИ;
- оформление заявки на разработку системы ЗИ (ТЗ или дополнения к ТЗ) или другого заменяющего её документа с аналогичным содержанием (в случае разработки отдельного ТЗ на систему ЗИ АСЗИ).

6.4 На стадии «Разработка концепции АС» в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ выполняют следующие работы.

6.4.1 На этапе «Изучение объекта» проводят:

- определение путей и оценку возможности реализации требований, предъявляемых к системе ЗИ создаваемой (модернизируемой) АСЗИ;
- обоснование необходимости привлечения организаций, имеющих необходимые лицензии, для создания системы ЗИ создаваемой (модернизируемой) АСЗИ;
- оценку ориентировочных сроков создания системы ЗИ АСЗИ;
- оценку материальных, трудовых и финансовых затрат на разработку и внедрение системы ЗИ создаваемой (модернизируемой) АСЗИ;
- обоснование целесообразности проведения НИР (составной части НИР), определение основных вопросов, подлежащих исследованию в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ;
- разработку ТТЗ на НИР (при необходимости).

6.4.2 На этапе «Проведение необходимых научно-исследовательских работ» проводят:
- анализ требований к назначению, структуре и конфигурации создаваемой (модернизируемой) АСЗИ;
- уточнение режимов обработки информации в АСЗИ в целом и в отдельных компонентах;
- анализ возможных уязвимостей и обоснование актуальных угроз безопасности информации и перечня мероприятий по их блокированию (нейтрализации);
- уточнение требований о ЗИ в АСЗИ;
- уточнение требований к архитектуре и конфигурации системы ЗИ АСЗИ;
- уточнение требований к составу и характеристикам основных и вспомогательных ПС и ТС, которые могут быть использованы при разработке системы ЗИ АСЗИ, режимам их работы;
- обоснование перечня сертифицированных средств ЗИ, использование которых возможно в составе системы ЗИ создаваемой (модернизируемой) АСЗИ;
- уточнение оценки материальных, трудовых и финансовых затрат на создание системы ЗИ создаваемой (модернизируемой) АСЗИ.
- оформление и утверждение отчета о НИР.

6.4.3 На этапе «Разработка вариантов концепции АС и выбор варианта концепции АС, удовлетворяющего требованиям пользователя» проводят:
- разработку альтернативных вариантов концепции создаваемой системы ЗИ и планов их реализации;
- оценку необходимых ресурсов на реализацию каждого варианта и обеспечение функционирования системы ЗИ;
- оценку эффектов, преимуществ и недостатков от реализации каждого варианта;
- выбор варианта концепции системы ЗИ АСЗИ.

6.4.4 На этапе «Оформление отчета о выполненной работе» разрабатывается самостоятельный отчет о работах, выполненных на стадии «Разработка концепции АС» в части системы ЗИ, или раздел в основной отчет о работах, выполненных в интересах создания (модернизации) АСЗИ в целом.

6.5 На стадии «Техническое задание» в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ выполняют следующие работы.

На этапе «Разработка и утверждение технического задания на создание АС» проводят разработку, оформлнение, согласование и утверждение ТЗ на АСЗИ в целом и, при необходимости, ТЗ на систему ЗИ.

ТЗ (раздел ТЗ, дополнение к ТЗ) на систему ЗИ должно разрабатываться в соответствии с требованиями ГОСТ 34.602.

6.6 Разработка (проектирование) системы ЗИ АСЗИ включает:
- разработку проектных решений по системе ЗИ АСЗИ;
- разработку документации на систему ЗИ АСЗИ;
- тестирование системы ЗИ АСЗИ.

6.7 Разработку системы ЗИ АСЗИ организует заказчик, проводит разработчик в соответствии с ТЗ на создание системы ЗИ АСЗИ на следующих стадиях создания АСЗИ, определенных ГОСТ 34.601:
- Эскизный проект;
- Технический проект;
- Рабочая документация.

6.8 На стадии «Эскизный проект» в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ выполняют следующие работы.

6.8.1 На этапе «Разработка предварительных проектных решений по системе и ее частям» проводят:

- определение субъектов доступа (пользователей, процессов и иных субъектов доступа) и объектов доступа (устройств, объектов файловой системы, запускаемых и исполняемых модулей, объектов системы управления базами данных, объектов, создаваемых прикладным программным обеспечением, иных объектов доступа);
- уточнение исходных данных, касающихся технических, информационных, программных и организационных аспектов создания и функционирования системы ЗИ АСЗИ и АСЗИ в целом;
- определение функций системы ЗИ создаваемой (модернизируемой) АСЗИ, состава комплексов задач и отдельных задач, решаемых подсистемой ЗИ;
- проработку и рассмотрение вариантов построения системы ЗИ с учетом результатов ранее проведенных исследований и новейших достижений науки и техники, в том числе по зарубежным аналогам, определение общих требований к системе ЗИ (ее структура, состав (число) и места размещения составных частей системы ЗИ);
- определение функций и параметров ТС и ПС системы ЗИ, особенностей их реализации в интересах блокирования (нейтрализации) угроз безопасности информации в АСЗИ;
- определение состава организационных мер ЗИ, ТС и ПС системы ЗИ, выбор сертифицированных СЗИ с учетом их совместимости с основными ТС и ПС создаваемой (модернизируемой) АСЗИ;
- обоснование номенклатуры СЗИ, специального технологического оборудования, средств контроля и измерений, подлежащих разработке в ходе создания АСЗИ.

6.8.2 На этапе «Разработка документации на АС и ее части» проводят разработку, оформление, согласование и утверждение документации в объеме, необходимом для описания полной совокупности принятых предварительных проектных решений и достаточном для дальнейшего выполнения работ по созданию системы ЗИ. Виды документов — по ГОСТ 34.201.

6.9 На стадии «Технический проект» в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ выполняют следующие работы.

6.9.1 На этапе «Разработка проектных решений по системе и ее частям» обеспечивают:

- разработку общих решений по системе ЗИ, по ее функциональной структуре, ТС и ПС системы ЗИ, алгоритмам функционирования системы ЗИ, функциям персонала, обслуживающего систему ЗИ;
- разработку алгоритмов решения задач ЗИ, параметров настройки ТС и ПС, обеспечивающих реализацию функциональных возможностей системы ЗИ;
- разработку макетов составных частей системы ЗИ (при необходимости).

6.9.2 На этапе «Разработка документации на АС и ее части» проводят разработку, оформление, согласование и утверждение технической документации на систему ЗИ. Виды документов — по ГОСТ 34.201.

6.9.3 На этапе «Разработка и оформление документации на поставку изделий для комплектования АС и (или) технических требований (технических заданий) на их разработку» проводят:

- подготовку и оформление документов на поставку ТС и ПС для комплектования системы ЗИ создаваемой (модернизируемой) АСЗИ;
- определение технических требований и составление ТЗ на разработку специальных СЗИ, специального технологического оборудования, средств контроля и измерений, не изготавливаемых серийно.

6.9.4 На этапе «Разработка заданий на проектирование в смежных частях проекта объекта информатизации» осуществляют разработку, оформление, согласование и утверждение заданий на проектирование помещений для АСЗИ с учетом требований о ЗИ.

6.10 На стадии «Рабочая документация» в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ проводят следующие работы.

6.10.1 На этапе «Разработка рабочей документации на систему и ее части» осуществляют разработку рабочей документации на систему ЗИ, содержащей все необходимые и достаточные сведения для обеспечения выполнения работ по вводу системы ЗИ АСЗИ в действие и ее эксплуатации, в том числе для поддержания уровня эксплуатационных характеристик (качества) системы ЗИ в соответствии с принятыми проектными решениями, ее оформление, согласование и утверждение, а также разработку программы и методик испытаний системы ЗИ. Виды документов — по ГОСТ 34.201.

6.10.2 На этапе «Разработка и адаптация программ» проводят:

- разработку ПС для СЗИ, адаптацию и/или привязку приобретаемых ПС, тестирование ПС системы ЗИ АСЗИ;

- разработку и испытания СЗИ, технологического оборудования, средств контроля и измерений системы ЗИ АСЗИ;
- сертификацию разрабатываемых ПС и СЗИ системы ЗИ АСЗИ по требованиям безопасности информации;
- разработку документации на ПС и СЗИ системы ЗИ АСЗИ;
- тестирование ПС системы ЗИ АСЗИ.

При тестировании ПС системы ЗИ АСЗИ:

- проверяют работоспособность и совместимость ПС системы ЗИ с информационными технологиями и ТС обработки информации;
- проверяют выполнение ПС системы ЗИ требований к системе ЗИ АСЗИ;
- корректируют документацию на систему ЗИ АСЗИ (при необходимости).

6.11 Внедрение системы ЗИ АСЗИ включает:

- установку и настройку СЗИ;
- разработку организационно-распорядительных документов, определяющих мероприятия по ЗИ в ходе эксплуатации АСЗИ;
- предварительные испытания системы ЗИ АСЗИ;
- опытную эксплуатацию и доработку системы ЗИ АСЗИ;
- приемочные испытания системы ЗИ АСЗИ;
- аттестацию АСЗИ на соответствие требованиям безопасности информации.

6.12 Внедрение системы ЗИ АСЗИ организует заказчик, проводит разработчик в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации [8] и рабочей документацией на систему ЗИ АСЗИ на стадии «Ввод в действие», определенной ГОСТ 34.601.

6.13 На стадии «Ввод в действие» в интересах внедрения системы ЗИ создаваемой (модернизируемой) АСЗИ проводят следующие работы.

6.13.1 На этапе «Подготовка объекта к вводу АС в действие» проводят работы по реализации:

- проектных решений по организационной структуре системы ЗИ создаваемой (модернизируемой) АСЗИ и АСЗИ в целом;
- организационных мер, обеспечивающих эффективное использование системы ЗИ.

6.13.2 На этапе «Подготовка персонала» проводят:

- обучение персонала АСЗИ и проверку его способности обеспечивать функционирование системы ЗИ и АСЗИ в целом;
- проверку и подготовку специалистов структурного подразделения или должностного лица (работника), ответственных за ЗИ в АСЗИ.

6.13.3 На этапе «Комплектация АС поставляемыми изделиями (программными и техническими средствами, программно-техническими комплексами, информационными изделиями)»:

- обеспечивают получение комплектующих изделий системы ЗИ серийного и единичного производства, материалов и монтажных изделий;
- проводят входной контроль качества комплектующих изделий системы ЗИ, проверку наличия документов по сертификации;
- проводят специальные исследования и специальные проверки закупленных средств.

6.13.4 На этапе «Строительно-монтажные работы» осуществляют:

- надзор за выполнением строительными организациями требований ЗИ;
- проверку реализации требований о ЗИ при приемке монтажных работ (в случае необходимости проводят соответствующие испытания).

6.13.5 На этапе «Пусконаладочные работы» осуществляют:

- автономную наладку ТС и ПС системы ЗИ;
- комплексную наладку всех СЗИ системы ЗИ.

6.13.6 На этапе «Проведение предварительных испытаний» осуществляют:

- испытания системы ЗИ на работоспособность и соответствие техническому заданию в соответствии с программой и методикой предварительных испытаний;
- устранение недостатков, выявленных в процессе испытаний, и внесение изменений в документацию на систему ЗИ создаваемой (модернизируемой) АСЗИ, в том числе эксплуатационную, в соответствии с протоколом испытаний;
- принятие решения о возможности опытной эксплуатации системы ЗИ АСЗИ.

6.13.7 На этапе «Проведение опытной эксплуатации» проводят:

- проверку функционирования системы ЗИ в составе АСЗИ, в том числе реализованных мер ЗИ;
- анализ выявленных в ходе опытной эксплуатации системы ЗИ уязвимостей АСЗИ, доработку, наладку системы ЗИ;
- проверку готовности пользователей и администраторов к эксплуатации системы ЗИ АСЗИ;
- оформление акта о завершении опытной эксплуатации системы ЗИ АСЗИ.

6.13.8 На этапе «Проведение приемочных испытаний» проводят:

- испытания системы ЗИ АСЗИ на соответствие ТЗ на систему ЗИ в соответствии с программой и методиками приемочных испытаний АСЗИ;
- анализ результатов испытаний системы ЗИ АСЗИ и устранение недостатков, выявленных при испытаниях;
- оформление разделов акта о приемке АСЗИ в постоянную эксплуатацию (в части системы ЗИ АСЗИ).

6.14 Аттестацию АСЗИ на соответствие требованиям безопасности информации организует заказчик, проводит организация, имеющая лицензию на данный вид деятельности, до ввода АСЗИ в эксплуатацию, с использованием информационных ресурсов, подлежащих защите, и содержит оценку соответствия ее системы ЗИ требованиям безопасности информации в реальных условиях эксплуатации, проводимую в соответствии с требованиями нормативных правовых актов и методических документов уполномоченного федерального органа исполнительной власти, а также национальных стандартов в области защиты информации.

6.15 Сопровождение системы ЗИ в ходе эксплуатации АСЗИ организует заказчик (оператор), проводит разработчик в соответствии с проектными решениями, рабочей документацией на систему ЗИ АСЗИ, организационно-распорядительными документами по ЗИ. Сопровождение системы ЗИ в ходе эксплуатации АСЗИ заключается в выполнении работ относительно системы ЗИ АСЗИ в соответствии с гарантийными обязательствами и по послегарантийному обслуживанию, которые осуществляются на стадии «Сопровождение АС», определенной ГОСТ 34.601.

6.16 На стадии «Сопровождение АС» проводят следующие работы.

6.16.1 На этапе «Выполнение работ в соответствии с гарантийными обязательствами» осуществляют работы по:

- устранению недостатков системы ЗИ, выявленных в процессе эксплуатации АСЗИ, и последующему контролю за стабильностью характеристик системы ЗИ АСЗИ, влияющих на эффективность ЗИ в течение установленных гарантийных сроков;
- внесению изменений в документацию на систему ЗИ и, при необходимости, в документацию на АСЗИ в целом.

6.16.2 На этапе «Послегарантийное обслуживание» осуществляют работы по:

- мониторингу качества функционирования системы ЗИ АСЗИ;
- установлению причин невыполнения требований о ЗИ в процессе функционирования АСЗИ;
- устранению недостатков в системе ЗИ и контролю за стабильностью ее характеристик, влияющих на эффективность ЗИ;
- внесению изменений в документацию на систему ЗИ и, при необходимости, в документацию на АСЗИ в целом.

7 Содержание и порядок выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении

7.1 ЗИ о создаваемой АСЗИ является составной частью работ по их созданию и осуществляется во всех организациях, участвующих в процессе создания (модернизации) этих систем, в случаях установленных федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации, нормативными правовыми актами уполномоченных федеральных органов исполнительной власти или заказчиком.

7.2 Основными видами работ по ЗИ о создаваемых (модернизируемых) АСЗИ являются:

- разработка замысла ЗИ о создаваемой (модернизируемой) АСЗИ;
- определение защищаемой информации о создаваемой (модернизируемой) АСЗИ на различных стадиях ее создания;
- определение носителей защищаемой информации о создаваемой (модернизируемой) АСЗИ и их уязвимостей, актуальных угроз безопасности информации;

- определение и технико-экономическое обоснование организационных и технических мероприятий, которые необходимо проводить в интересах ЗИ о создаваемой (модернизируемой) АСЗИ на различных стадиях ее создания;

- обоснование, разработка и/или закупка средств, необходимых для ЗИ о создаваемой (модернизируемой) АСЗИ;

- обоснование и разработка мероприятий по контролю состояния ЗИ о создаваемой (модернизируемой) АСЗИ на различных стадиях ее создания;

- разработка документов, регламентирующих организацию и осуществление ЗИ о создаваемой (модернизируемой) АСЗИ.

7.3 Перечень информации, подлежащей защите, определяют на стадии формирования требований к АСЗИ и, при необходимости, уточняют на последующих стадиях ее создания.

7.4 К защищаемой информации о создаваемой (модернизируемой) АСЗИ относят:

- цель и задачи ЗИ в АСЗИ;

- перечень составных частей (сегментов) АСЗИ, участвующих в обработке защищаемой в АСЗИ информации;

- состав возможных уязвимостей АСЗИ, возможных последствий от реализации угроз безопасности информации для нарушения свойств безопасности информации (конфиденциальность, целостность, доступность);

- структурно-функциональные характеристики АСЗИ, включающие структуру и состав АСЗИ, физические, функциональные и технологические взаимосвязи между составными частями АСЗИ и взаимосвязи с иными системами, режимы обработки информации в АСЗИ в целом и в ее отдельных составных частях;

- меры и СЗИ, применяемые в АСЗИ;

- сведения о реализации системы ЗИ в АСЗИ.

Применительно к конкретной АСЗИ перечень защищаемой информации устанавливает заказчик.

7.5 Организация и обеспечение ЗИ о создаваемой (модернизируемой) АСЗИ возлагается:

- на стадиях «Формирование требований к АС» и «Разработка концепции АС» — на разработчика, заказчика работ, проводимых в интересах разработки требований и концептуальных положений;

- на стадии «Техническое задание» — на заказчика АСЗИ;

- на стадиях «Эскизный проект», «Технический проект», «Рабочая документация» — на разработчика АСЗИ;

- на стадии «Ввод в действие» – на генерального конструктора или его заместителей, а по частным вопросам — на конструкторов, изготовителей ПС, ТС;

- на стадии «Сопровождение работ» — на оператора АСЗИ.

7.6 При разработке АСЗИ должна быть организована разрешительная система доступа разработчиков, эксплуатирующего персонала, а при необходимости — и сотрудников сторонних организаций (поставщиков ТС, ПС и услуг для гарантийного и послегарантийного обслуживания, контролирующих органов) к защищаемой информации о АСЗИ, документации на АСЗИ, ТС и ПС, а также к информационным ресурсам, содержащим защищаемую информацию.

7.7 Общее руководство работами по ЗИ при создании (модернизации) АСЗИ осуществляет один из заместителей руководителя организации (предприятия), осуществляющей ее разработку (модернизацию), или уполномоченное лицо.

7.8 В процессе создания (модернизации) АСЗИ должен проводиться контроль состояния ЗИ.

7.9 Контроль состояния ЗИ заключается в оценке:

- соблюдения положений нормативных документов, устанавливающих требования безопасности информации при создании (модернизации) АСЗИ;

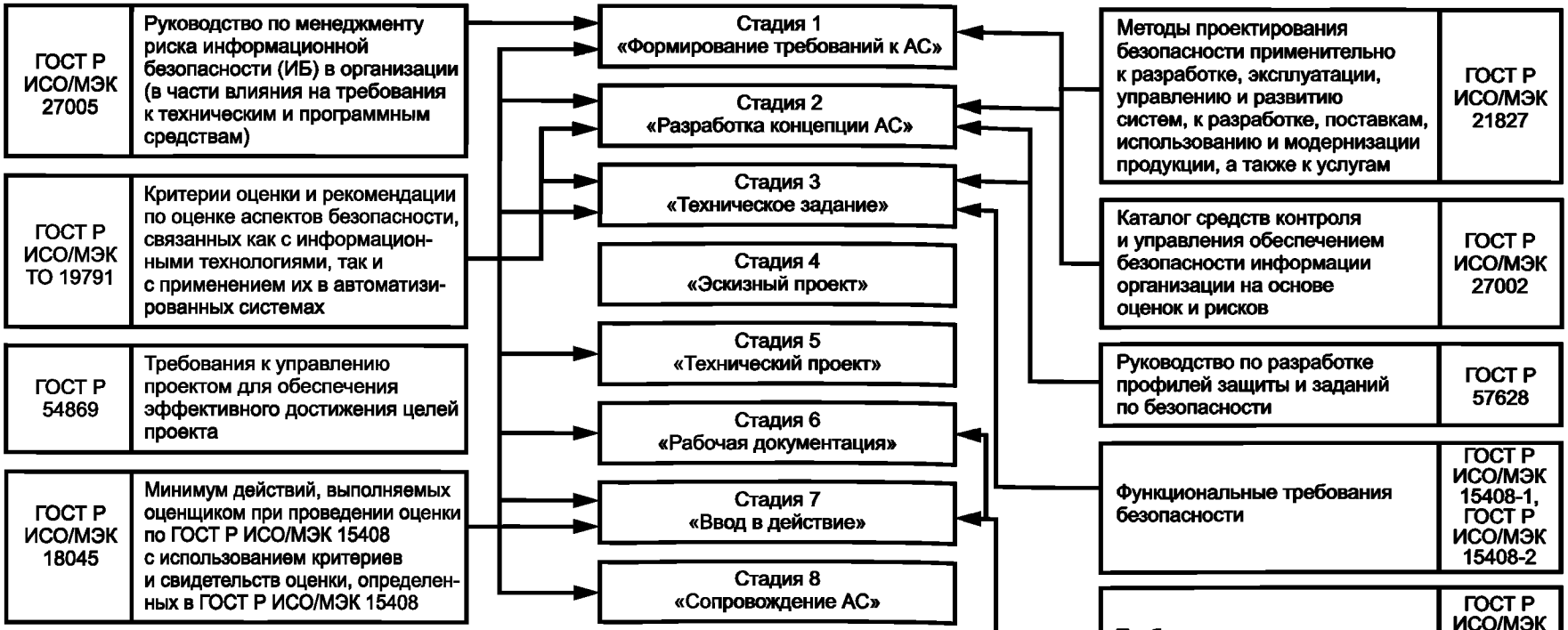
- эффективности ЗИ о создаваемой (модернизируемой) АСЗИ;

- знания исполнителями работ по созданию (модернизации) АСЗИ своих функциональных обязанностей в части ЗИ.

7.10 В зависимости от характера нарушений, выявленных в процессе контроля, обработка информации об АСЗИ может быть приостановлена до устранения причин нарушений.

Приложение А
(справочное)

Примерный перечень и содержание нормативной информации национальных стандартов, рекомендуемых к применению при создании автоматизированных систем в защищенном исполнении



Условное обозначение

Обозначение стандарта	Содержание нормативной информации

Библиография

[1] Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и/или оказанием услуг по защите государственной тайны (утверждено постановлением Правительства Российской Федерации от 15 апреля 1995 г. № 333)

[2] Положение о лицензировании деятельности по технической защите конфиденциальной информации (утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79)

[3] Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации (утверждено постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171)

[4] Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) (утверждено постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313)

[5] РД 50-34.698—90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов

[6] Положение о сертификации средств защиты информации (утверждено постановлением Правительства РФ от 26 июня 1995 г. № 608)

[7] Положение об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, накладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг) (утверждено постановлением Правительства Российской Федерации от 15 мая 2010 г. № 330)

[8] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в редакции Федеральных законов от 27 июня 2010 г. № 227-ФЗ, от 6 апреля 2011 г. № 65-ФЗ, от 21 июля 2011 г. № 252-ФЗ, от 28 июля 2012 г. № 139-ФЗ)

УДК 004.056:004.78:006.354 ОКС 35.020 П80

Ключевые слова: защищаемая информация, автоматизированная система в защищенном исполнении, требования о защите информации, средства защиты информации, система защиты информации

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Ю. Митрофанова*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 05.10.2018. Подписано в печать 12.11.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru