ГОСТ Р 51624-2000 Автоматизированные информационные системы в защищенном исполнении

ОБЩИЕ ПОЛОЖЕНИЯ

Предисловие

1 РАЗРАБОТАН 5 ЦНИИИ МО РФ
ВНЕСЕН Техническим комитетом по стандартизации "Защита информации" (ТК. 362)
2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 30 июня 2000 г. 175-ст
3 В настоящем стандарте реализованы нормы Законов Российской Федерации в информационной сфере и в областях защиты информации
4 ВВЕДЕН ВПЕРВЫЕ

ГОСТ Р 51624-2000
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, правила приемки, методы испытаний, маркировка, упаковка, транспортирование и хранение, гарантия изготовителя ГОСТ 21552-84 Средства вычислительной техники. Общие технические требования, правила приемки, методы испытаний, маркировка, упаковка, транспортирование и хранение ГОСТ БД 21552-84
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 Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования
ГОСТ 29339-92
ГОСТ Р 50543-93 Конструкции базовые несущие средств вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования
ГОСТ Р 50600-93
ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
ГОСТ Р 50752-95
ГОСТ Р 50922-96 Защита информации. Основные термины и определения
ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство
ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующне на информацию. Общие положения
ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

3 Определения и соглашения

3.1 В настоящем стандарте применяют следующие термины с соответствующими определениями:

3.1.1 Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно - розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации (по ГОСТ Р 51583).

3.1.2 Служебная тайна - защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная ин формация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости (по ГОСТ Р 51583).

3.1.3 Секретная информация - информация, содержащая сведения, отнесенные к государственной тайне.

3.1.4 Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (по ГОСТ Р 50922).

3.1.5 Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию (по ГОСТ Р 50922).

3.1.6 Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (по ГОСТ 34.003).

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

3.1.8 Интегрированная автоматизированная система - совокупность двух или более взаимоувязанных АС, в которой функционирование одной из них зависит от результатов функционирования другой (других) так, что эту совокупность можно рассматривать как единую АС (по ГОСТ 34.003).

3.1.9 Система защиты информации автоматизированной системы - совокупность всех технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации (по ГОСТ Р 51583).

3.1.10 Специальная проверка - проверка компонентов автоматизированной системы, осуществляемая с целью поиска и изъятия закладочного устройства (по ГОСТ Р 51583).

3.1.11 Специальные исследования (специсследования) - выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем и оценка соответствия зашиты информации требованиям нормативных документов по защите информации (по ГОСТ Р 51583).

3.1.12 Обработка информации - совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения информации (по ГОСТ Р 51275).

3.1.13 Техническое обеспечение автоматизированной системы - совокупность технических средств, используемых при функционировании АС (по ГОСТ 34.003).

3.1.14 Программное обеспечение автоматизированной системы - совокупность программ на носителях данных и программных документов, предназначенных для отладки, функционирования и проверки работоспособности АС (по ГОСТ 34.003).

3.1.15 Испытания - экспериментальное определение количественных и/или качественных характеристик свойств объекта испытаний как результата воздействия на него при его функционировании, при моделировании объекта и/или воздействий (по ГОСТ 16504).

3.1.16 Фактор, воздействующий на защищаемую информацию, - явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней (по ГОСТ Р 51275).

3.1.17 Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации, и/или несанкционированными и/или непреднамеренными воздействиями на нее.

3.1.18 Побочное электромагнитное излучение - электромагнитное излучение, возникающее при работе технических средств обработки информации (по ГОСТ Р 51275).

3.1.19 Электромагнитные наводки - токи и напряжения в токопроводящих элементах, электрические заряды или магнитные потоки, вызванные электромагнитным полем.

3.1.20 Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации) (по ГОСТ Р 51275).

3.1.21 Программная закладка - внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций программного обеспечения, позволяющих осуществлять несанкционированные воздействия на информацию (по ГОСТ Р 51275).

3.1.22 Вирус - вредоносная программа, способная создавать свои копии или другие вредоносные программы и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия.

3.1.23 Класс защищенности автоматизированной системы - определенная совокупность требований по защите информации, предъявляемых к автоматизированной системе.

3.1.24 Контролируемая зона - пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и/или транспортных средств.

Примечание- Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения); ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

3.2 В настоящем стандарте приняты следующие сокращения:

АС - автоматизированная система;
АСЗИ - автоматизированная система в защищенном исполнении;
ТЗ - техническое задание;
НИР - научно-исследовательская работа;
ОКР - опытно-конструкторская работа;
ЗИ - защита информации;
ПЭМИН - побочные электромагнитные излучения и наводки;
СНиП - санитарные нормы и правила;
ЕСКД - единая система конструкторской документации;
ТС - технические средства;
НСД - несанкционированный доступ;
ПС - программные средства;
НД - нормативный документ;
СрЗИ - средство защиты информации;
ЕСПД - единая система программной документации;
ЕСТД - единая система технологической документации.

4 Общие положения

4.1 Создание (модернизация) и эксплуатация АСЗИ должны осуществляться с учетом требований нормативных документов по защите информации, требований настоящего стандарта, стандартов и/или технического задания на АС в части требований по защите информации.
Порядок использования в АСЗИ шифровальной техники, предназначенной для защиты информации, содержащей сведения, составляющие государственную тайну, определяется в соответствии с требованиями [1].

4.2 АСЗИ могут быть разработаны и поставлены потребителю в виде защищенного изделия. Функционирующие (эксплуатируемые) и модернизируемые АС, предназначенные для обработки защищаемой информации, должны обеспечиваться дополнительной системой защиты информации.

4.3 Требования по защите информации устанавливаются заказчиком как на АСЗИ в целом, так при необходимости и на составные компоненты (части). Требования по защите информации, предъявляемые к компонентам (составным частям) АСЗИ должны быть согласованы с требованиями по защите информации системы в целом.

4.4 Требования по защите информации, предъявляемые к АСЗИ, задаются в ТЗ на создание системы в соответствии с ГОСТ 34.602 в виде отдельного подраздела ТЗ на НИР (ОКР) "Требования по защите информации".
При необходимости в ТЗ на создание АСЗИ или в его составные части заказчик может включать специфические требования по защите информации, дополняющие или уточняющие требования настоящего стандарта.
По результатам технического и эскизного проектирования АСЗИ требования по защите информации, при необходимости, допускается корректировать в порядке, установленном для внесения изменений в утвержденное ТЗ.

4.5 Защита информации в АСЗИ должна быть:

- целенаправленной, осуществляемой в интересах реализации конкретной цели защиты информации в АСЗИ;
- комплексной, осуществляемой в интересах защиты всего многообразия структурных элементов АСЗИ от всего спектра опасных для АСЗИ угроз;
- управляемой, осуществляемой на всех стадиях жизненного цикла АСЗИ, в зависимости от важности обрабатываемой информации, состояния ресурсов АСЗИ, условий эксплуатации АСЗИ результатов отслеживания угроз безопасности информации;
- гарантированной; методы и средства защиты информации должны обеспечивать требуемый уровень защиты информации от ее утечки по техническим каналам, несанкционированного доступа к информации, несанкционированным и непреднамеренным воздействиям на нее, независимо от форм ее представления.

4.6 В АСЗИ должна быть реализована система защиты информации, выполняющая следующие функции:

- предупреждение о появлении угроз безопасности информации;
- обнаружение, нейтрализацию и локализацию воздействия угроз безопасности информации;
- управление доступом к защищаемой информации;
- восстановление системы защиты информации и защищаемой информации после воздействия угроз;
- регистрацию событий и попыток несанкционированного доступа к защищаемой информации и несанкционированного воздействия на нее;
- обеспечение контроля функционирования средств и системы защиты информации и немедленное реагирование на их выход из строя.

Необходимый состав функций, которые должны быть реализованы в АС, устанавливают в соответствии с [2].

4.7 При разработке (модернизации) и эксплуатации АСЗИ должна быть организована решительная система доступа разработчиков, пользователей, эксплуатирующего персонала к техническим и программным средствам, а также информационным ресурсам АСЗИ.
Пользователям предоставляется право работать только с теми средствами и ресурсами, которые необходимы им для выполнения установленных функциональных обязанностей.
Полномочия разработчиков, пользователей и эксплуатирующего персонала по доступу к ресурсам АСЗИ устанавливаются заказчиком системы и отражаются в ТЗ на создание (модернизацию) АСЗИ в разделе "Положения о разрешительной системе допуска исполнителей к документам и сведениям на предприятии" и в инструкции по эксплуатации АСЗИ [2].

4.8 В АСЗИ защите подлежат:

- информационные ресурсы в виде информационных массивов и баз данных, содержащих защищаемую информацию, и представленные на магнитных, оптических и других носителях;
- средства автоматизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных и другие средства.

4.9 Система защиты информации в АСЗИ является неотъемлемой составной частью создаваемой АСЗИ или реализуется в виде дополнительной подсистемы модернизируемой функционирующей автоматизированной системы. Требования к системе защиты информации АСЗИ предъявляют согласно ГОСТ 34.602.

5 Общие требования

5.1 Общие требования к АСЗИ включают:

- функциональные требования;
- требования к эффективности;
- технические требования;
- экономические требования;
- требования к документации.

5.2 Функциональные требования к АСЗИ включают следующие группы требований:

- грифы секретности (конфиденциальности) обрабатываемой в АСЗИ информации;
- категорию (класс защищенности) АСЗИ;
- цели защиты информации;
- перечень защищаемой в АСЗИ информации и требуемые уровни эффективности ее защиты;
- возможные технические каналы утечки информации и способы несанкционированного доступа к информации, несанкционированных и непреднамеренных воздействий на информацию в АСЗИ, класс защищенности АСЗИ;
- задачи защиты информации в АСЗИ.

5.2.1 Определение грифа секретности (конфиденциальности) информации, категории защиты АСЗИ осуществляет заказчик в соответствии с действующими руководящими и нормативными документами в области защиты информации и [2].

5.2.2 Определение класса защищенности АСЗИ осуществляется в соответствии с [3], 14].

5.2.3 Цели защиты информации в АСЗИ

5.2.3.1 Общей целью ЗИ в АСЗИ является предотвращение или снижение величины ущерба, наносимого владельцу и/или пользователю этой системы, вследствие реализации угроз безопасности информации.
Частными целями защиты информации, обеспечивающими достижение общей цели АСЗИ, являются:

- предотвращение утечки информации по техническим каналам;
- предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации;
- соблюдение правового режима использования массивов, программ обработки информации, обеспечения полноты, целостности, достоверности информации в системах обработки;
- сохранение возможности управления процессом обработки и использования информации условиях несанкционированных воздействий на защищаемую информацию.

5.2.3.2 Цели защиты информации в АСЗИ должны включать:

- содержательную формулировку цели защиты;
- показатель эффективности достижения цели и требуемое его значение;
- время актуальности каждой цели защиты информации (этапы жизненного цикла, в течение которых цель должна достигаться).

5.2.4 Перечень защищаемой информации в АСЗИ и требуемые нормы (уровни) эффективности ее защиты

5.2.4.1 Определение конкретного перечня защищаемой информации в АСЗИ должно осуществляться исходя из назначения АСЗИ, целей защиты информации, состава и структуры АСЗИ, а также состава и структуры защиты информации.
Перечень защищаемой информации определяется как для АСЗИ в целом, так и для ее составных частей (компонентов).

5.2.4.2 Требования по эффективности защиты информации в АСЗИ должны включать:

- перечень реализуемых способов защиты информации;
- перечень показателей эффективности защиты информации;
- требуемые уровни эффективности защиты информации.

5.2.5 Выявление возможных технических каналов утечки информации в АСЗИ, способов несанкционированного доступа, несанкционированных и непреднамеренных воздействий на нее должно осуществляться на основе анализа состава, структуры, алгоритмов функционирования АСЗИ, условий размещения АСЗИ с использованием моделей угроз безопасности информации, номенклатуры воздействующих на информацию факторов в соответствии с [5].
Оценка опасности технических каналов утечки информации, возможных способов несанкционированного доступа к информации и несанкционированных воздействий на нее осуществляется по показателям и методикам, определенным в нормативных и методических документах Гостехкомиссии России и других ведомств, уполномоченных Правительством Российской Федерации на проведение соответствующих работ.

5.2.6 Формулировка каждой задачи защиты информации в АСЗИ должна включать:

- наименование конкретной угрозы безопасности для АСЗИ (ее компонента), которую необходимо предотвратить (устранить) при решении задачи;
- формулировку способа решения задачи;
- перечень функций, которые должны быть реализованы для решения данной задачи;
- требования к эффективности или гарантиям решения задачи;
- ограничения на ресурсы АСЗИ, выделяемые на решение данной задачи.

5.2.6.1 Задачи защиты информации в АСЗИ включают:

- предотвращение перехвата защищаемой информации, передаваемой по каналам связи;
- предотвращение утечки обрабатываемой защищаемой информации за счет побочных электромагнитных излучений и наводок;
- исключение несанкционированного доступа к обрабатываемой или хранящейся в АСЗИ защищаемой информации;
- предотвращение несанкционированных и непреднамеренных воздействии, вызывающих разрушение, уничтожение, искажение защищаемой информации или сбои в работе средств АСЗИ;
- выявление возможно внедренных в технические средства АСЗИ специальных электронных устройств перехвата информации;
- организация разрешительной системы допуска пользователей АСЗИ к работе с защищаемой информацией и ее носителями;
- осуществление контроля функционирования средств и систем защиты информации в АСЗИ.

5.3 Требования к эффективности или гарантиям решения задач защиты информации в АСЗИ включают:

- требования по предотвращению утечки защищаемой информации по техническим каналам;
- требования по предотвращению несанкционированного доступа к защищаемой информации;
- требования по предотвращению несанкционированных и непреднамеренных воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств АСЗИ;
- требования по выявлению внедренных в помещения и в технические средства специальных электронных устройств перехвата информации;
- требования по контролю функционирования системы защиты информации АСЗИ.

5.3.1 Требования по предотвращению утечки защищаемой информации по техническим каналам

5.3.1.1 Требования по предотвращению утечки защищаемой информации включают:

- требования по предотвращению утечки защищаемой информации за счет побочных электромагнитных излучений и наводок;
- требования по предотвращению утечки защищаемой информации по техническим каналам разведки;
- требования по предотвращению утечки защищаемой информации за счет сигналов, излучаемых техническими средствами АС, которые обеспечивают функционирование системы;
- требования по предотвращению утечки защищаемой информации за счет несанкционированного доступа к ней.

5.3.1.2 Средства вычислительной техники, входящие в состав АСЗИ и подлежащие защите, должны удовлетворять требованиям по защите информации от утечки за счет побочных электромагнитных излучений и наводок по ГОСТ 29339, ГОСТ Р 50543 и других нормативных документов [61. Номенклатура показателей эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок определяется в соответствии с действующими нормативными документами.

5.3.1.3 Требования по предотвращению утечки защищаемой информации по техническим каналам разведки включают:

- требования по предотвращению утечки защищаемой информации по каналам технической разведки;
- требования по предотвращению утечки защищаемой информации по каналам агентурной разведки, использующей технические средства.

Требования по предотвращению утечки защищаемой информации по каналам технической и агентурной разведки устанавливают в соответствии с [2].

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

5.3.1.5 Требования по предотвращению утечки защищаемой информации за счет встроенных электронных и/или программных закладок в АСЗИ включают требования по выявлению встроенных закладочных устройств и их устранению. Эти требования устанавливают в соответствии с действующими руководящими и нормативными документами [7].

5.3.2 Требования по предотвращению несанкционированного доступа к защищаемой информации устанавливают по ГОСТ Р 50739 и нормативным документам Гостехкомиссии России [3] [5], [8].

5.3.3 Требования по предотвращению несанкционированных и непреднамеренных воздействий, ' вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств АСЗИ информации, устанавливают в соответствии с действующими правовыми, руководящими и нормативными документами в области защиты информации.

Требования по предотвращению изменения информации за счет внешних воздействующих факторов на АСЗИ устанавливают с учетом требований, предъявляемых к компонентам АСЗИ по ГОСТ 16325, ГОСТ 20397, ГОСТ 21552, ГОСТ БД 21552, ГОСТ 27201.
Требования по предотвращению изменения защищаемой информации за счет внешних побочных явлений (электромагнитных полей) устанавливают в соответствии с нормами по электромагнитной совместимости и действующими нормативными документами..
Требования по предотвращению изменения защищаемой информации за счет субъективных преднамеренных действий злоумышленника на АСЗИ, включающих компьютерные вирусы, устанавливаются в соответствии с действующими нормативными документами и достигаются применением специальных программных и аппаратных средств защиты (антивирусные программы) и организации системы контроля безопасности программного обеспечения.

5.4 Технические требования по защите информации включают требования к основным вилам обеспечения АСЗИ (техническому и программному), к зданиям (помещениям) или объектам, в которых АСЗИ устанавливаются, а также к средствам защиты информации и контроля эффективности защиты информации.

5.4.1 Требования по защите информации к техническому обеспечению АСЗИ включают требования как к основным техническим средствам, используемым по функциональному назначению АСЗИ, так и к вспомогательным техническим средствам, обеспечивающим функционирование основных технических средств.

5.4.1.1 Технические требования, предъявляемые к основным техническим средствам, содержат требования по защите информации от утечки по ПЭМИН, от закладочных устройств, от внешних и внутренних воздействующих факторов, от несанкционированного доступа к информации и несанкционированных действий на нее.

5.4.1.2 Конструктивные требования, предъявляемые к техническим средствам АС, должны формироваться с учетом требований по защите информации и включаться в раздел "Конструктивные требования" ТЗ на разработку конкретного технического средства АСЗИ.

5.4.1.3 Технические средства АСЗИ должны обеспечивать сохранность информации при отключении электропитания, при авариях, а также в условиях неблагоприятных природных явления и стихийных бедствий.

5.4.1.4 Методы контроля, испытаний и приемки технических средств АСЗИ должны соответствовать ГОСТ 23773 и ГОСТ Р 50752.

5.4.1.5 Требования к системе заземления и сети электропитания АСЗИ должны устанавливаться в соответствии с (2).

5.4.2 Требования к защите сети телекоммуникаций (сети передачи данных) устанавливают и в соответствии с [2].

5.4.3 Требования по защите информации к программному обеспечению АСЗИ регламентируются в соответствии с ГОСТ Р 51188 и нормативными документами в области защиты информации [2] – [5], [7], [8].

5.4.4 Требования по ЗИ к зданиям (помещениям) или к устройствам, в которых устанавливаются АСЗИ, включают требования к ограждающим конструкциям здания (помещения), к технологии строительства, требования к средствам коммуникаций и требования к звукоизоляции помещений.

5.4.4.1 При необходимости реконструкции и расширения помещений и сооружений объекта, на котором размещается АСЗИ, требования по защите информации предъявляют в соответствии со СНиП и другими действующими руководящими и нормативными документами [9], [10].

5.4.4.2 При размещении основных технических средств АСЗИ в помещениях, предназначенных для ведения конфиденциальных (секретных) переговоров, должны быть приняты меры по защите от утечки речевой информации за счет акустоэлектрических преобразований в элементах основных и вспомогательных технических средств АСЗИ.

5.4.5 Требования, предъявляемые к средствам защиты информации и средствам контроля эффективности защиты информации.

5.4.5.1 Номенклатуру и содержание требований, предъявляемых к средствам зашиты информации и контроля эффективности защиты информации, определяют в соответствии с ГОСТ 2S 1-1",ГОСТ Р 34.10, ГОСТ Р 34.11 и техническими условиями на средства защиты информации и контроля ее эффективности.

5.4.6 Ограничения на аппаратные, программные, информационные, временные и другие ресурсы АСЗИ, выделяемые на решение задач защиты информации, определяют с учетом имеющихся ресурсов АСЗИ исходя из допустимого снижения эффективности, функционирования АСЗИ по основному функциональному назначению.

5.5 Экономические требования по ЗИ включают:

- допустимые затраты на создание АСЗИ и/или системы защиты информации в АСЗИ;
- допустимые затраты на эксплуатацию АСЗИ и/или системы защиты информации в АСЗИ.

5.6 Требования к документации на АСЗИ

5.6.1 Комплектность документации на АСЗИ устанавливается в нормативных документах и по ГОСТ 34.201, [II] и дополнительно включает документы, указанные в таблице 1.

5.6.2 Требования к комплектности конструкторской, технологической ч эксплуатационной документации на средства защиты информации и контроля ее эффективности
На технические средства разрабатывают конструкторскую и эксплуатационную документацию согласно требованиям ЕСКД.

Таблица 1 - Номенклатура дополнительной документации по защите информации на автоматизированную
систему
Наименование документа Код документа по ГОСТ 34.201 Примечание
1 Схема первичного электропитания основных и вспомогательных технических средств АСЗИ С7* С учетом требований по ЗИ
2 Схема заземления основных и вспомогательных технических средств АСЗИ С7** С учетом требований по ЗИ
3 Спецификация основных и вспомогательных технических средств, программных средств АСЗИ -
4 Руководство для абонентов АСЗИ (сети) по режимным вопросам ИЭ4 С учетом требований по ЗИ
5 Перечень контрольных испытаний и проверок (объем и периодичность) по подтверждению защищенности АСЗИ -
6 Предписание на эксплуатацию ТС Д130 С учетом требований по ЗИ
7 Сертификат соответствия (на каждое ТС, ПС системы и СрЗИ) -
8 Акт категорирования средств АСЗИ и системы в целом по вопросам защиты информации -
9 Акт классификации АСЗИ в части защиты от НСД к информации в системе -
10 Аттестат соответствия АСЗИ требованиям НД по защите информации -

11 Формуляр по защите информации (технический паспорт) -
12 Концепции, положения, руководства, наставления, инструкции, уставы, правила, нормы, модели (по ГОСТ Р 50600) -

На программные средства разрабатывают конструкторскую и эксплуатационную документацию в соответствии с ЕСПД.
На программно-технические средства разрабатывают конструкторскую и эксплуатационную документацию согласно требованиям ЕСПД, ЕСКД и ЕСТД.

5.6.3 Требования к составу, видам документов и содержанию организационно-распорядительной документации устанавливают в соответствии с ГОСТ Р 50600 и [21, [12J, [13].

УДК 65.011.56.012.45:006.354 ОКС 35.040, 35.240 Э01 ОКСТУ0090