ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации
ПОРЯДОК СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

ГОСТ 51583-2000

ОБЩИЕ ПОЛОЖЕНИЯ

1 Область применения

Настоящий стандарт распространяется на автоматизированные системы в защищенном исполнении, используемые в различных видах деятельности (исследование, управление, проектирование и т.п.), включая их >/< сочетания, в процессе создания и применения которых осуществляется обработка защищаемой информации, содержащей сведения, отнесенные к государственной или служебной тайне.

Настоящий стандарт устанавливает дополнительные требования и положения стандартов класса 34 "Информационная технология. Комплекс стандартов на автоматизированные системы" в части порядка создания и применения автоматизированных систем в защищенном исполнении.

Настоящий стандарт применяется на территории Российской Федерации органами государственной власти, местного самоуправления, организациями, предприятиями и учреждениями независимо от их организационно-правовой формы и формы собственности, которые заказывают, разрабатывают, изготавливают и используют (эксплуатируют) автоматизированные системы в защищенном исполнении.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты

ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

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

ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадий создания

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

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

ГОСТ 29339-92

ГОСТ Р 50543-93 Конструкции базовые несущие средств вычислительной техника. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования

ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

ГОСТ Р 50752-95

ГОСТ РВ 50797-95

ГОСТ Р 50922-96 Защита информации. Основные термины и определения

ГОСТ Р 50972-96 Защита информации. Радиомикрофоны. Технические требования к защите информации от утечки секретной информации

ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство

ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию

3 Определения и сокращения

3.1 В настоящем стандарте применяют следующие термины с соответствующими определениями

3.1.1 **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.

3.1.2 **Аттестация автоматизированной системы в защищенном исполнении** - процесс комплексной проверки выполнения заданных функций автоматизированной системы по обработке защищаемой информации на соответствие требованиям стандартов и/или нормативных документов в области защиты информации и оформления документов о ее соответствий выполнять функции по обработке защищаемой информации на конкретном объекте информатизации.

3.1.3 **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.

Примечание.

Отнесение информации к государственной тайне осуществляется в соответствии с Законом "О государственной тайне".

3.1.4 **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 информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

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

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

3.1.7 **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).

3.1.8 **Информационная сфера** - сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации [3].

3.1.9 **Информационная технология** - приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных (ГОСТ 34.003).

3.1.10 **Информационный процесс** - процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

3.1.11 **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 (ГОСТ 16504).

3.1.12 **Категорирование защищаемой информации** - установление градаций важности защищаемой информации (ГОСТ Р 50922).

3.1.13 **Мероприятие по защите информации** - совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации {ГОСТ Р 50922).

3.1.14 **Непреднамеренное воздействие на информацию** - ошибка пользователя информацией, сбой технических и программных средств информационных систем, природные явления или иные нецеленаправленные на изменение информации действия, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

3.1.15 **Несанкционированное воздействие на информацию** - воздействие на защищаемую информацию с нарушением установленных прав и/или правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

3.1.16 **Обработка информации** - совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией.

3.1.17 **Секретная информация** - информация, содержащая сведения, отнесенные к государственной тайне.

3.1.18 **Система защиты информации автоматизированной системы** - совокупность технических, программных и программно-технических средств зашиты информации и средств контроля эффективности защиты информации.

3.1.19 **Средство защиты информации** - техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации (ГОСТ Р 50922).

3.1.20 **Средство контроля эффективности защиты информации** - техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации (ГОСТР 50922).

3.1.21 **Приемочный контроль** - контроль продукции, по результатам которого принимается решение о ее пригодности к поставкам и/или использованию (ГОСТ 16504).

3.1.22 **Контроль эффективности защиты информации** - проверка соответствия качественных и количественных показателей эффективности мероприятий по защите информации требованиям или нормам эффективности защиты информации (ГОСТ Р 50922).

3.1.23. **Специальная проверка** - проверка компонентов автоматизированной системы, осуществляемая с целью поиска и изъятия закладочного устройства.

3.1.24 **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 защиты информации требованиям нормативных документов по защите информации.

3.2 В настоящем стандарте приняты следующие сокращения:

АС - автоматизированная система;

АСЗИ - автоматизированная система • защищенном исполнении;

ЗИ - защита информации;

ТЗ - техническое задание;

ЧТЗ - частное техническое задание;

НД - нормативная документация;

ШС - шифровальное средство;

СиЗИ - система защиты информации;

СВТ - средство вычислительной техники;

ТС - технические средства;

ПС - программные средства;

СрЗИ - средство защиты информации;

НИР- научно-исследовательская работа;

ОКР - опытно-конструкторская работа;

ФАПСИ - Федеральное агентство правительственной связи и информации;

НСД • несанкционированный доступ;

ПЭМИН - побочные электромагнитные излучения и наводки.

4 Общие положения по порядку создания автоматизированных систем в защищенном исполнении

4.1 АС представляет организационно-техническую систему, обеспечивающую выработку решений на основе автоматизации информационных процессов в различных сферах деятельности (управление, проектирование, производство и т.д.) или их сочетаниях.

4.2 АС реализует информационную технологию в виде определенной последовательности информационно-связанных функций, задач или процедур, выполняемых в автоматизированном или автоматическом режимах.

4.3 Целесообразность создания и внедрения АС определяется социальным, научно-техническим или другими полезными эффектами, получаемыми в результате автоматизации.

4.4 Процесс создания АСЗИ заключается в выполнении совокупности мероприятий, направленных на разработку и/или практической применение информационной технологии, реализующей функции по ЗИ, установленные в соответствии с требованиями стандартов и/или нормативных документов по ЗИ как во вновь создаваемых, так и в действующих АС.

4.5 Целью создания АСЗИ является исключение или существенное затруднение получения злоумышленником защищаемой информации, обрабатываемой в АС, а также исключение или существенное затруднение несанкционированного и/или непреднамеренного воздействия на защищаемую обрабатываемую информацию и ее носители.

4.6 Защита информации в АСЗИ является составной частью работ по их созданию, эксплуатации и осуществляется во всех органах государственной власти и на предприятиях (организациях), располагающих информацией, содержащей сведения, отнесенные к государственной или служебной тайне [1].

4.7 Разработка и внедрение вновь создаваемой АС производится в соответствии с ТЗ. ТЗ на АС является основным документом, определяющим требования, предъявляемые к АС, порядок создания АС и приемку АС при вводе в действие.

4.8 Для вновь создаваемых АС ТЗ разрабатывают на систему в целом, предназначенную для работы самостоятельно или в составе другой системы. Дополнительно могут быть разработаны ЧТЗ на части АС, на подсистемы АС. Поэтому требования по ЗИ при создании АСЗИ должны включаться разделом в общее ТЗ на АС или могут быть изложены в виде частного ЧТЗ или дополнения к основному ТЗ на АС.

Порядок утверждения и согласования ЧТЗ (дополнения к основному ТЗ на АС) не должен отличаться от установленного порядка утверждения и согласования ТЗ на АС по ГОСТ 34.602.

4.9 Для АСЗИ, создаваемой на базе действующей АС, разрабатывается ТЗ (ЧТЗ) или дополнение к основному ТЗ на АС, в которые включаются требования по ЗИ только в части создаваемой системы (подсистемы) защиты обрабатываемой информации в АС.

Утверждение и согласование ТЗ (ЧТЗ) или дополнения к основному ТЗ на АС производится в порядке, установленном ГОСТ 34.602.

4.10 Реализация мероприятий по защите информации в АСЗИ должна осуществляться непрерывно на всех стадиях и этапах создания АСЗИ во взаимосвязи с мерами по обеспечению установленного режима секретности проводимых работ.

Основные принципы и положения по созданию и функционированию АСЗИ должны соответствовать требованиям ГОСТ 29339, ГОСТ Р 50543, ГОСТ Р 50739, ГОСТ Р 50972. ГОСТ Р 51275, ГОСТ РВ 50797, нормативных документов [2], [9],[13], [14], [15].

Для АСЗИ, предназначенных для обработки информации, составляющей государственную тайну, а также несекретной информации с ограниченным доступом, используемой в управлении экологически опасными объектами, требования вышеперечисленных документов являются обязательными.

В остальных случаях требования вышеперечисленных документов носят рекомендательных характер и конкретные требования по созданию и функционированию АСЗИ в области защиты информации могут устанавливаться в нормативных документах, разрабатываемых собственником информации.

4.11 Типовое содержание работ на всех стадиях и этапах создания АСЗИ должно соответствовать требованиям ГОСТ 34.601, [8] и рекомендациям, приведенным в Приложении А.

4.12 Организации-участники работ по созданию АСЗИ должны иметь лицензии на право проведения работ в области защиты информации. Лицензирование организаций и предприятий осуществляется в установленном порядке.

4.13 Работы по созданию, производству и эксплуатации АСЗИ с использованием шифровальных средств для защиты сведений, отнесенных к государственной тайне, организуются в соответствии с положениями нормативных актов Российской Федерации, определяющих порядок разработки, изготовления и обеспечения эксплуатации шифровальных средств, систем и комплексов вооружения, использующих шифровальные средства.

4.14 Научно-техническое обеспечение создания АСЗИ должно соответствовать современному состоянию развития науки и техники, а технические решения по защите информации должны быть экономически оправданными.

4.15 Для создания АСЗИ могут применяться как серийно выпускаемые, так и вновь разработанные ТС и ПС обработки информации, а также технические, программные, программно-технические, шифровальные СрЗИ и средства для контроля эффективности. Выпускаемые средства должны иметь сертификаты соответствия, полученные в соответствующих системах сертификации по требованиям безопасности информации [4], [5].

Вновь разработанные средства должны быть сертифицированы в установленном порядке до начала опытной эксплуатации АСЗИ.

4.16 Процесс создания и применения АСЗИ должен быть документирован в полном соответствии с требованиями ГОСТ 34.201, в том числе и НД по защите обрабатываемой информации.

4.17 Заказчик, собственник и владелец АСЗИ, а также организации-участники создания АСЗИ несут ответственность за обеспечение зашиты обрабатываемой информации в АСЗИ и выполняемые работы по ЗИ на всех стадиях создания АСЗИ как это предусмотрено в законодательстве Российской Федерации.

4.18 Технические, программные и программно-технические СрЗИ специального применения создаются разработчиком АСЗИ. Конструкторская документация на их изготовление включается в состав документации на АСЗИ отдельными документами или разделами основных документов.

4.19 За обеспечение создания АСЗИ несут ответственность: - заказчик - в части включения в ТЗ (ЧТЗ) на АСЗИ и ее компонентов, а также в техническую, программную, конструкторскую и эксплуатационную документацию обоснованных требований по защите обрабатываемой информации и контроля их выполнения в процессе экспертизы документации, испытаний и приемки как ЛСЗИ в цепом, так и ее компонентов;

- предприятие - разработчик - в части обеспечения соответствия разрабатываемой АСЗИ и СиЗИ требованиям ТЗ(ЧТЗ) по защите обрабатываемой информации, действующим стандартам, нормам и другим НД;

- предприятие - изготовитель - в части осуществления технических мер по обеспечению соответствия изготавливаемых технических средств и программной продукции заданным требованиям по защите обрабатываемой информации, реализованным в конструкторской и программной документации.

4.20 Общее руководство работами по ЗИ при создании ЛСЗИ в целом осуществляет главный конструктор АСЗИ или его заместители, а при создании компонентов АСЗИ - главные конструктора этих компонентов или их заместители.

Методическое руководство работами по ЗИ в АСЗИ в процессе жизненного цикла АСЗИ осуществляют подразделения организаций (штатные специалисты) по ЗИ, участвующие в создании АСЗИ [6], [7].

5. Особенности испытаний и применения автоматизированной системы в защищенном исполнении

5.1 Состав реализуемых стадий и этапов создания для каждой конкретной АСЗИ, а также содержание выполняемых на них работ по защите обрабатываемой информации устанавливают на стадии "Техническое задание" при разработке ТЗ (ЧТЗ) в соответствии с требованиями ГОСТ 34.602.

Номенклатура требований по ЗИ, предъявляемая к АСЗИ, разрабатывается в соответствии с требованиями НД по ЗИ, содержащими требования по проведению сертификации комплектующих изделий, по проведению специальных исследований и специальных проверок средств обработки информации как иностранного так и совместного производства и по проведению аттестации АСЗИ по требованиям безопасности информации.

5.2 Ввод АСЗИ в эксплуатацию осуществляется только после выполнения всех мероприятий по ЗИ и проведения испытаний испытательным центром (лабораторией) на соответствие требованиям НД по защите информации.

5.3 Применение АСЗИ для обработки защищаемой информации разрешается только после ее аттестации на соответствие требованиям безопасности информации.

5.4 Эксплуатация АСЗИ должна осуществляться в полном соответствии с утвержденной организационно - распорядительной и эксплуатационной документацией на АСЗИ, оценка которым должна быть дана при испытаниях АСЗИ на соответствие требованиям НД по защите информации.

5.5 Должностные лица, обслуживающий персонал и пользователи (операторы) АСЗИ несут ответственность за несоблюдение ими установленного порядка работы по ЗИ и применения мер и средств защиты информации.

5.6 При выявлении нарушений требований ЗИ на АСЗИ установленным НД эксплуатация АСЗИ должна быть прекращена.

5.7 Прекращение эксплуатации АСЗИ возможно также по следующим основаниям:

- согласно принятому собственником (владельцем) АСЗИ решению и оформленному в установленном порядке;

- согласно принятому решению органа надзора (контроля) из-за несоответствия требованиям НД по защите информации или по другим причинам, приводящим к утечке ЗИ или другим угрозам защищаемой информации;

- по решению суда.

5.8 Организационно-методическое руководство работами по созданию, изготовлению, обеспечению и эксплуатации средств криптографической ЗИ, сертификации этих средств, а также контроль за состоянием и развитием этого направления работ осуществляют ведомства, уполномоченные Правительством Российской Федерации на проведение соответствующих работ.

5.9 Порядок обеспечения эксплуатации АСЗИ с использованием шифровальной техники для защиты сведений, отнесенных к государственной тайне, регламентируется в [9].

5.10 Ответственность за надлежащее исполнении правил эксплуатации средств криптографической ЗИ (в том числе во время приемочных испытаний) возлагается на руководство организаций, эксплуатирующих данные средства.

5.11. Контроль за выполнением требований инструкций по эксплуатации средств криптографической ЗИ возлагается на специальные подразделения по ЗИ на предприятии (организации) [9].

5.12. Тематические исследования по криптографической ЗИ в составе комплексов технических средств АСЗИ проводятся организациями имеющими лицензию на этот вид работ в соответствии с [9].

5.13. Специальные исследования ТС и средств АСЗИ проводятся организациями (учреждениями), имеющими лицензии Гостехкомиссии России на соответствующий вид деятельности.

5.14. Сертификация средств, комплексов и систем ЗИ осуществляется в соответствии с требованиями [4], [5].

5.15 Аттестацию на соответствие требованиям защиты информации АСЗИ осуществляют в соответствии с требованиями [10].

5.16 Испытания СВТ АСЗИ на соответствие требованиям по защите обрабатываемой информации от утечки за счет побочных электромагнитных излучений и наводок осуществляют по ГОСТ Р 50752.

5.17 Испытания СВТ и АСЗИ на соответствие требованиям ГОСТ Р 50739, [11] по защите от НСД к информации осуществляют по [12].

5.18 Испытания программных средств АСЗИ на наличие компьютерных вирусов осуществляют по ГОСТ Р 51188.