Руководящий документ
Временное положение
по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники

Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Принятые сокращения

АС - автоматизированная система
ВД - временный документ
ЗАС - засекречивающая аппаратура связи
КСЗ - комплекс средств защиты
НСД - несанкционированный доступ
НТД - нормативно-техническая документация
ОС - операционная система
ППП - пакет прикладных программ
ПРД - правила разграничения доступа
РД - руководящий документ
СВТ - средства вычислительной техники
СЗИ - система защиты информации
СЗИ НСД - система защиты информации от несанкционированного доступа
СЗСИ - система защиты секретной информации
СНТП - специальное научно-техническое подразделение
СРД - система разграничения доступа
СУБД - система управления базами данных
ТЗ - техническое задание
ЭВМ - электронно-вычислительная машина
ЭВТ - электронно-вычислительная техника

1. Общие положения

1.1. Настоящее Положение устанавливает единый на территории Российской Федерации порядок исследований и разработок в области:
- защиты информации, обрабатываемой автоматизированными системами различного уровня и назначения, от несанкционированного доступа;
- создания средств вычислительной техники общего и специального назначения, защищенных от утечки, искажения или уничтожения

информации за счет НСД[1] , в том числе программных и технических средств защиты информации от НСД;
- создания программных и технических средств защиты информации от НСД в составе систем защиты секретной информации в создаваемых АС.

1.2. Положение определяет следующие основные вопросы:
- организационную структуру и порядок проведения работ по защите информации от НСД и взаимодействия при этом на государственном уровне;
- систему государственных нормативных актов, стандартов, руководящих документов и требований по этой проблеме;
- порядок разработки и приемки защищенных СВТ, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД;
- порядок приемки указанных средств и систем перед сдачей в эксплуатацию в составе АС, порядок их эксплуатации и контроля за работоспособностью этих средств и систем в процессе эксплуатации.

1.3. Положение разработано в развитие Инструкции № 0126-87 в части требований к программным и техническим средствам и системам защиты информации от НСД и базируется на Концепции защиты СВТ и АС от НСД к информации.

Организационные мероприятия по предупреждению утечки и защите информации, являющиеся составной частью решения проблемы защиты информации от НСД, базируются на требованиях указанной инструкции, дополняют программные и технические средства и системы и в этой части являются предметом рассмотрения настоящего Временного положения.

1.4. Временное положение обязательно для выполнения всеми органами государственного управления, государственными предприятиями, воинскими частями, другими учреждениями, организациями и предприятиями (независимо от форм собственности), обладающими государственными секретами, и предназначено для заказчиков, разработчиков и пользователей защищенных СВТ, автоматизированных систем, функционирующих с использованием информации различной степени секретности.

1.5. Разрабатываемые и эксплуатируемые программные и технические средства и системы защиты информации от НСД должны являться неотъемлемой составной частью защищенных СВТ, автоматизированных систем, обрабатывающих информацию различной степени секретности.

1.6. При разработке средств и систем защиты в АС и СВТ необходимо руководствоваться требованиями следующих руководящих документов:
- концепция защиты средств вычислительной техники и автоматизированных

систем от несанкционированного доступа к информации;
- настоящее Временное положение;
- защита от несанкционированного доступа к информации. Термины и определения;
- средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;
- автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

2. Организационная структура, порядок проведения работ по защите информации от НСД и взаимодействия на государственном уровне

2.1. Заказчиком защищенных СВТ является заказчик соответствующей АС, проектируемой на базе этих СВТ.

Заказчик защищенных СВТ финансирует их разработку или принимает долевое участие в финансировании разработок СВТ общего назначения в части реализации своих требований.

2.2. Заказчиком программных и технических средств защиты информации от НСД может являться государственное учреждение или коллективное предприятие независимо от формы собственности.

2.3. Постановку задач по комплексной[2] защите информации, обрабатываемой автоматизированными системами, а также контроль за состоянием и развитием этого направления работ осуществляет Гостехкомиссия России.

2.4. Разработчиками защищенных СВТ общего и специального назначения, в том числе их общесистемного программного обеспечения, являются государственные предприятия - производители СВТ, а также другие организации, имеющие лицензию на проведение деятельности в области защиты информации.

2.5. Разработчиками программных и технических средств и систем защиты информации от НСД могут быть предприятия, имеющие лицензию на проведение указанной деятельности.

2.6. Проведение научно-исследовательских и опытно-конструкторских работ в области защиты секретной информации от НСД, создание защищенных СВТ общего назначения осуществляется по государственному

заказу по представлению заинтересованных ведомств, согласованному с Гостехкомиссией России.

2.7. Организация и функционирование государственных и отраслевых сертификационных центров определяются Положением об этих центрах. На них возлагается проведение сертификационных испытаний программных и технических средств защиты информации от НСД. Перечень сертификационных центров утверждает Гостехкомиссия России.

3. Система государственных нормативных актов, стандартов, руководящих документов и требований по защите информации от НСД

3.1. Система государственных нормативных актов, стандартов, руководящих документов и требований по защите информации от НСД базируется на законах, определяющих вопросы защиты государственных секретов и информационного компьютерного права.

3.2. Система указанных документов определяет работу в двух направлениях:
- первое - разработка СВТ общего и специального назначения, защищенных от утечки, искажения или уничтожения информации, программных и технических (в том числе криптографических) средств и систем защиты информации от НСД;
- второе - разработка, внедрение и эксплуатация систем защиты АС различного уровня и назначения как на базе защищенных СВТ, в том числе программных и технических средств и систем защиты информации от НСД, прошедших сертификационные испытания, так и на базе средств и систем собственной разработки.

3.3. К системе документации первого направления относятся документы (в том числе, ГОСТы, РД и требования), определяющие:
- различные уровни оснащенности СВТ средствами защиты информации от НСД и способы оценки этих уровней (критерии защищенности);
- порядок разработки защищенных СВТ; взаимодействие, права и обязанности заказчиков и разработчиков на стадиях заказа и разработки защищенных СВТ;
- порядок приемки и сертификации защищенных СВТ; взаимодействие, права и обязанности заказчиков и разработчиков на стадиях приемки и сертификации защищенных СВТ;
- разработку эксплуатационных документов и сертификатов.

3.4. К системе документации второго направления относятся документы (в том числе, ГОСТы, РД и требования), определяющие:
- порядок организации и проведения разработки системы защиты секретной

информации, взаимодействие, права и обязанности заказчика и разработчика АС в целом и СЗСИ в частности;
- порядок разработки и заимствования программных и технических средств и систем защиты информации от НСД в процессе разработки СЗСИ;
- порядок настройки защищенных СВТ, в том числе программных и технических средств и систем защиты информации от НСД на конкретные условия функционирования АС;
- порядок ввода в действие и приемки программных и технических средств и систем защиты информации от НСД в составе принимаемой АС;
- порядок использования защищенных СВТ, в том числе программных и технических средств и систем защиты информации от НСД, прошедших сертификационные испытания, в соответствии с классами и требованиями по защите в конкретных системах;
- порядок эксплуатации указанных средств и систем;
- разработку эксплуатационных документов и сертификатов;
- порядок контроля защищенности АС;
- ответственность должностных лиц и различных категорий исполнителей (пользователей) за выполнение установленного порядка разработки и эксплуатации АС в целом и СЗСИ в частности.

3.5. Состав документации, определяющей работу в этих направлениях, устанавливают Госстандарт Российской Федерации и Гостехкомиссия России.

3.6. Обязательным требованием к ТЗ на разработку СВТ и АС должно быть наличие раздела требований по защите от НСД, а в составе документации, сопровождающей выпуск СВТ и АС, должен обязательно присутствовать документ (сертификат), содержащий результаты анализа их защищенности от НСД.

4. Порядок разработки и изготовления защищенных СВТ, в том числе программных и технических средств и систем защиты информации от НСД

4.1. При разработке и изготовлении защищенных СВТ, в том числе программных и технических средств и систем защиты необходимо руководствоваться существующей системой разработки и постановки продукции на производство, определенной ГОСТ 21552-84 и ВД к нему, ГОСТ 16325-88 и ВД к нему, ГОСТ 15.001-88, ГОСТ 23773-88, ГОСТ 34.201-89, ГОСТ 34.602-89, РД 50-601-10-89, РД 50-601-11-89, РД 50-601-12-89 и другими документами.

4.2. Разработку защищенных СВТ общего назначения, в том числе их общесистемного программного обеспечения, осуществляют предприятия-

производители СВТ по государственному заказу в соответствии с ТЗ, согласованным с Гостехкомиссией России (в случае встроенных криптографических средств и систем с Главным шифрорганом страны и предприятием-разработчиком этих средств и систем).

4.3. Разработку защищенных СВТ специального назначения, в том числе их программного обеспечения (общесистемного и прикладного), осуществляют предприятия-производители СВТ по государственному заказу в соответствии с ТЗ, согласованным с Гостехкомиссией России (в случае встроенных криптографических средств и систем - Главным шифрорганом страны и предприятием-разработчиком этих средств и систем) и утвержденным заказчиком СВТ специального назначения.

4.4. Порядок разработки защищенных программных средств на базе общесистемного программного обеспечения, находящегося в эксплуатации.

4.4.1. Разработка защищенных программных средств на базе общесистемного программного обеспечения (ОС, СУБД, сетевые программные средства), находящегося в эксплуатации или поставляемого вместе с незащищенными СВТ предприятиями-изготовителями этих СВТ или Государственным фондом алгоритмов и программ (ГосФАП), может осуществляться по заказу для государственных нужд в соответствии с ТЗ, согласованным с разработчиком соответствующих общесистемных программных средств, с Гостехкомиссией России в пределах ее компетенции и утвержденным заказчиком этих программных средств.

4.4.2. Предприятие-разработчик общесистемного программного средства обязано в этом случае предоставить предприятию-разработчику защищенного программного средства всю необходимую документацию и оказывать консультации при разработке.

4.4.3. При необходимости, определяемой заказчиком работ, предприятие-разработчик общесистемного программного средства может быть соисполнителем разработки защищенного программного средства.

4.4.4. Разработку защищенных программных средств могут осуществлять также предприятия заинтересованных ведомств по отраслевому заказу. В этом случае ТЗ, отвечающее тем же требованиям, согласовывается головной организацией этой отрасли с Гостехкомиссией России в пределах ее компетенции и утверждается заказчиком защищенных программных средств.

4.5. Порядок разработки защищенных программных средств на базе импортных общесистемных программных прототипов.

4.5.1. Разработку (адаптацию) защищенных программных средств на базе импортных общесистемных программных прототипов осуществляют по государственному или отраслевому заказу предприятия-разработчики соответствующих типов СВТ, специализированные организации и предприятия заинтересованных ведомств по согласованию с приобретающим ведомством и в соответствии с ТЗ, согласованным с Гостехкомиссией России в пределах ее компетенции и утвержденным заказчиком этих защищенных средств в зависимости от уровня заказа.

4.5.2. Предварительным этапом разработки защищенных программных средств на базе импортных общесистемных программных прототипов является снятие защиты от копирования и вскрытия механизма работы прототипа, а также проведение анализа защитных средств прототипа на предмет их соответствия требованиям ТЗ в целях использования задействованных средств защиты, их дополнения и модификации.

Проведение работ предварительного этапа может осуществляться по отдельному ТЗ.

4.6. Порядок разработки программных средств контроля защищенности разработанных защищенных СВТ, программных средств и систем защиты.

4.6.1. Все предприятия, осуществляющие разработку защищенных СВТ, в том числе программных средств и систем защиты, обязаны разрабатывать тестовые программные средства для контроля защищенности в процессе приемки и эксплуатации защищенных СВТ и программных средств.

4.6.2. Для создания программных средств контроля могут привлекаться в качестве соисполнителей специализированные организации, имеющие на то лицензию Гостехкомиссии России, функциональной направленностью которых является "вскрытие" механизмов защиты общесистемных программных средств.

4.6.3. Создание программных средств контроля может осуществляться как по общему с разработкой защищенных средств ТЗ, так и по частному ТЗ, порядок согласования и утверждения которого аналогичен изложенному в п. 4.5.1.

4.7. Порядок разработки технических средств защиты информации от НСД.

4.7.1. Разработка технических средств защиты информации от НСД для использования в государственных структурах может производиться по государственному или отраслевому заказу.

4.7.2. Разработка технических средств защиты информации от НСД производится совместно с программными средствами, обеспечивающими их работоспособность в составе защищенных СВТ.

Кроме того, технические средства могут поддерживать защищенность общесистемных программных средств в целях безопасности информации.

4.7.3. Разработку технических средств защиты информации от НСД осуществляют как предприятия-разработчики защищенных СВТ, так и компетентные предприятия заинтересованных ведомств по ТЗ, порядок согласования и утверждения которого аналогичен изложенному в п.4.5.1.

5. Порядок приемки и сертификации защищенных СВТ общего и специального назначения, в том числе программных и технических средств и систем защиты информации от НСД

5.1. Исследования (проверки, испытания) и приемка защищенных СВТ общего и специального назначения, в том числе программных и технических средств и систем защиты информации от НСД производится установленным порядком в соответствии с ГОСТ В15.307-77, ГОСТ В15.210-78, ГОСТ 23773-88 и НТД по безопасности информации.

5.2. Сертификационные испытания защищенных СВТ общего и специального назначения, в том числе программных и технических средств и систем защиты информации от НСД проводят государственные и отраслевые сертификационные центры.

5.3. Право на проведение сертификационных испытаний защищенных СВТ, в том числе программных и технических средств и систем защиты информации от НСД предоставляется Гостехкомиссией России по согласованию с Госстандартом России и в случае использования криптографических средств и систем защиты с Главным шифрорганом страны, предприятиям-разработчикам защищенных СВТ, специализированным организациям ведомств, разрабатывающих защищенные СВТ, в том числе программные и технические средства и системы защиты информации от НСД.

5.4. В соответствии с Положением о сертификации средств и систем вычислительной техники и связи по требованиям защиты информации (в дальнейшем: Положение о сертификации) по результатам сертификационных испытаний оформляется акт, а разработчику выдается сертификат, заверенный Гостехкомиссией России и дающий право на использование и распространение этих средств как защищенных.

5.5. Средства, получившие сертификат, включаются в номенклатуру защищенных СВТ, в том числе программных и технических средств и систем защиты информации от НСД.

Обработка секретной информации разрешается только с использованием сертифицированных средств и систем защиты.

5.6. Разработанные программные средства после их приемки представляются для регистрации в специализированный фонд Государственного фонда алгоритмов и программ.

6. Порядок разработки, сертификации, внедрения и эксплуатации средств криптографической защиты информации от несанкционированного доступа

6.1. Данный раздел определяет взаимодействие сторон и порядок проведения работ при создании, сертификации и эксплуатации средств криптографической защиты информации (СКЗИ) от несанкционированного доступа на государственных предприятиях, в ведомствах.

Действие данного раздела распространяется на программные, технические и программно-технические средства в составе СВТ и АС, применяемые для криптографической защиты от НСД к информации, обрабатываемой, хранимой, накапливаемой и передаваемой в вычислительных системах, построенных на базе отдельных ЭВМ, комплексов ЭВМ и локальных вычислительных сетей, расположенных в пределах одной контролируемой зоны.

Разрешается применение положений данного раздела также в случае нескольких контролируемых зон при условии, что для связи между ними используются защищенные с помощью аппаратуры ЗАС или СКЗИ каналы, по которым в соответствии с действующими нормативными документами разрешена передача секретной информации соответствующего грифа (см. п.6.15 данного раздела).

6.2. Организационно-методическое руководство работами по созданию и эксплуатации СКЗИ, сертификацию СКЗИ, а также контроль за состоянием и развитием этого направления работ осуществляют Гостехкомиссия России и Главный шифрорган страны при посредстве ряда уполномоченных ими специализированных организаций.

6.3. С помощью СКЗИ может осуществляться защита от несанкционированного доступа к несекретной и служебной информации, а

также к информации, имеющей грифы "Секретно", "Совершенно секретно" и "Особой важности".

6.4. При выполнении разработки СКЗИ (или изделия СВТ, содержащего в своем составе СКЗИ), предназначаемого для защиты секретной информации любых грифов, а также для защиты ценной и особо ценной информации[3], техническое задание на СКЗИ должно быть согласовано с Гостехкомиссией России и Главным шифрорганом страны.

Вместе с техническим заданием должны быть направлены схема конфигурации защищаемых СВТ или АС, описание структуры подлежащих защите информационных объектов (с указанием максимального грифа секретности), а также данные о характеристиках допуска и предполагаемых административных структурах пользователей.

6.5. По результатам рассмотрения исходных данных вышеупомянутые органы представляют разработчику СКЗИ рекомендации по использованию одного из аттестованных алгоритмов шифрования, а также (при необходимости) описание его криптосхемы, криптографические константы, тестовые примеры для проверки правильности реализации алгоритма, рекомендации по построению ключевой системы СКЗИ и ряд других документов.

6.6. На основе полученных документов разработчик реализует СКЗИ в виде программного или технического изделия и с привлечением специализированных организаций готовит необходимые материалы для сертификации СКЗИ в соответствии с Положением о сертификации.

Приемку полученных в результате разработки опытных образцов осуществляет комиссия, создаваемая Заказчиком СКЗИ. В состав комиссии должны быть включены представители Гостехкомиссии России и Главного шифроргана страны.

6.7. Сертификация СКЗИ осуществляется на хозрасчетных началах. Положительная сертификация СКЗИ завершается выдачей сертификационного удостоверения.

6.8. Применение СКЗИ, не прошедших в установленном порядке сертификацию для защиты от НСД к секретной информации любых грифов, а также ценной и особо ценной информации запрещается.

6.9. При внедрении АС, содержащей в своем составе сертифицированное СКЗИ и при условии, что данная АС предназначается для обработки секретной информации с грифом не выше "Совершенно секретно" или для

обработки ценной информации, дополнительного разрешения на эксплуатацию сертифицированного СКЗИ не требуется (кроме случаев, специально оговоренных в сертификационном удостоверении на СКЗИ).

Для АС, предназначенных для обработки информации с грифом "Особой важности" или для обработки особо ценной информации, должно быть получено письменное разрешение Гостехкомиссии России и Главного шифроргана страны на эксплуатацию СКЗИ в составе конкретной АС.

6.10. Эксплуатация СКЗИ, применяемых для защиты секретной или ценной информации, должна осуществляться в соответствии с требованиями разрабатываемых Инструкции по обеспечению безопасности эксплуатации СКЗИ в составе АС и Инструкции о порядке использования действующих сменных ключей.

В организации, осуществляющей эксплуатацию АС, должна быть создана служба (орган) безопасности информации, на которую возлагаются ответственность за реализацию мероприятий, предусмотренных вышеназванными инструкциями.

6.11. Гриф секретности действующих сменных ключей и соответствующих ключевых документов при защите информации от НСД с помощью СКЗИ, должен соответствовать максимальному грифу секретности информации, шифруемой с использованием этих ключей.

Носители с записанной на них ключевой документацией СКЗИ учитываются, хранятся и уничтожаются как обычные документы соответствующего грифа секретности согласно Инструкции по обеспечению режима секретности № 0126-87.

6.12. СКЗИ без введенных криптографических констант и действующих сменных ключей имеют гриф секретности, соответствующий грифу описания криптосхемы. СКЗИ с загруженными криптографическими константами имеет гриф секретности, соответствующий грифу криптографических констант. Гриф секретности СКЗИ с загруженными криптографическими константами и введенными ключами определяется максимальным грифом содержащихся в СКЗИ ключей и криптографических констант.

6.13. Шифртекст, полученный путем зашифрования с помощью СКЗИ открытой секретной информации любых грифов, является несекретным.

Внешние носители данных (магнитные ленты, диски, кассеты, дискеты и т.п.) с зашифрованной информацией могут пересылаться, храниться и

учитываться как несекретные, если они не содержат и ранее не содержали открытой секретной информации.

6.14. Для передачи за пределы контролируемой зоны шифртекста, полученного путем зашифрования с помощью СКЗИ несекретной информации, могут использоваться незащищенные каналы связи.

Если гриф исходной информации (до зашифрования) был "Для служебного пользования", то допускается применение только сертифицированного СКЗИ.

6.15. Для передачи за пределы контролируемой зоны шифртекста, полученного путем зашифрования с помощью СКЗИ информации с грифами "Секретно" и выше, должны использоваться каналы связи, защищенные с помощью связной шифраппаратуры, для которых в соответствии с действующими нормативными документами получено разрешение на передачу секретной информации. Специальное разрешение на эксплуатацию СКЗИ в этом случае не требуется.

Порядок создания шифраппаратуры, т.е. криптографических средств различных видов (технических и программно-технических), предназначенных для защиты информации, передаваемой за пределы контролируемой зоны по незащищенным каналам связи, регламентируется Положением о разработке, изготовлении и обеспечении эксплуатации шифровальной техники, государственных и ведомственных систем связи и управления и комплексов вооружения, использующих шифровальную технику.

6.16. Ответственность за надлежащее исполнение правил эксплуатации СКЗИ (в том числе в период проведения приемочных испытаний), возлагается на руководство предприятий, эксплуатирующих данные СКЗИ.

6.17. Контроль за выполнением требований инструкций по эксплуатации СКЗИ возлагается на службы защиты информации предприятий, эксплуатирующих данные СКЗИ.

7. Порядок организации и проведения разработок системы защиты секретной информации в ведомствах и на отдельных предприятиях

7.1. Для решения научно-технических, методических и принципиальных практических вопросов по проблеме защиты информации от НСД в АС в системе ведомств может проводиться комплекс научно-исследовательских и опытно-конструкторских работ по отраслевым планам.

7.2. В целях организации проблемных исследований, централизации разработок средств и систем защиты информации от НСД, осуществления научно-методического руководства проведением работ по этой проблеме в системе ведомств при головных организациях по АС могут создаваться специализированные отраслевые подразделения, осуществляющие взаимодействие с аналогичными подразделениями других министерств и ведомств.

7.3. Научное руководство работами по защите информации от НСД осуществляет главный конструктор интегрированных АС страны.

7.4. Общее руководство работами по защите информации от НСД, осуществление единой технической политики, организационно-методическое руководство и координацию работ, финансирование НИОКР по отраслевым заказам, взаимодействие с Гостехкомиссией России, другими ведомствами, а также контроль за организацией и проведением работ по защите информации от НСД в центральных аппаратах ведомств осуществляют научно-технические и режимные подразделения или назначаются кураторы этого направления работ.

7.5. На предприятии научно-техническое руководство и непосредственную организацию работ по созданию СЗСИ интегрированной АС осуществляет главный конструктор этой системы, а по типам АС - главные конструкторы этих систем, научные руководители тем, начальники объектов ЭВТ или другие должностные лица, обеспечивающие научно-техническое руководство всей разработкой соответствующей АС.

7.6. При разработке системы защиты в АС следует руководствоваться классификацией автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требованиями по защите информации в автоматизированных системах различных классов.

Система защиты секретной информации реализуется в виде подсистемы АС и включает комплекс организационных, программных, технических (в том числе криптографических) средств, систем и мероприятий по защите информации от НСД. СЗСИ состоит из системной и функциональной частей. Системная часть является общей и применяется при разработке, внедрении и эксплуатации всех или большинства задач АС, функциональная часть обеспечивает защиту информации при решении конкретных задач.

7.7. Разработку СЗСИ АС осуществляют подразделение, разрабатывающее на предприятии АС, группа или отдельные специалисты по разработке средств и мер защиты[4] и (или) специализированные научно-

исследовательские, конструкторские и проектные предприятия (в том числе других министерств и ведомств) по договорам, заключаемым заказчиком АС.

В структуре крупных подразделений с большим объемом работ по режимному обеспечению выделяются также службы безопасности или секретные органы.

7.8. На подразделение разработки средств и мер защиты информации возлагаются разработка и внедрение системного режимного обеспечения (адаптация и настройка программных и технических средств и систем централизованной разработки), а также разработка требований к функциональному режимному обеспечению.

К разработке и внедрению системного режимного обеспечения привлекаются специалисты - разработчики обеспечивающих и функциональных подсистем АС, служб безопасности или секретных органов.

Разработка и внедрение режимного обеспечения АС осуществляется при взаимодействии со специальными научно-техническими подразделениями - службами защиты информации и подразделениями режимно-секретной службы предприятия.

7.9. Методическое руководство и участие в разработке требований по защите информации от НСД, аналитического обоснования необходимости создания режимного обеспечения АС, согласование выбора СВТ (в том числе общесистемного программного обеспечения), программных и технических средств и систем защиты, организацию работ по выявлению возможностей и предупреждению утечки секретной информации при ее автоматизированной обработке осуществляет СНТП предприятия.

В выработке требований по защите информации от НСД СНТП участвует совместно с заказчиком соответствующей АС, отраслевым органом обеспечения безопасности и военным представительством Министерства обороны в части вопросов, относящихся к его компетенции.

7.10. Общее руководство работами по обеспечению режима секретности при разработке АС осуществляет заместитель руководителя предприятия-разработчика по режиму.

Общее руководство работами по обеспечению режима секретности при эксплуатации АС осуществляет заместитель руководителя предприятия (организации), отвечающий за обеспечение режима секретности.

Организацию контроля эффективности средств и мер защиты информации разрабатывает предприятие и осуществляет руководитель, отвечающий на предприятии за организацию работ по защите информации.

7.11. При разработке СЗСИ необходимо максимально использовать имеющиеся или разрабатываемые типовые общесистемные компоненты, заимствуя программные и технические средства и системы защиты информации от НСД централизованной разработки, используя защищенные СВТ.

7.12. В рамках существующих стадий и этапов создания АС (ГОСТ 34.601-90) выполняются необходимые этапы работ по созданию СЗСИ.

7.13. В комплексе работ по созданию АС должны предусматриваться опережающая разработка и внедрение системной части СЗСИ.

7.14. На предпроектной стадии по обследованию объекта автоматизации группой обследования, назначенной приказом заказчика АС:
- устанавливается наличие или отсутствие секретной информации в АС, подлежащей разработке, оценивается ее степень секретности и объемы;
- определяются режим обработки секретной информации, класс АС, комплекс основных технических СВТ, общесистемные программные средства, предполагаемые к использованию в разрабатываемой АС;
- оценивается возможность использования типовых или разрабатываемых централизованно и выпускаемых серийно средств защиты информации;
- определяются степень участия персонала ВЦ, функциональных и производственных служб, научных и вспомогательных работников объекта автоматизации в обработке информации, характер взаимодействия между собой и с подразделениями режимно-секретной службы;
- определяются мероприятия по обеспечению режима секретности на стадии разработки секретных задач.

7.15. На основании результатов предпроектного обследования разрабатываются аналитическое обоснование создания СЗСИ и раздел ТЗ на ее отработку.

7.16. На стадии разработки проектов СЗСИ заказчик контролирует ее разработку.

7.17. На стадиях технического и рабочего проектирования разработчик системной части СЗСИ обязан:
- уточнить состав средств защиты в применяемых версиях ОС и ППП, описать порядок их настройки и эксплуатации, сформулировать требования к разработке функциональных задач и баз данных АС;

- разработать или адаптировать программные и технические средства защиты, разработать организационные мероприятия по системной части СЗСИ;
- разработать организационно-распорядительную и проектную документацию СЗСИ и рабочую документацию по эксплуатации средств и мер защиты;
- осуществлять методическую помощь разработчикам функциональной части СЗСИ.

7.18. На стадиях технического и рабочего проектирования разработчик функциональной части СЗСИ обязан:
- представить разработчику системной части СЗСИ необходимые исходные данные для проектирования;
- при методической помощи разработчиков системной части СЗСИ предусмотреть при решении функциональных задач АС использование средств и мер защиты;
- разработать проектную документацию по режимному обеспечению задачи АС и рабочие инструкции для эксплуатации функциональных задач АС, определяющие порядок работы персонала ВЦ и пользователей при обработке секретной информации с учетом функционирования СЗСИ;
- обосновать количество лиц (и их квалификацию), необходимых для непосредственной эксплуатации (применения) разработанных средств (системы) защиты секретной информации;
- определить порядок и условия использования стандартных штатных средств защиты обрабатываемой информации, включенных разработчиком в ОС, ППП и т.п.;
- выполнить генерацию пакета прикладных программ в комплексе с выбранными стандартными средствами защиты.

7.19. Разработка, внедрение и эксплуатация СЗСИ АС осуществляется в отрасли или на отдельном предприятии в соответствии с требованиями следующей организационно-распорядительной и проектной документацией, учитывающей конкретные условия функционирования АС различного уровня и назначения:
- Положение о порядке организации и проведения в отрасли (на предприятии) работ по защите секретной информации в АС;
- Инструкция по защите секретной информации, обрабатываемой в АС отрасли (на предприятии или в подразделениях предприятия);
- раздел Положения о разрешительной системе допуска исполнителей к документам и сведениям на предприятии, определяющий особенности системы допуска в процессе разработки и функционирования АС;
- приказы, указания, решения:
- о создании соответствующих подразделений разработчиков, о

формировании группы обследования, о создании экспертных комиссий;
- о начале обработки на объекте ЭВТ информации определенной степени секретности;
- о назначении лиц, ответственных за эксплуатацию вычислительной системы, баз данных СЗСИ;
- о назначении уполномоченных службы безопасности и т.д.;
- проектная документация различных стадий создания СЗСИ.

7.20. Разработка, внедрение и эксплуатация СЗСИ в АС производится установленным порядком в соответствии с требованиями ГОСТ 34.201-89, ГОСТ 34.602-89, ГОСТ 34.601-90, РД 50-680-88, РД 50-682-89, РД 50-34.698-90 и других документов.

7.21. Модернизация АС должна рассматриваться как самостоятельная разработка самой АС и СЗСИ для нее. Организация работ при этом должна соответствовать содержанию настоящего раздела.

8. Порядок приемки СЗСИ перед сдачей в эксплуатацию в составе АС

8.1. На стадии ввода в действие КСЗ осуществляются:
- предварительные испытания средств защиты;
- опытная эксплуатация средств защиты и функциональных задач АС в условиях их работы;
- приемочные испытания средств защиты;
- приемочные испытания СЗСИ в составе автоматизированной системы комиссией соответствующего ранга.

8.2. Предварительные испытания средств защиты проводит разработчик этих средств совместно с заказчиком и с привлечением специалистов отраслевых органов безопасности информации в целях проверки отдельных средств по ГОСТ 21552-84, ГОСТ 16325-88 и ГОСТ 23773-88, соответствия технической документации требованиям ТЗ, выработки рекомендаций по их доработке и определения порядка и сроков проведения опытной эксплуатации.

8.3. Допускается проведение опытной эксплуатации средств защиты до эксплуатации функциональных задач АС или параллельно с ней. Опытную эксплуатацию осуществляет заказчик с участием разработчика в соответствии с программой в целях проверки работоспособности средств защиты на реальных данных и отработки технологического процесса. На этапе опытной эксплуатации допускается обработка информации, имеющей гриф "Секретно" и "Совершенно секретно".

Для информации, имеющей гриф "Особой важности", возможность обработки на этапе опытной эксплуатации определяют совместно заказчик, разработчик и отраслевой орган безопасности информации.

Опытная эксплуатация функциональных задач АС должна включать проверку их функционирования в условиях работы средств защиты.

8.4. При положительных результатах опытной эксплуатации все программные, технические средства, организационная документация сдаются заказчику по акту.

Приемка технических средств защиты в эксплуатацию заключается в проверке их характеристик и функционирования в конкретных условиях, а программных средств защиты - в решении контрольного примера (теста), наиболее приближенного к конкретным условиям функционирования АС, с запланированными попытками обхода систем защиты. Контрольный пример готовят разработчики совместно с заказчиком.

8.5. Приемочные испытания СЗСИ проводятся в составе автоматизированной системы, предъявляемой комиссии заказчика.

Ответственность за организацию работ при вводе в действие СЗСИ, за функционирование средств защиты после приемочных испытаний несет заказчик.

8.6. Отчетные материалы по результатам приемочных испытаний СЗСИ оформляются в соответствии с ГОСТ 34.201-89 и РД 50-34.698-90 и направляются в орган по сертификации для оформления сертификата.

Виды документов на программные средства защиты определены ГОСТ 19.101-77, на технические средства - ГОСТ 2.102-68, а на эксплуатационные документы - ГОСТ 2.601-68.

9. Порядок эксплуатации программных и технических средств и систем защиты секретной информации от НСД

9.1. Обработка информации в АС должна производиться в соответствии с технологическим процессом обработки секретной информации, разработанным и утвержденным в порядке, установленном на предприятии для проектирования и эксплуатации АС.

9.2. Для эксплуатации СЗСИ - комплекса программно-технических средств и организационных мероприятий по их сопровождению, направленного на исключение несанкционированного доступа к

обрабатываемой в АС информации, приказом руководителя предприятия (структурного подразделения) назначаются лица, осуществляющие:
- сопровождение СЗСИ, включая вопросы организации работы и контроля за использованием СЗСИ в АС;
- оперативный контроль за функционированием СЗСИ;
- контроль соответствия общесистемной программной среды эталону;
- разработку инструкции, регламентирующей права и обязанности операторов (пользователей) при работе с секретной информацией.

10. Порядок контроля эффективности защиты секретной информации в АС

10.1. Контроль эффективности защиты информации в АС проводится в целях проверки сертификатов на средства защиты и соответствия СЗИ требованиям стандартов и нормативных документов Гостехкомиссии России по защите информации от НСД на следующих уровнях:
- государственном, осуществляемом Инспекцией Гостехкомиссии России по оборонным работам и работам, в которых используются сведения, составляющие государственную тайну;
- отраслевом, осуществляемом ведомственными органами контроля (главными научно-техническими и режимными управлениями, головными организациями по защите информации в АС);
- на уровне предприятия (отдельной организации), осуществляемом военными представительствами Вооруженных Сил (по оборонным работам), специальными научно-техническими подразделениями и режимно-секретными службами (органами, службами безопасности).

10.2. Инициатива проведения проверок принадлежит организациям, чья информация обрабатывается в АС, Гостехкомиссии России и ведомственным (отраслевым) органам контроля.

10.3. Проверка функционирующих средств и систем защиты информации от НСД осуществляется с помощью программных (программно-технических) средств на предмет соответствия требованиям ТЗ с учетом классификации АС и степени секретности обрабатываемой информации.

10.4. По результатам проверки оформляется акт, который доводится до сведения руководителя предприятия, пользователя и других организаций и должностных лиц в соответствии с уровнем контроля.

10.5. В зависимости от характера нарушений, связанных с функционированием средств и систем защиты информации от НСД, действующей АС в соответствии с положением о Гостехкомиссии России

могут быть предъявлены претензии вплоть до приостановки обработки информации, выявления и устранения причин нарушений.

Возобновление работ производится после принятия мер по устранению нарушений и проверки эффективности защиты органами контроля и только с разрешения органа, санкционировавшего проверку.

В случае прекращения работ по результатам проверки Инспекцией Гостехкомиссии России они могут быть возобновлены только с разрешения Гостехкомиссии России, а в отношении должностных лиц, виновных в этих нарушениях, решается вопрос о привлечении их к ответственности в соответствии с требованиями Инструкции № 0126-87 и действующим законодательством.

11. Порядок обучения, переподготовки и повышения квалификации специалистов в области защиты информации от НСД

11.1. Подготовка молодых специалистов и переподготовка кадров в области защиты информации, обрабатываемой в АС, от НСД осуществляется в системе Госкомитета Российской Федерации по делам науки и высшей школы и Вооруженных Сил кафедрами вычислительной техники и автоматизированных систем высших учебных заведений по договорам с министерствами, ведомствами и отдельными предприятиями.

11.2. Подготовка осуществляется по учебным программам, согласованным с Гостехкомиссией России.

11.3. Повышение квалификации специалистов, работающих в этой области, осуществляют межотраслевые и отраслевыми институты повышения квалификации и вышеуказанные кафедры вузов по программам, согласованным с Гостехкомиссией России и отраслевыми органами контроля.

---

[1] В дальнейшем "защищенных СВТ"

[2] Под комплексной защитой информации понимается реализация требований по защите: от НСД к информации, от утечки по техническим каналам, от возможно внедренных специальных электронных устройств и программ-«вирусов».

[3] Ценная информация - это информация, ущерб от нарушения защиты которой (связанный, например, с утечкой промышленных и коммерческих секретов) может превысить 100 тыс. рублей в государственном секторе экономики (но не более 1 млн. рублей); Особо ценная информация - это

информация, ущерб от нарушения защиты которой может превысить 1 млн. рублей в государственном секторе экономики.

[4] В дальнейшем: подразделение разработки средств и мер защиты.