СБОРНИК

РУКОВОДЯЩИХ ДОКУМЕНТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

СОДЕРЖАНИЕ

Руководящий документ.
Защита от несанкционированного доступа к информации.
Термины и определения

Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.

Настоящий руководящий документ устанавливает термины и определения понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

Установленные термины обязательны для применения во всех видах документации.

Для каждого понятия установлен один термин. Применение синонимов термина не допускается.

Для отдельных терминов даны (в скобках) краткие формы, которые разрешается применять в случаях, исключающих возможность их различного толкования.

Для справок приведены иностранные эквиваленты русских терминов на английском языке, а также алфавитные указатели терминов на русском и английском языках.

1. Термины и определения

Термин	Определение
1. Доступ к информации (Доступ) Access to information	Ознакомление с информацией, ее обработка, в частности, копирование модификация или уничтожение информации
2. Правила разграничения доступа (ПРД) Security policy	Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа
3. Санкционированный доступ к информации Authorized access to information	Доступ к информации, не нарушающий правила разграничения доступа
4. Несанкционированный доступ к информации (НСД) Unauthorized access to information	Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных

	систем
5. Защита от несанкционированного доступа (Защита от НСД) Protection from unauthorized access	Предотвращение или существенное затруднение несанкционированного доступа
6. Субъект доступа (Субъект) Access subject	Лицо или процесс, действия которого регламентируются правилами разграничения доступа
7. Объект доступа (Объект) Access object	Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа
8. Матрица доступа Access matrix	Таблица, отображающая правила разграничения доступа
9. Уровень полномочий субъекта доступа Subject privilege	Совокупность прав доступа субъекта доступа
10. Нарушитель правил разграничения доступа (Нарушитель ПРД) Security policy violator	Субъект доступа, осуществляющий несанкционированный доступ к информации
11. Модель нарушителя правил разграничения доступа (Модель нарушителя ПРД) Security policy violator’s model	Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа
12. Комплекс средств защиты (КСЗ) Trusted computing base	Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации
13. Система разграничения доступа (СРД) Security policy realization	Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах
14. Идентификатор доступа Access identifier	Уникальный признак субъекта или объекта доступа

15. Идентификация Identification	Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
16. Пароль Password	Идентификатор субъекта доступа, который является его (субъекта) секретом
17. Аутентификация Authentication	Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности
18. Защищенное средство вычислительной техники (защищенная автоматизированная система) Trusted computer system	Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты
19. Средство защиты от несанкционированного доступа (Средство защиты от НСД) Protection facility	Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа
20. Модель защиты Protection model	Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа
21. Безопасность информации Information security	Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз
22. Целостность информации Information integrity	Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения)
23. Конфиденциальная информация Sensitive information	Информация, требующая защиты
24. Дискреционное управление доступом Discretionary access control	Разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту

25. Мандатное управление доступом Mandatory access control	Разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности
26. Многоуровневая защита Multilevel secure	Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности
27. Концепция диспетчера доступа Reference monitor concept	Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам
28. Диспетчер доступа (ядро защиты) Security kernel	Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа
29. Администратор защиты Security administrator	Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации
30. Метка конфиденциальности (Метка) Sensitivity label	Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте
31. Верификация Verification	Процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие
32. Класс защищенности средств вычислительной техники (автоматизированной системы) Protection class of computer systems	Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации
33. Показатель защищенности средств вычислительной техники (Показатель защищенности) Protection criterion of computer systems	Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники
34. Система защиты сек-	Комплекс организационных мер и программно-

ретной информации (СЗСИ) Secret information security system	технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах
35. Система защиты информации от несанкционированного доступа (СЗИ НСД) System of protection from unauthorized access to information	Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах
36. Средство криптографической защиты информации (СКЗИ) Cryptographic information protection facility	Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности
37. Сертификат защиты (Сертификат) Protection certificate	Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных
38. Сертификация уровня защиты (Сертификация) Protection level certification	Процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите

2. Алфавитный указатель терминов на русском языке

3. Алфавитный указатель терминов на английском языке

Руководящий документ.
Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Принятые сокращения

АС - автоматизированная система
КСЗ - комплекс средств защиты
НСД - несанкционированный доступ
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. Настоящий документ излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа (НСД), являющейся частью общей проблемы безопасности информации.

1.2. Концепция предназначена для заказчиков, разработчиков и пользователей СВТ и АС, которые используются для обработки, хранения и передачи требующей защиты информации.

1.3. Концепция является методологической базой нормативно-технических и методических документов, направленных на решение следующих задач:

выработка требований по защите СВТ и АС от НСД к информации;
создание защищенных от НСД к информации СВТ и АС;
сертификация защищенных СВТ и АС.

1.4. Концепция предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в пробле-

ме защиты информации от НСД: направление, связанное с СВТ, и направление, связанное с АС.

Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации.

Помимо пользовательской информации при создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

В связи с этим, если понятия защищенность (защита) информации от НСД в АС и защищенность (защита) АС от НСД к информации эквивалентны, то в случае СВТ можно говорить лишь о защищенности (защите) СВТ от НСД к информации, для обработки, хранения и передачи которой оно предназначено.

При этом защищенность СВТ есть потенциальная защищенность, т.е. свойство предотвращать или существенно затруднять НСД к информации в дальнейшем при использовании СВТ в АС.

2. Определение НСД

2.1. При анализе общей проблемы безопасности информации выделяются те направления, в которых преднамеренная или непреднамеренная деятельность человека, а также неисправности технических средств, ошибки программного обеспечения или стихийные бедствия могут привести к утечке, модификации или уничтожению информации.

Известны такие направления исследования проблемы безопасности информации, как радиотехническое, побочные электромагнитные излучения и наводки, акустическое, НСД и др.

2.2. НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС.

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

3. Основные принципы защиты от НСД

3.1. Защита СВТ и АС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.

3.2. Защита СВТ обеспечивается комплексом программно-технических средств.

3.3. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

3.4. Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

3.5. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

3.6. Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

3.7. Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

4. Модель нарушителя в АС

4.1. В качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей.

Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

4.2. Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС - запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

4.3. В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты.

5. Основные способы НСД

К основным способам НСД относятся:

непосредственное обращение к объектам доступа;

создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

модификация средств защиты, позволяющая осуществить НСД;

внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

6. Основные направления обеспечения защиты от НСД

6.1. Обеспечение защиты СВТ и АС осуществляется:

системой разграничения доступа (СРД) субъектов к объектам доступа;

обеспечивающими средствами для СРД.

6.2. Основными функциями СРД являются:

реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;

реализация ПРД субъектов и их процессов к устройствам создания твердых копий;

изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;

управление потоками данных в целях предотвращения записи данных на носители несоответствующего грифа;

реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

6.3. Обеспечивающие средства для СРД выполняют следующие функции:

идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;

регистрацию действий субъекта и его процесса;

предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;

реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;

тестирование;

очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;

учет выходных печатных и графических форм и твердых копий в АС;

контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

6.4. Ресурсы, связанные как с СРД, так и с обеспечивающими ее средствами, включаются в объекты доступа.

6.5. Способы реализации СРД зависят от конкретных особенностей СВТ и АС. Возможно применение следующих способов защиты и любых их сочетаний:

распределенная СРД и СРД, локализованная в программно-техническом комплексе (ядро защиты);

СРД в рамках операционной системы, СУБД или прикладных программ;

СРД в средствах реализации сетевых взаимодействий или на уровне приложений;

использование криптографических преобразований или методов непосредственного контроля доступа;

программная и (или) техническая реализация СРД.

7. Основные характеристики технических средств защиты от НСД

7.1. Основными характеристиками технических средств защиты являются:

степень полноты и качество охвата ПРД реализованной СРД;

состав и качество обеспечивающих средств для СРД;

гарантии правильности функционирования СРД и обеспечивающих ее средств.

7.2. Полнота и качество охвата ПРД оценивается по наличию четких непротиворечивых заложенных в СРД правил доступа к объектам доступа и мерам их надежной идентификации. Учитываются также возможности контроля разнообразных дисциплин доступа к данным.

7.3. При оценке состава и качества обеспечивающих средств для СРД учитываются средства идентификации и опознания субъектов и порядок их использования, полнота учета действий субъектов и способы поддержания привязки субъекта к его процессу.

7.4. Гарантии правильности функционирования оцениваются по способам проектирования и реализации СРД и обеспечивающих ее средств (формальная и неформальная верификация) и по составу и качеству препятствующих обходу СРД средств (поддержание целостности СРД и обеспечивающих средств, восстановление после сбоев, отказов и попыток НСД, контроль дистрибуций, возможность тестирования на этапе эксплуатации).

7.5. Оцениваемые АС или СВТ должны быть тщательно документированы. В состав документации включаются Руководство пользователя по использованию защитных механизмов и Руководство по управлению средствами защиты. Для АС и СВТ, претендующих на высокий уровень защищенности, оценка осуществляется при наличии проектной документации (эскизный, технический и рабочий проекты), а также описаний процедур тестирования и их результатов.

8. Классификация АС

8.1. Классификация необходима для более детальной, дифференцированной разработки требований по защите от НСД с учетом специфических особенностей этих систем.

8.2. В основу системы классификации АС должны быть положены следующие характеристики объектов и субъектов защиты, а также способов их взаимодействия:

информационные, определяющие ценность информации, ее объем и степень (гриф) конфиденциальности, а также возможные последствия неправильного функционирования АС из-за искажения (потери) информации;

организационные, определяющие полномочия пользователей;

технологические, определяющие условия обработки информации, например, способ обработки (автономный, мультипрограммный и т.д.), время циркуляции (транзит, хранение и т.д.), вид АС (автономная, сеть, стационарная, подвижная и т.д.).

9. Организация работ по защите от НСД

9.1. Организация работ по защите СВТ и АС от НСД к информации должна быть частью общей организации работ по безопасности информации.

9.2. Обеспечение защиты основывается на требованиях по защите к разрабатываемым СВТ и АС, формулируемых заказчиком и согласуемых с разработчиком.

Эти требования задаются либо в виде желаемого уровня защищенности СВТ или АС, либо в виде определенного, соответствующего этому уровню перечня требований.

Требования по защите обеспечиваются разработчиком в виде комплекса средств защиты. Организационные мероприятия для АС реализуются заказчиком.

Ответственность за разработку КСЗ возлагается на главного конструктора СВТ или АС.

9.3. Проверка выполнения технических требований по защите проводится аналогично с другими техническими требованиями в процессе испытаний (предварительных, государственных и др.).

По результатам успешных испытаний оформляется документ (сертификат), удостоверяющий соответствие СВТ или АС требованиям по защите и дающий право разработчику на использование и (или) распространение их как защищенных.

9.4. Разработка мероприятий по защите должна проводиться одновременно с разработкой СВТ и АС и выполняться за счет финансовых и материально-технических средств (ресурсов), выделенных на разработку СВТ и АС

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации

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

Настоящий руководящий документ устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

Руководящий документ разработан в дополнение ГОСТ 34.003-90, ГОСТ 34.601-90, РД 50-680-88, РД 50-34.680-90 и других документов.

Документ может использоваться как нормативно-методический материал для заказчиков и разработчиков АС при формулировании и реализации требований по защите.

Принятые сокращения

АС - автоматизированные системы

НСД - несанкционированный доступ

РД - руководящий документ

СЗИ - система защиты информации

СЗИ НСД - система защиты информации от несанкционированного доступа

1. Классификация АС

1.1. Классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

1.2. Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

1.3. Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

1.4. Основными этапами классификации АС являются:

разработка и анализ исходных данных;

выявление основных признаков АС, необходимых для классификации;

сравнение выявленных признаков АС с классифицируемыми;

присвоение АС соответствующего класса защиты информации от НСД.

1.5. Необходимыми исходными данными для проведения классификации конкретной АС являются:

перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;

перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;

матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

режим обработки данных в АС.

1.6. Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

1.7. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

наличие в АС информации различного уровня конфиденциальности;

уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

режим обработки данных в АС - коллективный или индивидуальный.

1.8. Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

1.9. Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

2. Требования по защите информации от НСД для АС

2.1. Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприя-

тиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

2.2. В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

управления доступом;

регистрации и учета;

криптографической;

обеспечения целостности.

2.3. В зависимости от класса АС в рамках этих подсистем должны быть реализованы требования в соответствии с пп. 2.4, 2.7 и 2.10. Подробно эти требования сформулированы в пп. 2.5, 2.6, 2.8, 2.9 и 2.11-2.15.

2.4. Требования к АС третьей группы

Обозначения:

" - " - нет требований к данному классу;

" + " - есть требования к данному классу.

Подсистемы и требования	**Классы**	
	3Б	**3А**
1. Подсистема управления доступом		
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:		
в систему	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-
к программам	-	-
к томам, каталогам, файлам, записям, полям записей	-	-
1.2. Управление потоками информации		
2. Подсистема регистрации и учета		
2.1. Регистрация и учет:		
входа (выхода) субъектов доступа в (из) систему(ы) (узел сети)	+	+
выдачи печатных (графических) выходных документов	-	+
запуска (завершения) программ и процессов (заданий, задач)	-	-
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	-
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, програм-	-	-

мам, томам, каталогам, файлам, записям, полям записей		
изменения полномочий субъектов доступа	-	-
создаваемых защищаемых объектов доступа	-	-
2.2. Учет носителей информации	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+
2.4. Сигнализация попыток нарушения защиты	-	-
3. Криптографическая подсистема		
3.1. Шифрование конфиденциальной информации	-	-
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-
4. Подсистема обеспечения целостности		
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+
4.3. Наличие администратора (службы) защиты информации в АС	-	-
4.4. Периодическое тестирование СЗИ НСД	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+
4.6. Использование сертифицированных средств защиты	-	+

2.5. Требования к классу защищенности 3Б:

Подсистема управления доступом:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.

Подсистема регистрации и учета:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

- должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку).

Подсистема обеспечения целостности:

- должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;

целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

2.6. Требования к классу защищенности 3А:

Подсистема управления доступом:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Подсистема регистрации и учета:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

результат попытки входа: успешная или неуспешная (при НСД);

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

дата и время выдачи (обращения к подсистеме вывода);

краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности;

спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

- должно проводиться несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации;

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

Подсистема обеспечения целостности:

- должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;

целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

- должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;

- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

2.7. Требования к АС второй группы

Обозначения:

" - " - нет требований к данному классу;

" + " - есть требования к данному классу.

Подсистемы и требования	Классы	
	2Б	2А
1. Подсистема управления доступом		
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:		
в систему	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	+
к программам	-	+
к томам, каталогам, файлам, записям, полям записей	-	+
1.2. Управление потоками информации	-	+
2. Подсистема регистрации и учета		
2.1. Регистрация и учет:		
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+
выдачи печатных (графических) выходных документов	-	+
запуска (завершения) программ и процессов (заданий, задач)	-	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	+
изменения полномочий субъектов доступа	-	-
создаваемых защищаемых объектов доступа	-	+
2.2. Учет носителей информации	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+
2.4. Сигнализация попыток нарушения защиты	-	-
3. Криптографическая подсистема		
3.1. Шифрование конфиденциальной информации	-	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	+
4. Подсистема обеспечения целостности		
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+
4.2. Физическая охрана средств вычислительной техники и носи-	+	+

телей информации		
4.3. Наличие администратора (службы) защиты информации в АС	-	+
4.4. Периодическое тестирование СЗИ НСД	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+
4.6. Использование сертифицированных средств защиты	-	+

2.8. Требования к классу защищенности 2Б:

Подсистема управления доступом:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Подсистема регистрации и учета:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

результат попытки входа: успешная или неуспешная (при НСД);

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

Подсистема обеспечения целостности:

- должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;

целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;

- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

2.9. Требования к классу защищенности 2А.

Подсистема управления доступом:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по их логическим адресам (номерам);

- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них информации.

Подсистема регистрации и учета:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

результат попытки входа: успешная или неуспешная (при НСД);

идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

дата и время выдачи (обращения к подсистеме вывода);

спецификация устройства выдачи [логическое имя (номер) внешнего устройства], краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

идентификатор субъекта доступа, запросившего документ;

- должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

дата и время запуска;

имя (идентификатор) программы (процесса, задания);

идентификатор субъекта доступа, запросившего программу (процесс, задание);

результат запуска (успешный, неуспешный - несанкционированный);

- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная,

идентификатор субъекта доступа;

спецификация защищаемого файла;

- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;

идентификатор субъекта доступа;

спецификация защищаемого объекта [логическое имя (номер)];

- должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

- должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

Криптографическая подсистема:

- должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должны выполняться автоматическое освобождение и очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

- доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;

- должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.

Подсистема обеспечения целостности:

- должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;

целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

- должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

- должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД;

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;

- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

2.10. Требования к АС первой группы

Обозначения:

" - " - нет требований к данному классу;

" + " - есть требования к данному классу.

Подсистемы и требования	**Классы**				
	1Д	**1Г**	**1В**	**1Б**	**1А**
1. Подсистема управления доступом					
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:					
в систему	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	+	+	+	+
к программам	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей	-	+	+	+	+
1.2. Управление потоками информации	-	-	+	+	+
2. Подсистема регистрации и учета					
2.1. Регистрация и учет:					
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+	+
выдачи печатных (графических) выходных документов	-	+	+	+	+
запуска (завершения) программ и процессов (заданий, задач)	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	+	+	+	+
изменения полномочий субъектов доступа	-	-	+	+	+
создаваемых защищаемых объектов доступа	-	-	+	+	+
2.2. Учет носителей информации	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	-	-	+	+	+
3. Криптографическая подсистема					
3.1. Шифрование конфиденциальной информации	-	-	-	+	+

3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	+
4. Подсистема обеспечения целостности					
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	-	-	+	+	+

2.11. Требования к классу защищенности 1Д:

Подсистема управления доступом:

- должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Подсистема регистрации и учета:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

результат попытки входа: успешная или неуспешная - несанкционированная;

идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнала (учетную карточку);

- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

Подсистема обеспечения целостности:

- должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;

целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

2.12. Требования к классу защищенности 1Г:

Подсистема управления доступом:

- должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;

- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;

- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

Подсистема регистрации и учета:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

результат попытки входа: успешная или неуспешная - несанкционированная;

идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

код или пароль, предъявленный при неуспешной попытке;

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. В параметрах регистрации указываются:

дата и время выдачи (обращения к подсистеме вывода);

спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

идентификатор субъекта доступа, запросившего документ;

- должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

дата и время запуска;

имя (идентификатор) программы (процесса, задания);

идентификатор субъекта доступа, запросившего программу (процесс, задание);

результат запуска (успешный, неуспешный - несанкционированный);

- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;

идентификатор субъекта доступа;

спецификация защищаемого файла;

- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;

идентификатор субъекта доступа;

спецификация защищаемого объекта [логическое имя (номер)];

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов);

Подсистема обеспечения целостности:

- должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;

целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

2.13. Требования к классу защищенности 1В:

Подсистема управления доступом:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и (или) адресам;

- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Подсистема регистрации и учета:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

результат попытки входа: успешная или неуспешная - несанкционированная;

идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

код или пароль, предъявленный при неуспешной попытке;

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

дата и время выдачи (обращение к подсистеме вывода);

спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

идентификатор субъекта доступа, запросившего документ;

объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем), неуспешный;

- должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

дата и время запуска;

имя (идентификатор) программы (процесса, задания);

идентификатор субъекта доступа, запросившего программу (процесс, задание);

результат запуска (успешный, неуспешный - несанкционированный);

- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;

идентификатор субъекта доступа;

спецификация защищаемого файла;

имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;

вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;

идентификатор субъекта доступа;

спецификация защищаемого объекта [логическое имя (номер)];

имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;

вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

- должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

дата и время изменения полномочий;

идентификатор субъекта доступа (администратора), осуществившего изменения;

- должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в журнал (учетную карточку);

- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

- должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;

- должна осуществляться сигнализация попыток нарушения защиты.

Подсистема обеспечения целостности:

- должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;

целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке и (или) хранении защищаемой информации;

- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

- должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

- должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в год;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;

- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

2.14. Требования к классу защищенности 1Б:

Подсистема управления доступом:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной не менее восьми буквенно-цифровых символов;

- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по физическим адресам (номерам);

- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Подсистема регистрации и учета:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

результат попытки входа: успешный или неуспешный - несанкционированный;

идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

код или пароль, предъявленный при неуспешной попытке;

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа - фактически выданного количества листов в графе «Брак»). В параметрах регистрации указываются:

дата и время выдачи (обращения к подсистеме вывода);

спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

идентификатор субъекта доступа, запросившего документ;

объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи успешный (весь объем), неуспешный;

- должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:

дата и время запуска;

имя (идентификатор) программы (процесса, задания);

идентификатор субъекта доступа, запросившего программу (процесс, задание);

результат запуска (успешный, неуспешный - несанкционированный);

- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;

идентификатор субъекта доступа;

спецификация защищаемого файла;

имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;

вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;

идентификатор субъекта доступа;

спецификация защищаемого объекта [логическое имя (номер)];

имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;

вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

- должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

дата и время изменения полномочий;

идентификатор субъекта доступа (администратора), осуществившего изменения;

идентификатор субъекта, у которого проведено изменение полномочий и вид изменения (пароль, код, профиль и т.п.);

спецификация объекта, у которого проведено изменение статуса защиты и вид изменения (код защиты, уровень конфиденциальности);

- должен осуществляться автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки;

- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

- должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;

- должна осуществляться сигнализация попыток нарушения защиты на терминал администратора и нарушителя.

Криптографическая подсистема:

- должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные портативные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться принудительная очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

- доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;

- должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.

Подсистема обеспечения целостности:

- должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

целостность СЗИ НСД проверяется по контрольным суммам всех компонент СЗИ как в процессе загрузки, так и динамически в процессе работы АС;

целостность программной среды обеспечивается качеством приемки программных средств в АС, предназначенных для обработки защищенных файлов;

- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

- должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

- должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также оперативное восстановление функций СЗИ НСД при сбоях;

- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

2.15. Требования к классу защищенности 1А:

Подсистема управления доступом:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролю временного действия длиной не менее восьми буквенно-цифровых символов.

- должна осуществляться аппаратурная идентификация и проверка подлинности терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по уникальным встроенным устройствам;

- должна осуществляться идентификация и проверка подлинности программ, томов, каталогов, файлов, записей, полей записей по именам и контрольным суммам (паролям, ключам);

- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Подсистема регистрации и учета:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

результат попытки входа: успешная или неуспешная - несанкционированная;

идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

код или пароль, предъявленный при неуспешной попытке;

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа - фактически выданного количества листов в графе «Брак»). В параметрах регистрации указываются:

дата и время выдачи (обращения к подсистеме вывода);

спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

идентификатор субъекта доступа, запросившего документ;

объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем), неуспешный;

- должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:

дата и время запуска;

имя (идентификатор) программы (процесса, задания);

идентификатор субъекта доступа, запросившего программу (процесс, задание);

результат запуска (успешный, неуспешный - несанкционированный);

полная спецификация соответствующего файла "образа" программы (процесса, задания) - устройство (том, каталог), имя файла (расширение);

- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;

идентификатор субъекта доступа;

спецификация защищаемого файла;

имя программы (процесса, задания, задачи), осуществляющей доступ к файлу, вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;

идентификатор субъекта доступа;

спецификация защищаемого объекта [логическое имя (номер)];

имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;

вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

- должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

дата и время изменения полномочий и статуса;

идентификатор субъекта доступа (администратора), осуществившего изменения;

идентификатор субъекта доступа, у которого изменены полномочия и вид изменений (пароль, код, профиль и т.п.);

спецификация объекта, у которого изменен статус защиты, и вид изменения (код защиты, уровень конфиденциальности);

- должен осуществляться автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

- должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, в которой содержалась защищаемая информация;

- должна осуществляться надежная сигнализация попыток нарушения защиты на терминал администратора и нарушителя.

Криптографическая подсистема:

- должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на любые съемные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться автоматическая очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

- должны использоваться разные криптографические ключи для шифрования информации, принадлежащей различным субъектам доступа (группам субъектов);

- доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;

- должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные

центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.

Подсистема обеспечения целостности:

- должны быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

целостность СЗИ НСД проверяется по имитовставкам алгоритма ГОСТ 28147-89 или по контрольным суммам другого аттестованного алгоритма всех компонент СЗИ как в процессе загрузки, так и динамически в процессе функционирования АС;

целостность программной среды обеспечивается качеством приемки любых программных средств в АС;

- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

- должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

- должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также автоматическое оперативное восстановление функций СЗИ НСД при сбоях;

- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

2.16. Организационные мероприятия в рамках СЗИ НСД в АС, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесенную к категории секретной, должны отвечать государственным требованиям по обеспечению режима секретности проводимых работ.

2.17. При обработке или хранении в АС информации, не отнесенной к категории секретной, в рамках СЗИ НСД государственным, коллективным, частным и совместным предприятиям, а также частным лицам рекомендуются следующие организационные мероприятия:

выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;

определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;

установление и оформление правил разграничения доступа, т.е. совокупности правил, регламентирующих права доступа субъектов к объектам;

ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;

получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;

обеспечение охраны объекта, на котором расположена защищаемая АС, (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи;

выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;

организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;

разработка СЗИ НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию;

осуществление приемки СЗИ НСД в составе АС.

2.18. При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ:

не ниже 4 класса - для класса защищенности АС 1В;

не ниже 3 класса - для класса защищенности АС 1Б;

не ниже 2 класса - для класса защищенности АС 1А.

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

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

Настоящий Руководящий документ устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Под СВТ понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Принятые сокращения

АС – автоматизированная система
КД – конструкторская документация
КСЗ – комплекс средств защиты
НСД – несанкционированный доступ
ПРД – правила разграничения доступа
СВТ – средства вычислительной техники

1. Общие положения

1.1. Данные показатели содержат требования защищенности СВТ от НСД к информации.

1.2. Показатели защищенности СВТ применяются к общесистемным программным средствам и операционным системам (с учетом архитектуры ЭВМ).

Конкретные перечни показателей определяют классы защищенности СВТ.

Уменьшение или изменение перечня показателей, соответствующего конкретному классу защищенности СВТ, не допускается.

Каждый показатель описывается совокупностью требований.

Дополнительные требования к показателю защищенности СВТ и соответствие этим дополнительным требованиям оговаривается особо.

1.3. Требования к показателям реализуются с помощью программно-технических средств.

Совокупность всех средств защиты составляет комплекс средств защиты.

Документация КСЗ должна быть неотъемлемой частью конструкторской документации на СВТ.

1.4. Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

первая группа содержит только один седьмой класс;

вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

1.5. Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

1.6. Применение в комплекте СВТ средств криптографической защиты информации по ГОСТ 28147-89 может быть использовано для повышения гарантий качества защиты.

2. Требования к показателям защищенности

2.1. Показатели защищенности

2.1.1. Перечень показателей по классам защищенности СВТ приведен в таблице.

Обозначения:

"-" – нет требований к данному классу;

"+" – новые или дополнительные требования,

"=" – требования совпадают с требованиями к СВТ предыдущего класса.

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Маркировка документов	-	-	+	=	=	=
Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=

Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надежное восстановление	-	-	-	+	=	=
Целостность КСЗ	-	+	+	+	=	=
Контроль модификации	-	-	-	-	+	=
Контроль дистрибуции	-	-	-	-	+	=
Гарантии архитектуры	-	-	-	-	-	+
Тестирование	+	+	+	+	+	=
Руководство для пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

2.1.2. Приведенные в данном разделе наборы требований к показателям каждого класса являются минимально необходимыми.

2.1.3. Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность СВТ оказалась ниже уровня требований шестого класса.

2.2. Требования к показателям защищенности шестого класса.

2.2.1. Дискреционный принцип контроля доступа.

КСЗ должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.).

Для каждой пары (субъект – объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).

КСЗ должен содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа.

Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.

Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.).

2.2.2. Идентификация и аутентификация.

КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ. КСЗ должен подвергать проверке подлинность идентификации – осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации. КСЗ должен

препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.

2.2.3. Тестирование.

В СВТ шестого класса должны тестироваться:

реализация дискреционных ПРД (перехват явных и скрытых запросов, правильное распознавание санкционированных и несанкционированных запросов на доступ, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);

успешное осуществление идентификации и аутентификации, а также их средств защиты.

2.2.4. Руководство для пользователя.

Документация на СВТ должна включать в себя краткое руководство для пользователя с описанием способов использования КСЗ и его интерфейса с пользователем.

2.2.5. Руководство по КСЗ.

Данный документ адресован администратору защиты и должен содержать:

описание контролируемых функций;

руководство по генерации КСЗ;

описание старта СВТ и процедур проверки правильности старта.

2.2.6. Тестовая документация.

Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с п. 2.2.3.) и результатов тестирования.

2.2.7. Конструкторская (проектная) документация.

Должна содержать общее описание принципов работы СВТ, общую схему КСЗ, описание интерфейсов КСЗ с пользователем и интерфейсов частей КСЗ между собой, описание механизмов идентификации и аутентификации.

2.3. Требования к показателям пятого класса защищенности.

2.3.1. Дискреционный принцип контроля доступа.

Данные требования включает в себя аналогичные требование шестого класса (п.2.2.1).

Дополнительно должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

2.3.2. Очистка памяти.

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации.

2.3.3. Идентификация и аутентификация.

Данные требования полностью совпадают с аналогичными требованиями шестого класса (п.2.2.2).

2.3.4. Гарантии проектирования.

На начальном этапе проектирования СВТ должна быть построена модель защиты. Модель должна включать в себя ПРД к объектам и непротиворечивые правила изменения ПРД.

2.3.5. Регистрация.

КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

использование идентификационного и аутентификационного механизма;

запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);

создание и уничтожение объекта;

действия по изменению ПРД.

Для каждого из этих событий должна регистрироваться следующая информация:

дата и время;

субъект, осуществляющий регистрируемое действие;

тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);

успешно ли осуществилось событие (обслужен запрос на доступ или нет).

КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией.

2.3.6. Целостность КСЗ.

В СВТ пятого класса защищенности должны быть предусмотрены средства периодического контроля за целостностью программной и информационной части КСЗ.

2.3.7. Тестирование.

В СВТ пятого класса защищенности должны тестироваться:

реализация ПРД (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);

успешное осуществление идентификации и аутентификации, а также их средства защиты;

очистка памяти в соответствии с п. 2.3.2;

регистрация событий в соответствии с п. 2.3.5, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней;

работа механизма, осуществляющего контроль за целостностью КСЗ.

2.3.8. Руководство пользователя.

Данное требование совпадает с аналогичным требованием шестого класса (п. 2.2.4).

2.3.9. Руководство по КСЗ.

Данный документ адресован администратору защиты и должен содержать:

описание контролируемых функций;

руководство по генерации КСЗ;

описания старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации.

2.3.10. Тестовая документация.

Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с требованиями п.2.3.7), и результатов тестирования.

2.3.11. Конструкторская и проектная документация.

Должна содержать:

описание принципов работы СВТ;

общую схему КСЗ;

описание интерфейсов КСЗ с пользователем и интерфейсов модулей КСЗ;

модель защиты;

описание механизмов контроля целостности КСЗ, очистки памяти, идентификации и аутентификации.

2.4. Требования к показателям четвертого класса защищенности.

2.4.1. Дискреционный принцип контроля доступа.

Данные требования включают аналогичные требования пятого класса (п. 2.3.1).

Дополнительно КСЗ должен содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т.е. от доступа, не допустимого с точки зрения заданного ПРД). Под "явными" здесь подразумеваются действия, осуществляемые с использованием системных средств - системных макрокоманд, инструкций языков высокого уровня и т.д., а под "скрытыми" - иные действия, в том числе с использованием собственных программ работы с устройствами.

Дискреционные ПРД для систем данного класса являются дополнением мандатных ПРД.

2.4.2. Мандатный принцип контроля доступа.

Для реализации этого принципа должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.

КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

КСЗ должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:

субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;

субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.

Реализация мандатных ПРД должна предусматривать возможности сопровождения: изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

В СВТ должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.

2.4.3. Очистка памяти.

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен затруднять субъекту доступ к остаточной информации. При перераспределении оперативной памяти КСЗ должен осуществлять ее очистку.

2.4.4. Изоляция модулей.

При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса (одного субъекта), от программных модулей других процессов (других субъектов) - т.е. в оперативной памяти ЭВМ программы разных пользователей должны быть защищены друг от друга.

2.4.5. Маркировка документов.

При выводе защищаемой информации на документ в начале и конце проставляют штамп № 1 и заполняют его реквизиты в соответствии с Инструкцией № 0126-87 (п. 577).

2.4.6. Защита ввода и вывода на отчуждаемый физический носитель информации.

КСЗ должен различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные ("помеченные"). При вводе с "помеченного" устройства (вывода на "помеченное" устройство) КСЗ должен обеспечивать соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с "помеченным" каналом связи.

Изменения в назначении и разметке устройств и каналов должны осуществляться только под контролем КСЗ.

2.4.7. Сопоставление пользователя с устройством.

КСЗ должен обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки).

Идентифицированный КСЗ должен включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству.

2.4.8. Идентификация и аутентификация.

КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ, должен проверять подлинность идентификатора субъекта - осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации и препятствовать входу в СВТ неидентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась.

КСЗ должен обладать способностью надежно связывать полученную идентификацию со всеми действиями данного пользователя.

2.4.9. Гарантии проектирования.

Проектирование КСЗ должно начинаться с построения модели защиты, содержащей:

непротиворечивые ПРД;

непротиворечивые правила изменения ПРД;

правила работы с устройствами ввода и вывода информации и каналами связи.

2.4.10. Регистрация.

Данные требования включают аналогичные требования пятого класса защищенности (п.2.3.5). Дополнительно должна быть предусмотрена регистрация всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.).

2.4.11. Целостность КСЗ.

В СВТ четвертого класса защищенности должен осуществляться периодический контроль за целостностью КСЗ.

Программы КСЗ должны выполняться в отдельной части оперативной памяти.

2.4.12. Тестирование.

В четвертом классе защищенности должны тестироваться:

реализация ПРД (перехват запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов в соответствии с дискреционными и мандатными правилами, верное сопоставление меток субъектов и объектов, запрос меток вновь вводимой информации, средства защиты механизма разграничения доступа, санкционированное изменение ПРД);

невозможность присвоения субъектом себе новых прав;

очистка оперативной и внешней памяти;

работа механизма изоляции процессов в оперативной памяти;

маркировка документов;

защита вода и вывода информации на отчуждаемый физический носитель и сопоставление пользователя с устройством;

идентификация и аутентификация, а также их средства защиты;

запрет на доступ несанкционированного пользователя;

работа механизма, осуществляющего контроль за целостностью СВТ;

регистрация событий, описанных в п. 2.4.10, средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией.

2.4.13. Руководство для пользователя.

Данное требование совпадает с аналогичным требованием шестого (п. 2.2.4) и пятого (п. 2.3.8) классов.

2.4.14. Руководство по КСЗ.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.3.9).

2.4.15. Тестовая документация.

Должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с п. 2.4.12) и результатов тестирования.

2.4.16. Конструкторская (проектная) документация.

Должна содержать:

общее описание принципов работы СВТ;

общую схему КСЗ;

описание внешних интерфейсов КСЗ и интерфейсов модулей КСЗ;

описание модели защиты;

описание диспетчера доступа;

описание механизма контроля целостности КСЗ;

описание механизма очистки памяти;

описание механизма изоляции программ в оперативной памяти;

описание средств защиты ввода и вывода на отчуждаемый физический носитель информации и сопоставления пользователя с устройством;

описание механизма идентификации и аутентификации;

описание средств регистрации.

2.5. Требования к показателям третьего класса защищенности.

2.5.1. Дискреционный принцип контроля доступа.

Данные требования полностью совпадают с требованиями пятого (п. 2.3.1) и четвертого классов (п. 2.4.1).

2.5.2. Мандатный принцип контроля доступа.

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.2).

2.5.3. Очистка памяти.

Для СВТ третьего класса защищенности КСЗ должен осуществлять очистку оперативной и внешней памяти. Очистка должна производиться путем записи маскирующей информации в память при ее освобождении (перераспределении).

2.5.4. Изоляция модулей.

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.4).

2.5.5. Маркировка документов.

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.5).

2.5.6. Защита ввода и вывода на отчуждаемый физический носитель информации.

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.6).

2.5.7. Сопоставление пользователя с устройством.

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.7).

2.5.8. Идентификация и аутентификация.

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.8).

2.5.9. Гарантии проектирования.

На начальном этапе проектирования КСЗ должна строиться модель защиты, задающая принцип разграничения доступа и механизм управления доступом. Эта модель должна содержать:

непротиворечивые правила изменения ПРД;

правила работы с устройствами ввода и вывода;

формальную модель механизма управления доступом.

Должна предлагаться высокоуровневая спецификация части КСЗ, реализующего механизм управления доступом и его интерфейсов. Эта спецификация должна быть верифицирована на соответствие заданных принципов разграничения доступа.

2.5.10. Регистрация.

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.10).

2.5.11. Взаимодействие пользователя с КСЗ.

Для обеспечения возможности изучения, анализа, верификации и модификации КСЗ должен быть хорошо структурирован, его структура должна быть модульной и четко определенной. Интерфейс пользователя и КСЗ должен быть определен (вход в систему, запросы пользователей и КСЗ и т.п.). Должна быть обеспечена надежность такого интерфейса. Каждый интерфейс пользователя и КСЗ должен быть логически изолирован от других таких же интерфейсов.

2.5.12. Надежное восстановление

Процедуры восстановления после сбоев и отказов оборудования должны обеспечивать полное восстановление свойств КСЗ.

2.5.13. Целостность КСЗ.

Необходимо осуществлять периодический контроль за целостностью КСЗ.

Программы должны выполняться в отдельной части оперативной памяти. Это требование должно подвергаться верификации.

2.5.14. Тестирование.

СВТ должны подвергаться такому же тестированию, что и СВТ четвертого класса (п. 2.4.12).

Дополнительно должны тестироваться:

очистка памяти (п. 2.5.3);

работа механизма надежного восстановления.

2.5.15. Руководство для пользователя.

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.13).

2.5.16. Руководство по КСЗ.

Документ адресован администратору защиты и должен содержать:

описание контролируемых функций;

руководство по генерации КСЗ;

описание старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации;

руководство по средствам надежного восстановления.

2.5.17. Тестовая документация

В документации должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (п. 2.5.14), а также результатов тестирования.

2.5.18. Конструкторская (проектная) документация.

Требуется такая же документация, что и для СВТ четвертого класса (п.2.4.16). Дополнительно необходимы:

высокоуровневая спецификация КСЗ и его интерфейсов;

верификация соответствия высокоуровневой спецификации КСЗ модели защиты.

2.6. Требования к показателям второго класса защищенности.

2.6.1. Дискреционный принцип контроля доступа.

Данные требования включают аналогичные требования третьего класса (п.2.5.1).

Дополнительно требуется, чтобы дискреционные правила разграничения доступа были эквивалентны мандатным правилам (т.е. всякий запрос на доступ должен быть одновременно санкционированным или несанкционированным одновременно и по дискреционным правилам, и по мандатным ПРД).

2.6.2. Мандатный принцип контроля доступа.

Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.2).

2.6.3. Очистка памяти.

Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.3).

2.6.4. Изоляция модулей.

При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса (одного субъекта), от программных модулей других процессов (других субъектов) - т.е. в оперативной памяти ЭВМ программы

разных пользователей должны быть изолированы друг от друга. Гарантии изоляции должны быть основаны на архитектуре СВТ.

2.6.5. Маркировка документов.

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п.2.5.5).

2.6.6. Защита ввода и вывода на отчуждаемый физический носитель информации.

Данные требования полностью совпадают с аналогичным требованием третьего класса (п.2.5.6).

2.6.7. Сопоставление пользователя с устройством.

Данные требования полностью совпадают с аналогичным требованием четвертого (п.2.4.7) и третьего (п.2.5.7) классов.

2.6.8. Идентификация и аутентификация.

Требование полностью совпадает с аналогичным требованием четвертого (п.2.4.8) и третьего (п.2.5.8) классов.

2.6.9. Гарантии проектирования.

Данные требования включают аналогичные требования третьего класса (п.2.5.9).

Дополнительно требуется, чтобы высокоуровневые спецификации КСЗ были отображены последовательно в спецификации одного или нескольких нижних уровней, вплоть до реализации высокоуровневой спецификации КСЗ на языке программирования высокого уровня. При этом методами верификации должно осуществляться доказательство соответствия каждого такого отображения спецификациям высокого (верхнего для данного отображения) уровня. Этот процесс может включать в себя как одно отображение (высокоуровневая спецификация - язык программирования), так и последовательность отображений в промежуточные спецификации с понижением уровня, вплоть до языка программирования. В результате верификации соответствия каждого уровня предыдущему должно достигаться соответствие реализации высокоуровневой спецификации КСЗ модели защиты, изображенной на чертеже (см. рис. Схема модели защиты).

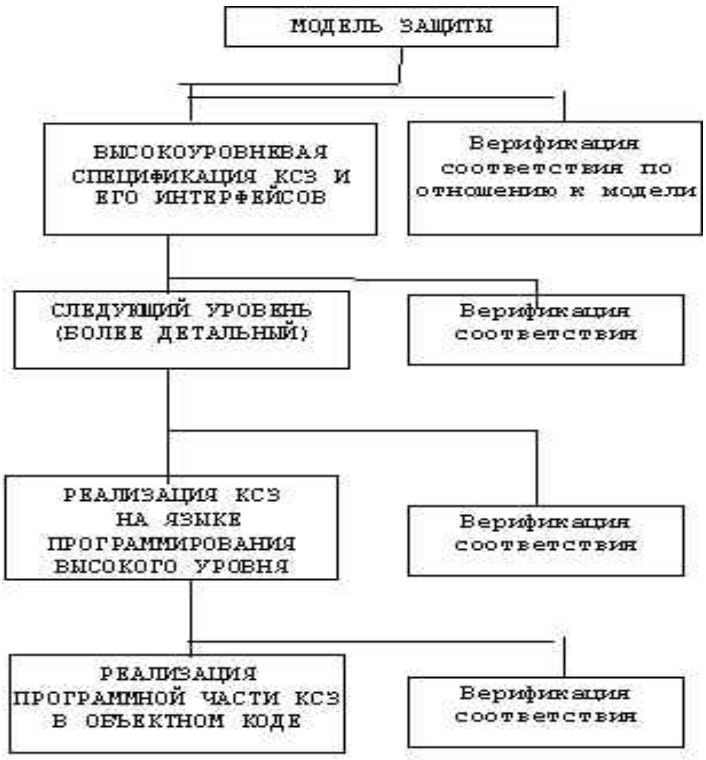

СХЕМА МОДЕЛИ ЗАЩИТЫ (к п.2.6.9)

2.6.10. Регистрация.

Данные требования полностью совпадают с аналогичным требованием четвертого (п.2.4.10) и третьего (п.2.5.10) классов.

2.6.11. Взаимодействие пользователя с КСЗ.

Данные требования полностью совпадают с аналогичным требованием третьего класса (п.2.5.11).

2.6.12. Надежное восстановление.

Данные требования полностью совпадают с аналогичным требованием третьего класса (п.2.5.12).

2.6.13. Целостность КСЗ.

Данные требования полностью совпадают с аналогичным требованием третьего класса (п.2.5.13).

2.6.14. Контроль модификации.

При проектировании, построении и сопровождении СВТ должно быть предусмотрено управление конфигурацией СВТ, т.е. контроль изменений в формальной модели, спецификациях (разных уровней), документации, исходном тексте, версии в объектном коде. Должно обеспечиваться соответствие между документацией и текстами программ. Должна осуществляться сравниваемость генерируемых версий. Оригиналы программ должны быть защищены.

2.6.15. Контроль дистрибуции.

Должен осуществляться контроль точности копирования в СВТ при изготовлении копий с образца. Изготовляемая копия должна гарантированно повторять образец.

2.6.16. Тестирование.

СВТ второго класса должны тестироваться так же, как и СВТ третьего класса (п.2.5.14).

Дополнительно должен тестироваться контроль дистрибуции.

2.6.17. Руководство для пользователя.

Данные требования полностью совпадают с аналогичным требованием четвертого (п.2.4.13) и третьего (п.2.5.15) классов.

2.6.18. Руководство по КСЗ.

Данные требования включают аналогичные требования третьего класса (п. 2.5.16).

Дополнительно должны быть представлены руководства по надежному восстановлению, по работе со средствами контроля модификации и дистрибуции.

2.6.19. Тестовая документация.

Должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (п.2.6.16), а также результатов тестирования.

2.6.20. Конструкторская (проектная) документация.

Требуется такая же документация, что и для СВТ третьего класса (п.2.5.18).

Дополнительно должны быть описаны гарантии процесса проектирования и эквивалентность дискреционных (п.2.6.1) и мандатных (п.2.6.2) ПРД.

2.7. Требования к показателям первого класса защищенности.

2.7.1. Дискреционный принцип контроля доступа.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.1).

2.7.2. Мандатный принцип контроля доступа.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.2).

2.7.3. Очистка памяти.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.3).

2.7.4. Изоляция модулей.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.4).

2.7.5. Маркировка документов.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.5).

2.7.6. Защита ввода и вывода на отчуждаемый физический носитель информации.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.6).

2.7.7. Сопоставление пользователя с устройством.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.7).

2.7.8. Идентификация и аутентификация.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.8).

2.7.9. Гарантии проектирования.

Данные требования включают аналогичные требования второго класса (п.2.6.9).

Дополнительно требуется верификация соответствия объектного кода тексту КСЗ на языке высокого уровня.

2.7.10. Регистрация.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.10).

2.7.11. Взаимодействие пользователя с КСЗ.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.11).

2.7.12. Надежное восстановление.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.12).

2.7.13. Целостность КСЗ.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.13).

2.7.14. Контроль модификации.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.14).

2.7.15. Контроль дистрибуции.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.15).

2.7.16. Гарантии архитектуры.

КСЗ должен обладать механизмом, гарантирующим перехват диспетчером доступа всех обращений субъектов к объектам.

2.7.17. Тестирование.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.16).

2.7.18. Руководство пользователя.

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.17).

2.7.19. Руководство по КСЗ

Данные требования полностью совпадают с аналогичным требованием второго класса (п.2.6.18).

2.7.20. Тестовая документация

Данные требования полностью совпадают с аналогичными требованиями второго класса (п.2.6.19).

2.7.21. Конструкторская (проектная) документация

Требуется такая же документация, что и для СВТ второго класса (п.2.6.20).

Дополнительно разрабатывается описание гарантий процесса проектирования (п.2.7.9).

3. Оценка класса защищенности СВТ (сертификация СВТ)

Оценка класса защищенности СВТ проводится в соответствии с Положением о сертификации средств и систем вычислительной техники и связи по требованиям защиты информации, Временным положением по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники и другими документами.

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.

Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.

Настоящий руководящий документ устанавливает классификацию межсетевых экранов (МЭ) по уровню защищенности от несанкционированного доступа (НСД) к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Под сетями ЭВМ, распределенными автоматизированными системами (АС) в данном документе понимаются соединенные каналами связи системы обработки данных, ориентированные на конкретного пользователя.

МЭ представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Руководящий документ разработан в дополнение к Руководящим документам Гостехкомиссии России “Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации” и “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации”.

Документ предназначен для заказчиков и разработчиков МЭ, а также сетей ЭВМ, распределенных автоматизированных систем с целью использования при формулировании и реализации требований по их защите от НСД к информации.

1. Общие положения

1.1. Данные показатели содержат требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ.

1.2. Показатели защищенности применяются к МЭ для определения уровня защищенности, который они обеспечивают при межсетевом взаимодействии.

Конкретные перечни показателей определяют классы защищенности МЭ.

1.3. Деление МЭ на соответствующие классы по уровням контроля межсетевых информационных потоков с точки зрения защиты информации необходимо в целях разработки и применения обоснованных и экономически оправданных мер по достижению требуемого уровня защиты информации при взаимодействии сетей ЭВМ, АС.

1.4. Дифференциация подхода к выбору функций защиты в МЭ определяется АС, для защиты которой применяется данный экран.

1.5. Устанавливается пять классов защищенности МЭ.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый низкий класс защищенности - пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый - для 1Г, третий - 1В, второй - 1Б, самый высокий - первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой.

1.6. Требования, предъявляемые к МЭ, не исключают требований, предъявляемых к средствам вычислительной техники (СВТ) и АС в соответствии с руководящими документами Гостехкомиссии России “Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации” и “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации”.

При включении МЭ в АС определенного класса защищенности, класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться.

Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса.

Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:

при обработке информации с грифом “секретно” - не ниже 3 класса;

при обработке информации с грифом “совершенно секретно” - не ниже 2 класса;

при обработке информации с грифом “особой важности” - не ниже 1 класса.

2. Требования к межсетевым экранам

Показатели защищенности	**Классы защищенности**				
	5	**4**	**3**	**2**	**1**
Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
Идентификация и аутентификация	-	-	+	=	+
Регистрация	-	+	+	+	=

Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	-	-	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	+
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

2.2. Требования к пятому классу защищенности МЭ.

2.2.1. Управление доступом.

МЭ должен обеспечивать фильтрацию на сетевом уровне.

Решение по фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов.

2.2.2. Администрирование: идентификация и аутентификация.

МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его локальных запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия.

2.2.3. Администрирование: регистрация.

МЭ должен обеспечивать регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова. Регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ;

В параметрах регистрации указываются:

дата, время и код регистрируемого события;

результат попытки осуществления регистрируемого события - успешная или неуспешная;

идентификатор администратора МЭ, предъявленный при попытке осуществления регистрируемого события.

2.2.4. Целостность.

МЭ должен содержать средства контроля за целостностью своей программной и информационной части.

2.2.5. Восстановление.

МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств МЭ.

2.2.6. Тестирование.

В МЭ должна обеспечиваться возможность регламентного тестирования:

реализации правил фильтрации (см. п. 2.2.1);

процесса идентификации и аутентификации администратора МЭ (см. п. 2.2.2);

процесса регистрации действий администратора МЭ (см. п. 2.2.3.);

процесса контроля за целостностью программной и информационной части МЭ (см. п.2.2.4);

процедуры восстановления (см. п. 2.2.5.).

2.2.7. Руководство администратора МЭ.

Документ содержит:

описание контролируемых функций МЭ;

руководство по настройке и конфигурированию МЭ;

описание старта МЭ и процедур проверки правильности старта;

руководство по процедуре восстановления.

2.2.8. Тестовая документация.

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.2.6), и результаты тестирования.

2.2.9. Конструкторская (проектная) документация.

Должна содержать:

общую схему МЭ;

общее описание принципов работы МЭ;

описание правил фильтрации;

описание средств и процесса идентификации и аутентификации;

описание средств и процесса регистрации;

описание средств и процесса контроля за целостностью программной и информационной части МЭ;

описание процедуры восстановления свойств МЭ.

2.3. Требования к четвертому классу защищенности МЭ.

2.3.1. Управление доступом.

Данные требования полностью включают аналогичные требования пятого класса (п.2.2.1).

Дополнительно МЭ должен обеспечивать:[*]

фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

фильтрацию с учетом любых значимых полей сетевых пакетов.

2.3.2. Регистрация.

МЭ должен обеспечивать возможность **регистрации и учета фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации.**

2.3.3. Администрирование: идентификация и аутентификация.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.2).

2.3.4. Администрирование: регистрация.

Данные требования включают аналогичные требования пятого класса (п.2.2.3).

Дополнительно МЭ должен обеспечивать регистрацию запуска программ и процессов (заданий, задач).

2.3.5. Целостность.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.4).

2.3.6. Восстановление.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.5).

2.3.7. Тестирование.

В МЭ должна обеспечиваться возможность регламентного тестирования:

реализации правил фильтрации (см. п. 2.3.1);

процесса регистрации (см. п. 2.3.2);

процесса идентификации и аутентификации администратора МЭ (см. п. 2.3.3);

процесса регистрации действий администратора МЭ (см. п. 2.3.4);

процесса контроля за целостностью программной и информационной части МЭ (см. п.2.3.5);

процедуры восстановления (см. п. 2.3.6).

2.3.8. Руководство администратора МЭ.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.2.7).

2.3.9. Тестовая документация.

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.3.7), и результаты тестирования.

2.3.10. Конструкторская (проектная) документация.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.2.9) по составу документации.

2.4. Требования к третьему классу защищенности МЭ.

2.4.1. Управление доступом.

Данные требования полностью включают аналогичные требования четвертого класса (п. 2.3.1).

Дополнительно МЭ должен обеспечивать:

фильтрацию на транспортном уровне запросов на установление виртуальных соединений. При этом, по крайней мере, учитываются транспортные адреса отправителя и получателя;

фильтрацию на прикладном уровне запросов к прикладным сервисам. При этом, по крайней мере, учитываются прикладные адреса отправителя и получателя;

фильтрацию с учетом даты/времени.

2.4.2. Идентификация и аутентификация.

МЭ должен обеспечивать возможность **аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.**

2.4.3. Регистрация.

Данные требования включают аналогичные требования четвертого класса (п.2.3.2).

Дополнительно МЭ должен обеспечивать:

регистрацию и учет запросов на установление виртуальных соединений;

локальную сигнализацию попыток нарушения правил фильтрации.

2.4.4. Администрирование: идентификация и аутентификация.

Данные требования включают аналогичные требования пятого класса (п.2.2.2).

Дополнительно МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.

При удаленных запросах администратора МЭ на доступ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.

2.4.5. Администрирование: регистрация.

Данные требования полностью включают аналогичные требования четвертого класса (п.2.3.4).

Дополнительно МЭ должен обеспечивать регистрацию действия администратора МЭ по изменению правил фильтрации.

2.4.6. Администрирование: простота использования.

Многокомпонентный МЭ должен обеспечивать возможность дистанционного управления своими компонентами, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.

2.4.7. Целостность.

Данные требования полностью включают аналогичные требования пятого класса (п.2.2.4).

Дополнительно должен обеспечиваться контроль целостности программной и информационной части МЭ по контрольным суммам.

2.4.8. Восстановление.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.5).

2.4.9. Тестирование.

В МЭ должна обеспечиваться возможность регламентного тестирования

реализации правил фильтрации (см. п. 2.4.1);

процесса регистрации (см. п. 2.4.3);

процесса идентификации и аутентификации запросов (см. п. 2.4.2);

процесса идентификации и аутентификации администратора МЭ (см. п. 2.4.4);

процесса регистрации действий администратора МЭ (см. п. 2.4.5);

процесса контроля за целостностью программной и информационной части МЭ (см. п. 2.4.7);

процедуры восстановления (см. п. 2.4.8.).

2.4.10. Руководство администратора МЭ.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.7).

2.4.11. Тестовая документация.

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.4.9), и результаты тестирования.

2.4.12. Конструкторская (проектная) документация.

Данные требования полностью включают аналогичные требования пятого класса (п. 2.2.9) по составу документации.

Дополнительно документация должна содержать описание средств и процесса централизованного управления компонентами МЭ.

2.5. Требования ко второму классу защищенности МЭ.

2.5.1. Управление доступом.

Данные требования включают аналогичные требования третьего класса (п.2.4.1).

Дополнительно МЭ должен обеспечивать:

возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети;

возможность трансляции сетевых адресов.

2.5.2. Идентификация и аутентификация.

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п.2.4.2).

2.5.3. Регистрация.

Данные требования включают аналогичные требования третьего класса (п.2.4.3).

Дополнительно МЭ должен обеспечивать:

дистанционную сигнализацию попыток нарушения правил фильтрации;

регистрацию и учет запрашиваемых сервисов прикладного уровня;

программируемую реакцию на события в МЭ.

2.5.4. Администрирование: идентификация и аутентификация.

МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю временного действия. МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.

При удаленных запросах на доступ администратора МЭ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.

2.5.5. Администрирование: регистрация.

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п.2.4.5).

2.5.6. Администрирование: простота использования.

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п.2.4.6).

2.5.7. Целостность.

МЭ должен содержать средства контроля за целостностью своей программной и информационной части по контрольным суммам **как в процессе загрузки, так и динамически.**

2.5.8. Восстановление.

МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать оперативное восстановление свойств МЭ.

2.5.9. Тестирование.

В МЭ должна обеспечиваться возможность регламентного тестирования

реализации правил фильтрации (см. п. 2.5.1);

процесса идентификации и аутентификации (см. п. 2.5.2);

процесса регистрации (см. п. 2.5.3);

процесса идентификации и аутентификации администратора МЭ (см. п. 2.5.4);

процесса регистрации действий администратора МЭ (см. п. 2.5.5);

процесса контроля за целостностью программной и информационной части МЭ (см. п. 2.5.7);

процедуры восстановления (см. п. 2.5.8).

2.5.10. Руководство администратора МЭ.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.7).

2.5.11. Тестовая документация.

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.5.9), и результаты тестирования.

2.5.12. Конструкторская (проектная) документация.

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п. 2.4.12) по составу документации.

2.6. Требования к первому классу защищенности МЭ.

2.6.1. Управление доступом.

Данные требования полностью совпадают с аналогичными требованиями второго класса (п.2.5.1).

2.6.2. Идентификация и аутентификация.

Данные требования полностью включают аналогичные требования второго класса (п.2.5.2).

Дополнительно МЭ должен обеспечивать идентификацию и аутентификацию всех субъектов прикладного уровня.

2.6.3. Регистрация.

Данные требования полностью совпадают с аналогичными требованиями второго класса (п.2.5.3).

2.6.4. Администрирование: идентификация и аутентификация.

МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации **по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролю временного действия.** МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.

При удаленных запросах на доступ администратора МЭ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.

2.6.5. Администрирование: регистрация.

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п.2.4.5).

2.6.6. Администрирование: простота использования.

Многокомпонентный МЭ должен обеспечивать возможность централизованного управления своими компонентами, в том числе, кон-

фигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.

Должен быть предусмотрен графический интерфейс для управления МЭ.

2.6.7. Целостность.

МЭ должен содержать средства контроля за целостностью своей программной и информационной части по контрольным суммам аттестованного алгоритма как в процессе загрузки, так и динамически.

2.6.8. Восстановление.

Данные требования полностью совпадают с аналогичными требованиями второго класса (п.2.5.8).

2.6.9. Тестирование.

В МЭ должна обеспечиваться возможность регламентного тестирования:

реализации правил фильтрации (см. п. 2.6.1);

процесса идентификации и аутентификации (см. п. 2.6.2);

процесса регистрации (см. п. 2.6.3);

процесса идентификации и аутентификации администратора МЭ (см. п. 2.6.4);

процесса регистрации действий администратора МЭ (см. п. 2.6.5);

процесса централизованного управления компонентами МЭ и графический интерфейс для управления МЭ (см. п. 2.6.6);

процесса контроля за целостностью программной и информационной части МЭ (см. п. 2.6.7);

процедуры восстановления (см. п. 2.6.8).

2.6.10. Руководство администратора МЭ.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.7).

2.6.11. Тестовая документация.

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.6.9), и результаты тестирования.

2.6.12. Конструкторская (проектная) документация.

Данные требования полностью включают аналогичные требования третьего класса (п. 2.4.12) по составу документации.

Дополнительно документация должна содержать описание графического интерфейса для управления МЭ.

3. Термины и определения

Администратор МЭ - лицо, ответственное за сопровождение МЭ.

Дистанционное управление компонентами МЭ - выполнение функций по сопровождению МЭ (компоненты) администратором МЭ с узла (ра-

бочей станции) сети, на котором не функционирует МЭ (компонента) с использованием сетевых протоколов.

Критерии фильтрации - параметры, атрибуты, характеристики, на основе которых осуществляется разрешение или запрещение дальнейшей передачи пакета (данных) в соответствии с заданными правилами разграничения доступа (правилами фильтрации). В качестве таких параметров могут использоваться служебные поля пакетов (данных), содержащие сетевые адреса, идентификаторы, адреса интерфейсов, портов и другие значимые данные, а также внешние характеристики, например, временные, частотные характеристики, объем данных и т.п.

Локальное (местное) управление компонентами МЭ - выполнение функций по сопровождению МЭ (компоненты) администратором МЭ на том же узле (платформе), на котором функционирует МЭ (компонента) с использованием интерфейса МЭ.

Межсетевой экран (МЭ) - это локальное (однокомпонентное) или функционально - распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС. МЭ обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как следствие, субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

Правила фильтрации - перечень условий по которым с использованием заданных критериев фильтрации осуществляется разрешение или запрещение дальнейшей передачи пакетов (данных) и перечень действий, производимых МЭ по регистрации и/или осуществлению дополнительных защитных функций.

Межсетевой экран может строиться с помощью экранирующих агентов, которые обеспечивают установление соединения между субъектом и объектом, а затем пересылают информацию, осуществляя контроль и/или регистрацию. Использование экранирующих агентов позволяет предоставить дополнительную защитную функцию - сокрытие от субъекта истинного объекта. В то же время, субъекту кажется, что он непосредственно взаимодействует с объектом. Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования

формулируется как защита внутренней области от неконтролируемой и потенциально враждебной внешней.

Сетевые адреса - адресные данные, идентифицирующие субъекты и объекты и используемые протоколом сетевого уровня модели международной организации по стандартизации взаимодействия открытых систем (ISO OSI). Сетевой протокол выполняет управление коммуникационными ресурсами, маршрутизацию пакетов, их компоновку для передачи в сети. В этих протоколах решается возможность доступа к подсети, определяется маршрут передачи и осуществляется трансляция сообщения. Управление доступом на сетевом уровне позволяет отклонять нежелательные вызовы и дает возможность различным подсетям управлять использованием ресурсов сетевого уровня. Поэтому, в данных протоколах возможно выполнение требований по защите в части проверки подлинности сетевых ресурсов, источника и приемника данных, принимаемых сообщений, проведения контроля доступа к ресурсам сети.

Трансляция адреса - функция МЭ, скрывающая внутренние адреса объектов (субъектов) от внешних субъектов.

Транспортные адреса - адресные данные, идентифицирующие субъекты и объекты и используемые протоколом транспортного уровня модели ISO OSI. Протоколы транспортного уровня обеспечивают создание и функционирование логических каналов между программами (процессами, пользователями) в различных узлах сети, управляют потоками информации между портами, осуществляют компоновку пакетов о запросах и ответах.

Централизованное управление компонентами МЭ - выполнение с одного рабочего места (рабочей станции, узла) всех функций по сопровождению МЭ (его компонент), только со стороны санкционированного администратора, включая инициализацию, останов, восстановление, тестирование, установку и модификацию правил фильтрации данных, параметров регистрации, дополнительных защитных функций и анализ зарегистрированных событий.

Экранирование - функция МЭ, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области. В результате экранирования уменьшается уязвимость внутренних объектов, поскольку первоначально сторонний нарушитель должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно и жестко. Кроме того, экранирующая система, в отличие от универсальной, может и должна быть устроена более простым и, следовательно, более безопасным образом, на ней должны присутствовать только те компоненты, которые необходимы для выполнения функций экранирования. Экранирование дает также возможность контролировать информационные потоки, направленные во внешнюю область, что способст-

вует поддержанию во внутренней области режима конфиденциальности. Помимо функций разграничения доступа, экраны осуществляют регистрацию информационных обменов.

---

* В дальнейшем дополнительные требования выделяются жирным шрифтом.

Руководящий документ.
Защита информации.
Специальные защитные знаки.
Классификация и общие требования.

Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.

1. Общие положения

1.1. Настоящий руководящий документ устанавливает классификацию по классам защиты специальных защитных знаков, предназначенных для контроля доступа к объектам защиты, а также для защиты документов от подделки.

1.2. Основными объектами защиты, для которых могут применяться специальные защитные знаки, являются:

документированная информация на материальном носителе;

специальные почтовые отправления;

специальные изделия, технические средства и приборы (в том числе регулируемые и критичные к установке), товары народного потребления, подлежащие опечатыванию и контролю;

продукция специального назначения, контейнеры, вагоны, емкости при их перевозке и хранении;

помещения, сейфы, запасные выходы, аварийные устройства.

1.3. Документами, защищаемыми с помощью специальных защитных знаков, являются документы, удостоверяющие личность, пропуска сотрудников организаций и учреждений, лицензии, патенты, кредитные карточки, ценные бумаги и т.п.

1.4. Специальные защитные знаки реализуются в виде рисунка, метки, материала, вещества, обложки, ламината, самоклеящейся ленты, отдельных наклеек, самоклеющихся пломб или другого продукта, созданного на основе физико-химических технологий для контроля доступа к объектам защиты, а также для защиты документов от подделки.

1.5. Настоящий документ определяет требования к специальным защитным знакам при их сертификации в Системе сертификации средств защиты информации по требованиям безопасности информации (РООС RU 0001.01БИ00).

1.6. Настоящий документ является руководящим документом для заказчиков специальных защитных знаков и испытательных лабораторий, проводящих сертификационные испытания в Системе сертификации средств защиты информации по требованиям безопасности информации.

2. Термины и определения

Специальный защитный знак (СЗЗ) - сертифицированное и зарегистрированное в установленном порядке изделие, предназначенное для контроля несанкционированного доступа к объектам защиты путем определения подлинности и целостности СЗЗ путем сравнения самого знака или композиции «СЗЗ - подложка» по критериям соответствия характерным признакам визуальными, инструментальными и другими методами.

Несанкционированный доступ (НСД) - нарушение регламентированного доступа к объекту защиты.

Способ изготовления СЗЗ - технологические процессы (приемы и операции, характеризуемые, главным образом, технологическими признаками - последовательностью действий и приемов, их характером, применяемыми режимами, параметрами, инструментами и др.) и материалы (составы и композиции, пасты, пластмассы, лаки, краски и т.д., в том числе полученные химическим путем), используемые для изготовления и производства СЗЗ.

НОУ-ХАУ технология - совокупность различных технических, коммерческих и других сведений, оформленных в виде технической документации, а также навыков и производственного опыта, необходимых для освоения технологий и методов создания СЗЗ, применяемых в деятельности предприятия или в профессиональной деятельности, доступных определенному кругу лиц. Распространение сведений о НОУ-ХАУ технологиях производства СЗЗ должно быть ограничено соблюдением соответствующих режимных мер.

Идентификация СЗЗ - определение подлинности и целостности СЗЗ по его характерным признакам, а также отсутствия изменений в расположении СЗЗ на объекте защиты или документе путем визуального осмотра или с помощью технических средств общего применения, специализированных технических средств с использованием или без использования специальных методик.

Стойкость защитных свойств СЗЗ - способность к образованию комплекса устойчивых признаков, сигнализирующих о фактах воздействия на СЗЗ или попытке доступа к объекту защиты, а также способность сохранять весь комплекс характерных признаков подлинности и целостности СЗЗ при его регламентированном использовании.

Подлинность СЗЗ - соответствие внешнего вида и наличие в СЗЗ совокупности характерных признаков, предусмотренных техническими условиями.

Целостность СЗЗ - неизменность внешнего вида СЗЗ и совокупности характерных признаков, предусмотренных техническими условиями.

3. Классификация специальных защитных знаков и общие требования

3.1. Все СЗЗ делятся на 18 классов. Классификация СЗЗ осуществляется на основе оценки их основных параметров: возможности подделки, идентифицируемости и стойкости защитных свойств.

Характеристики	Класс СЗЗ защищенности		
	Возможность подделки	Идентифицируемость	Стойкость защитных свойств
1	A1	B1	C1
2	A1	B2	C1
3	A1	B3	C1
4	A1	B1	C2
5	A1	B2	C2
6	A1	B3	C2
7	A2	B1	C1
8	A2	B2	C1
9	A2	B3	C1
10	A2	B1	C2
11	A2	B2	C2
12	A2	B3	C2
13	A3	B1	C1
14	A3	B2	C1
15	A3	B3	C1
16	A3	B1	C2
17	A3	B2	C2
18	A3	B3	C2

3.2. Возможность подделки определяется технологией изготовления СЗЗ:

A1 - СЗЗ изготовлен с использованием отечественных НОУ-ХАУ технологий;

A2 - СЗЗ изготовлен с использованием зарубежных НОУ-ХАУ технологий;

A3 - СЗЗ изготовлен без использования НОУ-ХАУ технологий.

3.3. Идентифицируемость определяется уровнем сложности сигнальной информации в знаке:

B1 - целостность и подлинность СЗЗ могут быть однозначно определены с применением специальных технических средств контроля или с помощью приборов или устройств с дополнительной (оптической, компьютерной и т. п.) обработкой сигнала по специальной методике, основанной на технологии изготовления СЗЗ;

В2 - целостность и подлинность СЗЗ могут быть однозначно определены на основании специальных методик контроля без применения технических средств контроля или с использованием серийно-выпускаемых технических средств;

В3 - целостность и подлинность СЗЗ могут быть однозначно определены визуально без применения технических средств и специальных методик контроля.

3.4. По стойкости защитных свойств СЗЗ подразделяются на две группы:

С1 - в технических условиях на СЗЗ задано изменение его внешнего вида и хотя бы одного характерного признака при несанкционированных воздействиях на СЗЗ или нарушении условий его эксплуатации;

С2 - в технических условиях на СЗЗ задано изменение только его внешнего вида при несанкционированных воздействиях на СЗЗ или нарушении условий его эксплуатации.

3.5. Для защиты информации, отнесенной к государственной тайне, и защиты технических средств категорированных объектов используются только СЗЗ, сертифицированные по классу не ниже 6:

по классам 1 и 2 - для защиты объектов 1 категории и информации соответствующей степени секретности;

по классам 3 и 4 - для защиты объектов 2 категории и информации соответствующей степени секретности;

по классам 5 и 6 - для защиты объектов 3 категории и информации соответствующей степени секретности.

Использование СЗЗ, сертифицированных по классам 7 - 12, допускается только для защиты объектов 3 категории и информации соответствующего уровня секретности при обеспечении дополнительных организационно-технических мер защиты, согласованных с Гостехкомиссией России.

3.6. При нарушении режима сохранения информации о применяемой НОУ-ХАУ технологии, изменении условий производства и т. п. использование СЗЗ запрещается, ранее выданный сертификат аннулируется.

Руководящий документ.
Средства защиты информации.
Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах.
Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации.

Сборник руководящих документов по защите информации от несанкционированного доступа. Гостехкомиссия России, 1998 г.

Настоящий руководящий документ распространяется на электронные контрольно-кассовые машины (ККМ) и автоматизированные кассовые системы (АКС), которые осуществляют обработку информации, подлежащей контролю налоговыми органами.

Данный руководящий документ устанавливает термины и основные понятия в области защиты информации в ККМ и АКС, классификацию ККМ, АКС и требования по защите информации, связанной с налогообложением, в ККМ и АКС различных сфер применения.

Документ должен использоваться как нормативно-методический материал для производителей, разработчиков и поставщиков ККМ и АКС при формулировке и реализации требований по защите информации о денежных расчетах с населением, необходимой для правильного исчисления налогов и контроля налоговыми органами, а также испытательными лабораториями (центрами) при проведении сертификации данных устройств в Системе сертификации средств защиты информации по требованиям безопасности информации (РООС RU 0001.01БИ00).

Данный Руководящий документ разработан в соответствии с Законами Российской Федерации «О применении контрольно-кассовых машин», «Об информации, информатизации и защите информации» и в соответствии с Указом Президента Российской Федерации от 16 февраля 1993 г. №224 «Об обязательном применении контрольно-кассовых машин предприятиями, учреждениями и организациями всех форм собственности при осуществлении расчетов с населением».

Документ учитывает технические требования к электронным ККМ различных моделей и сфер применения, включенных в Госреестр Российской Федерации, технические требования к фискальной памяти электронных ККМ, пакетам прикладных программ в части защиты информации от несанкционированного доступа, утвержденные Государственной межведомственной экспертной комиссией по контрольно-кассовым машинам.

Принятые сокращения:

ККМ - контрольно-кассовая машина;

АКС - автоматизированная кассовая система;

СВТ - средство вычислительной техники;
ЗУ - запоминающее устройство;
ПЗУ - постоянное запоминающее устройство;
НСД - несанкционированный доступ;
ФД - фискальные данные;
ФП - фискальная память;
ППП - пакеты прикладных программ;
ЯЗ - ядро защиты.

1. Термины и определения

Установленные термины обязательны для применения во всех видах документации по защите информации. Для каждого понятия установлен один термин. Применение синонимов термина не допускается. Для отдельных терминов даны (в скобках) краткие формы, которые разрешается применять в случаях, исключающих возможность их различного толкования.

Контрольно-кассовая машина (ККМ) - устройство, предназначенное для автоматизации и механизации учета, контроля и первичной обработки информации кассовых операций и регистрации ее на печатаемых документах в соответствии с принятыми нормативными и правовыми документами.

Автоматизированная кассовая система (АКС) - система, состоящая из персонала и ККМ на основе средств вычислительной техники, реализующая технологию обработки информации кассовых операций.

Фискальные данные (ФД) - информация о денежных расчетах с населением, проведенных на ККМ, необходимая для правильного исчисления налогов и контроля со стороны налоговых органов, подлежащая ежесуточной (ежесменной) регистрации и долговременному хранению.

Фискальные функции (операции с ФД):

формирование и накопление ФД в суточных (сменных) счетчиках и регистрах с оформлением и печатью финансовых документов;

запись (регистрация) ФД в фискальную память с оформлением и печатью финансовых документов;

хранение ФД в фискальной памяти;

чтение ФД из фискальной памяти с оформлением и печатью документов.

Фискальная память ККМ (ФП) - комплекс программно-аппаратных средств в составе ККМ, обеспечивающий некорректируемую, ежесуточную (ежесменную) регистрацию и энергонезависимое долговременное хранение итоговой информации о денежных расчетах с населением, проведенных на ККМ, необходимой для правильного исчисления налогов.

Защита фискальных данных - предотвращение несанкционированного доступа к ФД с целью их корректировки (умышленного искажения), модификации или уничтожения вследствие неисправности технических

средств, ошибки программного обеспечения, преднамеренных и непреднамеренных действий человека.

Пакеты прикладных программ (ППП) - комплекс прикладных программ ККМ, предназначенный для решения взаимоувязанных задач реализации фискальных функций.

Системные данные - параметры системы, используемые при загрузке и определяющие конфигурацию средств вычислительной техники.

Фискализация - включение фискального режима ККМ.

Ядро защиты (ЯЗ) - технические, программные и микропрограммные элементы комплекса средств защиты фискальных данных, реализующие функцию управления доступом к фискальной памяти.

2. Классификация ККМ

2.1. Классификация распространяется на все действующие и проектируемые ККМ зарубежного и отечественного производства.

2.2. Деление контрольно-кассовых машин и средств вычислительной техники, входящих в состав АКС на соответствующие группы по их конструктивным и функциональным особенностям с точки зрения защиты информации, подлежащей контролю налоговыми органами, проводится для выработки и применения обоснованных мер по достижению требуемого уровня защищенности фискальных данных.

2.3. Дифференциация подходов к выбору методов, средств защиты и принципов построения ядра защиты определяется различием контрольно-кассовых машин по своему составу, функциональным и конструктивным особенностям, способам хранения фискальных данных.

2.4. Устанавливаются две группы ККМ, согласно которым к ККМ предъявляются требования по защите информации, хранимой в ФП. Каждая группа характеризуется определенной совокупностью требований по защите информации.

2.5. Первая группа ККМ включает устройства, имеющие закрытую архитектуру.

Признаки закрытой архитектуры:

наличие программного обеспечения, находящегося в ПЗУ и его исполнение путем прямого считывания команд из ПЗУ;

невозможность выполнения прикладного программного обеспечения, находящегося во внешней памяти.

2.6. Вторая группа ККМ включает устройства, имеющие открытую архитектуру.

Признаки открытой архитектуры:

наличие устройства, выполненного на базе универсальных средств вычислительной техники;

прикладное программное обеспечение в виде ППП загружается в оперативную память;

наличие стандартных интерфейсов ввода/вывода с возможностью подключения периферийных устройств;

модульное конструктивное исполнение.

2.7. В пределах каждой группы ККМ классифицируются по масштабам возможных материальных потерь вследствие уклонения от налогообложения. К первому классу относятся устройства, использование которых связано с обработкой информации о денежных оборотах на сумму до 700 минимальных размеров оплаты труда в сутки, а ко второму классу - устройства, связанные с обработкой информации о денежных оборотах на сумму свыше 700 минимальных размеров оплаты труда в сутки.

3. Требования по защите информации, хранимой в фискальной памяти, от НСД

3.1. ФП должна исключать возможность потери информации за счет физического старения носителя фискальных данных в период их хранения или под влиянием окружающей среды (световых и электромагнитных излучений, температуры и пр.) в соответствии с техническими требованиями, оговоренными в действующих нормативных документах, регламентирующих вопросы эксплуатации, хранения и транспортировки ККМ.

3.2. В качестве ФП запрещается использовать:

устройства, информация в которых сохраняется менее 6 лет с момента фискализации ККМ;

средства, срок службы которых до первого ремонта менее 10 лет;

микросхемы памяти, гарантированный срок хранения информации в которых менее 10 лет;

микросхемы памяти, требующие электро-, термо- тренировки для записи информации;

устройства, требующие технического обслуживания в период хранения фискальных данных;

устройства, допускающие стирание информации под воздействием внешних источников (ультрафиолетового излучения, электрических сигналов и т.п.).

3.3. ФП не должна иметь прямой электрической связи с системной магистралью процессора обработки данных.

3.4. Адреса ФП не должны находиться в области адресного пространства процессора обработки данных ККМ.

3.5. Комплекс средств защиты ФП должен обеспечивать:

защиту фискальных данных от сбоев по питанию;

защиту фискальных данных от несанкционированного изменения;

защиту от стирания (очистки) фискальных данных;

защиту от использования очищенной ФП без предварительной инициализации;

защиту от несанкционированной замены ФП;

защиту от несанкционированного отключения фискального режима;

контроль правильности записи в ФП фискальных данных;

сравнение даты записи фискальных данных с датой предыдущей записи в ФП и блокировку записи в случае, если дата осуществляемой записи более ранняя, чем дата предыдущей записи;

контроль целостности всех фискальных данных, содержащихся в ФП, при записи суточного (сменного) итога в ФП;

контроль правильности читаемых фискальных данных при снятии отчета ФП и выдачу сообщения при чтении (печати) испорченных фискальных данных.

3.6. Средства защиты должны обеспечивать следующие блокировки:

блокировку всех операций, кроме чтения ФП, при обнаружении испорченных фискальных данных в ФП;

блокировку попыток изменения местоположения десятичной точки до операции перерегистрации;

блокировку всех операций, кроме чтения ФП, при переполнении ФП;

блокировку всех операций при неисправности ФП;

блокировку всех операций при отсутствии ФП;

блокировку попыток подбора пароля доступа к фискальным данным;

блокировку попыток выполнения любых действий с ФП до записи заводского номера;

блокировку повторной записи заводского номера;

блокировку попыток выполнения любых действий с ФП, кроме чтения и записи заводского номера, до проведения фискализации;

блокировку попыток выполнения более 4-х перерегистраций;

блокировку попыток выполнения любых действий с использованием пароля доступа к ФП, до записи суточного (сменного) итога в ФП.

3.7. Программы управления работой ФП должны быть защищены от изменения.

4. Требования, предъявляемые к ККМ и АКС в зависимости от группы

4.1. Средства защиты ККМ первой группы устройств должны обеспечивать:

защиту системных данных от сбоев по питанию;

защиту от несанкционированной замены или изменения программного обеспечения в ПЗУ ККМ;

защиту фискальных данных от НСД не ниже 6 класса защищенности для ККМ 1 класса и не ниже 5 класса защищенности для ККМ 2 класса (согласно РД Средства вычислительной техники. Защита от несанкциониро-

ванного доступа к информации. Показатели защищенности от НСД к информации).

4.2. Средства защиты ККМ второй группы устройств должны обеспечивать:

запись и хранение системных данных в энергонезависимой памяти;

защиту системных данных от сбоев по питанию;

защиту системных данных от несанкционированного изменения;

защиту от загрузки операционной системы с внешнего устройства;

защиту от замены или изменения незагружаемого программного обеспечения;

защиту от замены или изменения загружаемого программного обеспечения;

блокировку попыток записи двух суточных (сменных) итогов подряд, без промежуточного оформления платежных документов;

защиту фискальных данных от НСД не ниже 5 класса защищенности для ККМ 1 класса и не ниже 4 класса защищенности для ККМ 2 класса (согласно РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации);

защиту фискальных данных от НСД не ниже класса защищенности 1Г для ККМ 1 класса, объединенных в АКС и не ниже класса защищенности 1В для ККМ 2 класса, объединенных в АКС (согласно РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации).

5. Порядок проведения сертификации ККМ и АКС

5.1. Сертификация ККМ, АКС и ППП для ККМ и АКС по требованиям защиты информации производится в соответствии с требованиями «Положения о сертификации средств защиты информации по требованиям безопасности информации» и «Типовыми методиками сертификации ППП по требованиям безопасности информации от НСД».

5.2. Сертификация ККМ и АКС отечественного производства производится с последующей аттестацией производства по выпуску сертифицированной продукции и выдачей сертификационной лицензии на право применения знака соответствия.

5.3. Сертификация партии устройств производится по репрезентативной выборке из партии с последующей выдачей сертификата на всю партию. Действие сертификата соответствия распространяется на аналогичные устройства последующих партий при условии проведения дополнительной проверки выборки из последующих партий.

5.4. Сертификация единичных образцов ККМ и АКС проводится по схеме испытаний единичного образца с последующей выдачей сертификата на единичный образец с указанием заводского номера (уникального кода идентификации).