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.

Принятые сокращения
1. Общие положения
2. Требования к показателям защищенности
2.1. Показатели защищенности
2.2. Требования к показателям защищенности шестого класса
2.3. Требования к показателям пятого класса защищенности
2.4. Требования к показателям четвертого класса защищенности
2.5. Требования к показателям третьего класса защищенности
2.6. Требования к показателям второго класса защищенности
2.7. Требования к показателям первого класса защищенности
3. Оценка класса защищенности СВТ (сертификация СВТ)

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).

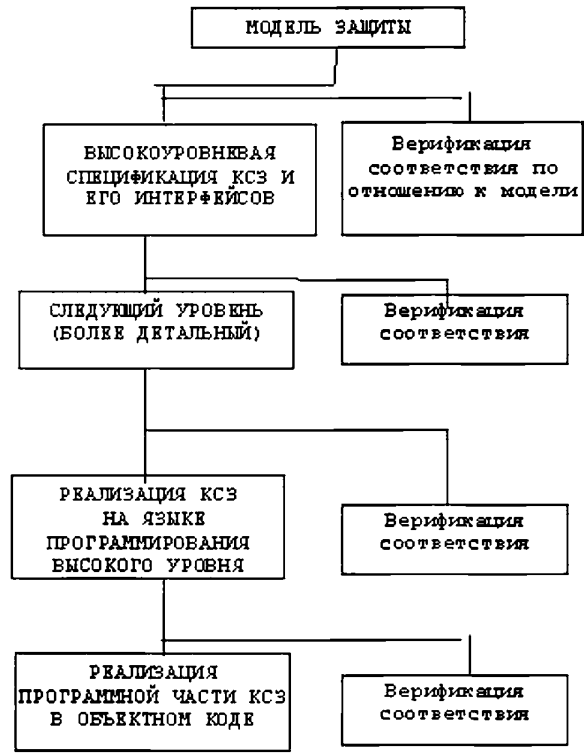

СХЕМА МОДЕЛИ ЗАЩИТЫ (к п.2.6.9)

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.