Министерство науки и высшего образования РФ

Томский государственный университет
систем управления и радиоэлектроники

А.А Конев, А.Ю. Якимук

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Учебно-методическое пособие
для студентов направлений подготовки
10.00.00 Информационная безопасность

Томск
2022

УДК 004.056
ББК 32.973.26-018.2
К 64

Конев А.А., Якимук А.Ю.
К 64 Защищенные информационные системы: учебно-методическое пособие. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2022. – 60 с.

Настоящее учебно-методическое пособие содержит описания лабораторных, практических и самостоятельных работ по дисциплине «Защищенные информационные системы» для направлений подготовки, входящих в укрупненную группу специальностей и направлений 10.00.00 Информационная безопасность.

УДК 004.056
ББК 32.973.26-018.2

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Целью преподавания дисциплины является освоение дисциплинарных компетенций, связанных с созданием и изучением современной защищенных информационных систем различного применения и степени сложности, обучение принципам и методам защиты информации, комплексного проектирования, построения, обслуживания и анализа защищенных информационных систем, а также содействовать формированию научного мировоззрения и развитию системного мышления .

Задачи изучения дисциплины – получение студентами:

– Системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности;

– Обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

– Разработка систем, комплексов, средств и технологий обеспечения информационной безопасности;

– Изучение методов контроля и оценки установленного программного и аппаратного обеспечения на защищаемых компьютерах в локальной сети;

– Разработка программ и методик испытаний средств и систем обеспечения информационной безопасности.

ЛАБОРАТОРНАЯ РАБОТА
Проектирование автоматизированной системы с учетом государственных стандартов

1. Цель работы

В рамках работы рассматривается понятие сложной системы: элементы и подсистемы, управление и информация, самоорганизация.

2. Краткие теоретические сведения

Конгломерат - совокупность элементов.

Система - совокупность элементов с определенными связями между ними. (Ф.С. Флейшман)

Индивидуальность системы проявляется в её структуре и поведении.

Структура - внутреннее устройство чего-либо.

Поведение - действия объекта.

Структура и поведение системы взаимно обусловлены. Сложности структуры системы сопутствует сложность её поведения.

Сложность системы характеризуют сложностью её поведения – разнообразие реакций на внешнее воздействие.

В порядке возрастания сложности поведения реальные системы разделяют на следующие типы: автоматические, решающие, самоорганизующие, предвидящие и превращающиеся.

Автоматические системы детерминировано реагируют на внешние воздействия. Система переходит в равновесное состояние при выходе из него. Примеры: маятник.

Решающие системы имеют постоянные стохастические критерии различия случайных сигналов и постоянные стохастические реакции на случайные воздействия. Постоянство их структуры поддерживается заменой

вышедших из строя элементов. Примеры: локатор, рецепторные механизмы организмов.

Самоорганизующие системы имеют гибкие критерии различия сигналов и гибкие реакции на воздействия, приспосабливающиеся к заранее неизвестным сигналам и воздействиям. Устойчивость высших форм таких систем обеспечивается постоянным воспроизведением (структурно-информационная устойчивость). Примеры: модель типа персептрона, кибернетические игрушки, простейшие организмы.

Предвидящие системы. На определенном уровне сложности самоорганизующие системы приобретают столь мощную память и устойчивость, что сложность их поведения начинает превосходить сложность воздействие индифферентного внешнего мира. Помня исходы взаимодействия с внешним миром до данного момента, такая система может «предвидеть» дальнейший ход взаимодействия, полагаясь на повторение прежних ситуаций. Пример: высшие животные, человек.

Система – совокупность взаимосвязанных элементов, объединенных единством цели и функциональной целостностью. (Шумский А.А., Шелупанов А.А.).

Элемент системы - это объект, имеющий некоторые свойства и реализующий определенную функцию системы. Внутренняя структура элемента не рассматривается.

В качестве элемента может выступать другая система. Тогда эта система будет подсистемой рассматриваемой системы.

Классификация – разделение совокупности объектов на классы по определенным признакам или совокупности признаков. Эти признаки должны быть существенными.

Таким образом, в класс входят элементы, которые обладают некоторыми общими признаками. Однозначной классификации систем нет.

Предыдущее разделение на классы основывалось на признаке возрастания сложности поведения систем.

В чем проявляется сложность поведения системы? В выборе возможных альтернатив поведения. Пусть состояние система характеризуется некоторым набором переменных - $(x_1, x_2 \dots x_n)$ (рис.1).

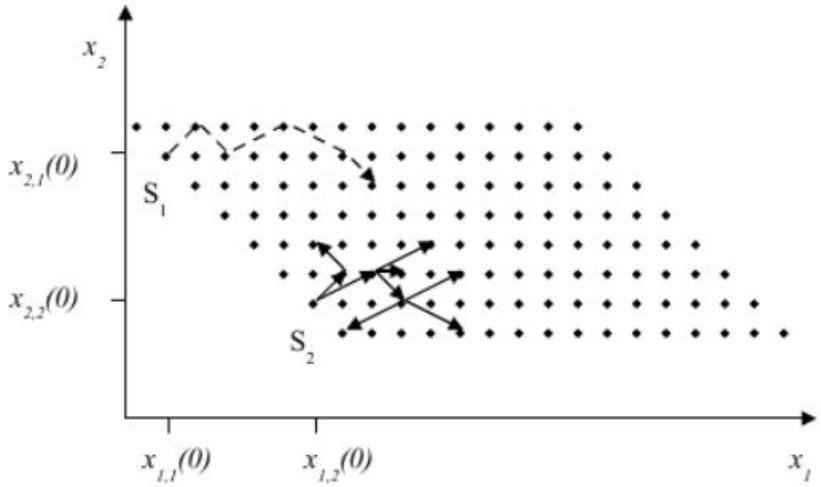

Рис. 1. Поведение простой (S_1) и сложной (S_2) систем в пространстве состояний

Рассмотрим две системы и сравним их по критерию сложности. Система S_1 начинает свое функционирование из состояния $S_1(0) = (x_{1,1}(0), x_{2,1}(0))$. Система S_2 начинает свое функционирование из состояния $S_2(0) = (x_{1,2}(0), x_{2,2}(0))$. Наблюдая за системой S_1, мы обнаружили, что ее траектория в пространстве состояний всегда описывается пунктирной линией. Наблюдения за системой S_2 , нам дали результат, изображенный на рисунке сплошными стрелками. При разных
испытаниях система ведет себя по-разному. Из этих наблюдений мы можем сделать вывод, что система S_2, сложнее системы S_1.

Однако это не означает, что система S2 сложная. Общепризнанной границы, разделяющей простые, сложные и большие системы нет. Но всегда мы можем, сравнивая две системы, определить, которая из них сложнее или они имеют одинаковую сложность.

Будем считать проявлением сложности системы возможность выбора альтернатив поведения. Механизм выбора может быть разнообразный, например, случайный выбор, выбор по критерию изменяющегося во времени.

Системы, которые по своей сложности не превосходят автоматические, будем считать простыми.

Системы, превосходящие по сложности автоматические, начиная с решающих систем, будем называть сложными.

Большими системами будем называть совокупность разнородным сложных систем со сравнительно слабыми связями между ними.

Термин “большая система” характеризует одну черту сложности – размерность системы.

Сложные системы характеризуются как минимум двумя признаками: свойство устойчивости и функциональной анизотропностью.

Свойство устойчивости – способность сохранять частичную работоспособность при отказе отдельных элементов или подсистем. Это свойство объясняется функциональной избыточностью сложной системы.

Функциональная анизотропность – неравноценность элементов и связей системы.

Простая система может находиться только в двух состояниях: полной работоспособности и полного отказа.

Понятие системы развивалась многими авторами до различной степени формализации. Например, в книге «Системный подход и общая теория систем». Уемов А.И. – М.: Мысль. 10978., собрано 35 различных определений

системы. Ведется работа над математической формализацией понятий системы, простоты и сложности системы, поведения, цели. Разрабатываются аксиоматические подходы теории сложных систем. Но это все еще далеко от завершения.

Отметим, как правило, все эти понятия на естественнонаучном уровне воспринимаются вполне однозначно. Например, при более детальном рассмотрении структуры и поведения конкретных систем различие между простыми и сложными системами становятся очевидны.

Любая система функционирует с какой-то целью. Понятие цели является одним из важнейших характеристик систем. Имеется даже определение системы как средство достижения цели. (Ф.И. Перегудов, Ф.П. Тарасенко. Основы системного анализа. Томск: Изд-во НТЛ, 2001ю-396 с.)

Рассмотрим искусственные системы. Искусственные системы создаются человеком для достижения какой-то цели. Деятельность человека носит целенаправленный характер. Цели редко достижимы при имеющихся на данный момент ресурсах (материальных, энергетических, временных, финансовых, интеллектуальных).

Возникает ситуация, которая называется проблемной. Проблематика ситуации осознается в несколько стадий.

Первая стадия – что-то не так. Затем идет осознание потребности. Потом формирование проблемы – почему потребность не может быть удовлетворена в данный момент. И наконец формулировка цели.

Цель – это субъективный образ (абстрактная модель) несуществующего, но желаемого состояния системы и окружающей среды. При этом предполагается, что это состояние решает проблемную ситуацию, которая привела к формулированию цели.

Рассмотрим виды целей по классификации, приведенной в книге Мильнер Б.З. Теория организаций. - М.: Инфа-М, 1998.

Цели:

- Конечные, бесконечные.
- Качественные, количественные.
- Развития, функционирования.
- Простые, сложные.
- Личные, организации.

Бесконечные цели это общее направление деятельности. Это как вектор в пространстве состояний системы. Тогда как конечная цель может иметь конкретное состояние системы или конкретное, числовое значение её параметров.

Пусть система описывается параметрами $(x_1, x_2 \dots x_n)$. И цель системы сформулирована в виде достижения минимума какой-то функции от этих параметров.

$F(x_1, x_2 \dots x_n) \rightarrow min.$

Пусть в каждый момент времени имеется возможность определить параметры $(x_1, x_2 \dots x_n)$, которые приближают значение функцию к минимуму. Но может оказаться, что эта последовательность окажется бесконечной. Цель бесконечная, но направление известно. Если же мы ограничимся не точным значением минимума, приближенным, то цель становится конечной.

В зависимости от характера решаемой проблемы формулировка целей может выражаться как в качественной, так и в количественной форме.

Цели функционирования и развития это два режима поведения системы по отношению к состоянию цели. В режиме функционирования считается, что поведение системы полностью удовлетворяет потребностям внешней среды и её поведение происходит при постоянстве заданных

целей. В режиме развития система в некоторый момент времени перестает удовлетворять потребностям внешней среды. В этом случае требуется корректировка цели.

Классификация по простым и сложным целям учитывает тот момент, что большинство систем, встречающихся нам в практической деятельности содержат в себе как элементы другие системы. Мы определили их как подсистемы. Эти подсистемы могут иметь свои цели, которые в той или степени подчинены цели системы, которой они принадлежат. В соответствии с этим цель системы может быть комплексной.

Критерий – количественный или порядковый показатель, на основании которого производится оценка, определение, классификация систем.

Выделяют две большие группы критериев при оценивании систем. Это критерий качества и критерий эффективности систем.

Критерии качества:

- Устойчивость.
- Помехоустойчивость.
- Управляемость.
- Способность.
- Самоорганизация.

Устойчивость системы во времени это необходимое свойство всех систем. Различают два вида устойчивости систем: вещественно-энергетическую и структурно-функциональную.

Вещественно-энергетическая устойчивость связана с постоянством вещественного состава и энергетического баланса системы.

Структурно-функциональная устойчивость с постоянством структуры системы и постоянством её реакций на внешние воздействия.

Один из этих видов устойчивости является определяющим в зависимости от сложности системы. Примеры:

1. Атомы, молекулы – 1-й вид.
2. Искусственные сооружения (мосты, здания) – 1-й тип, частично второй. Устойчивость = прочности.
3. Машины – 1-й и 2-й тип. Детали машин можно заменить. Постоянство структуры при переменном вещественном составе.
4. Клетка – 2-й тип в полной мере. Устойчивость = надежность.

С ростом сложности надежность сложных систем не имеет тенденции падать.

Критерии эффективности:

- Результативности (Результативность функционирования системы определяется достижением цели системы).
- Ресурсоемкости (Критерий эффективности ресурсоемкость характеризуется ресурсами всех видов, которые используются для достижения цели, количеством ресурсов затраченных для достижения цели, распределением затрат ресурсов по времени функционирования).
- Оперативности (Оперативность по исходу операции (функционирования) определяется временем необходимым для достижения цели. Оперативность по качеству алгоритма обеспечивающего получение результатов. В совокупности указанные критерии эффективности порождают новое свойство – эффективность процесса. Это свойство зависит как от самой системы, так и от внешней среды).

Для простых систем в понятии устойчивость объединяются такие свойства как:

– Прочность.
– Стойкость к внешним воздействиям.
– Сбалансированность.
– Стабильность.
– Гомеостаз (способность системы возвращаться в равновесное состояние при выводе из него внешними воздействиями).

Для сложных систем характерны различные формы структурной устойчивости:

– Надежность.
– Живучесть.

Свойства систем:

1. Свойство жизнеспособности. Система жизнеспособна во все моменты времени. Но если её постигла смерть в данный момент времени, то в последующие моменты времени ничто не может возродить её к жизни.
2. Свойство неограниченного расширения. Если система жива в данный момент времени, то в следующий момент времени она может пополниться любым числом элементов.
3. Физическая ограниченность времени реакции. О своем состоянии в данный момент времени система узнает лишь в следующий момент, отстающий от данного на интервал, принятый за единицу.

ПРАКТИЧЕСКАЯ РАБОТА №1
Классы защищенности СВТ

1. Цель работы

Целью работы является изучение классов защищенности средств вычислительной техники (СВТ) по показателям защищенности: дискреционный принцип контроля доступа; идентификация и аутентификация.

2. Краткие теоретические сведения

2.1 Дискреционный принцип контроля доступа

Шестой класс:

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.).

Пятый класс:

Данные требования включает в себя аналогичные требование шестого класса. Дополнительно должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

Четвертый класс:

Данные требования включают аналогичные требования пятого класса. 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.

Третий класс:

Данные требования полностью совпадают с требованиями пятого и четвертого классов.

Второй класс:

Данные требования включают аналогичные требования третьего класса. 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).

Первый класс:

Данные требования полностью совпадают с аналогичным требованием второго класса.

Полный перечень требований к показателям защищенности представлен в Приложении А.

2.2 Идентификация и аутентификация

Шестой класс:

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

Пятый класс:

Данные требования включает в себя аналогичные требование шестого класса.

Четвертый класс:

КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ. КСЗ должен проверять подлинность идентификатора субъекта – осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации и препятствовать входу в СВТ не идентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась. КСЗ должен обладать способностью надежно связывать полученную идентификацию со всеми действиями данного пользователя.

Третий класс:

Данные требования включает в себя аналогичные требование четвертого класса.

Второй класс:

Данные требования включает в себя аналогичные требование четвертого класса.

Первый класс:

Данные требования включает в себя аналогичные требование четвертого класса.

3. Задание на практическую работу

Задача 1.

Определить, к какому классу защищенности относится каждая из СВТ по показателю защищенности – дискреционный принцип контроля доступа. Класс имеет следующее содержание:

1.

- Контролирует доступ наименованных субъектов к наименованным объектам).
- Для каждой пары (субъект – объект) в СВТ должно быть задано явное перечисление допустимых типов доступа для каждой пары (субъект – объект).
- Содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа.

2.

- Предусмотрена возможность санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.
- Права изменять ПРД предоставляются выделенным субъектам (администрации, службе безопасности и т.д.).
- Имеются средства управления, ограничивающие распространение прав на доступ.

3.

- Имеются средства управления, ограничивающие распространение прав на доступ.
- Содержится механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых.

– Дискреционные правила разграничения доступа были эквивалентны мандатным правилам.

4.

– Контролирует доступ наименованных субъектов к наименованным объектам).
– Для каждой пары (субъект – объект) в СВТ должно быть задано явное перечисление допустимых типов доступа для каждой пары (субъект – объект).
– Содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа.
– Контроль доступа применяется к каждому объекту и каждому субъекту.
– Предусмотрена возможность санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.
– Права изменять ПРД предоставляются выделенным субъектам (администрации, службе безопасности и т.д.).
– Имеются средства управления, ограничивающие распространение прав на доступ.
– Содержится механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых.

Задача 2.

Определить, к какому классу защищенности относится каждая из СВТ по показателю защищенности – идентификация и аутентификация. Класс имеет следующее содержание:

1.

– КСЗ требует от пользователей идентифицировать себя при запросах на доступ.

– КСЗ располагает необходимыми данными для идентификации и аутентификации.
– КСЗ препятствует доступу к защищаемым ресурсам не идентифицированных пользователей идентификации которых при аутентификации не подтвердилась.
– КСЗ требует от пользователей идентифицировать себя при запросах на доступ.

2.

– КСЗ требует от пользователей идентифицировать себя при запросах на доступ.
– КСЗ проверяет подлинность идентификации – осуществляет аутентификацию.
– КСЗ располагает необходимыми данными для идентификации и аутентификации.
– КСЗ препятствует доступу к защищаемым ресурсам не идентифицированных пользователей аутентификацию.
– КСЗ располагает необходимыми данными для идентификации и аутентификации и препятствовать входу в СВТ не идентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась.

3.

– КСЗ препятствует доступу к защищаемым ресурсам пользователей, подлинность идентификации которых при аутентификации не подтвердилась.
– КСЗ требует от пользователей идентифицировать себя при запросах на доступ
– КСЗ проверяет подлинность идентификатора субъекта - осуществляет аутентификацию.
– КСЗ располагает необходимыми данными для идентификации и аутентификации и препятствовать

входу в СВТ не идентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась.

Задача 3.

Определить, к какому классу защищенности относится каждая из СВТ по показателям защищенности – дискреционный принцип контроля доступа; идентификация и аутентификация. Класс имеет следующее содержание:

1.

- Контролирует доступ наименованных субъектов к наименованным объектам).
- Для каждой пары (субъект – объект) в СВТ должно быть задано явное перечисление допустимых типов доступа для каждой пары (субъект – объект).
- Содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа.
- Контроль доступа применяется к каждому объекту и каждому субъекту.
- 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.

2.

- Предусмотрена возможность санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.
- Права изменять ПРД предоставляются выделенным субъектам (администрации, службе безопасности и т.д.).

– Имеются средства управления, ограничивающие распространение прав на доступ.
– Содержится механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых.
– Дискреционные правила разграничения доступа были эквивалентны мандатным правилам.
– КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ.
– КСЗ должен проверять подлинность идентификатора субъекта - осуществлять аутентификацию.
– КСЗ должен располагать необходимыми данными для идентификации и аутентификации и препятствовать входу в СВТ не идентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась.

3.

– Контролирует доступ наименованных субъектов к наименованным объектам).
– Для каждой пары (субъект – объект) в СВТ должно быть задано явное перечисление допустимых типов доступа для каждой пары (субъект – объект) содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа.
– Контроль доступа применяется к каждому объекту и каждому субъекту.
– Предусмотрена возможность санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.

- Права изменять ПРД предоставляются выделенным субъектам (администрации, службе безопасности и т.д.).
- Имеются средства управления, ограничивающие распространение прав на доступ.
- Содержится механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых.
- 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 не идентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.
- КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ.
- КСЗ должен проверять подлинность идентификатора субъекта - осуществлять аутентификацию.
- КСЗ должен располагать необходимыми данными для идентификации и аутентификации и препятствовать.
- входу в СВТ не идентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась.

4. Контрольные вопросы

1. Что такое дискреционный принцип контроля доступа?

2. Содержание показателя защищённости: дискреционный принцип контроля доступа?

3. Что такое идентификация? Аутентификация?

4. Чем характеризуется шестой класс защищенности СВТ?

5. Чем характеризуется пятый класс защищенности СВТ?

6. Чем характеризуется четвертый класс защищенности СВТ?

7. Чем характеризуется третий класс защищенности СВТ?

8. Чем характеризуется второй класс защищенности СВТ?

9. Чем характеризуется первый класс защищенности СВТ?

ПРАКТИЧЕСКАЯ РАБОТА №2
Показатели защищенности

1. Цель работы

Целью работы является работа с показателями защищенности средств вычислительной техники (СВТ) по показателям защищенности: дискреционный принцип контроля доступа; идентификация и аутентификация; очистка памяти.

2. Краткие теоретические сведения

Ниже представлены требования к показателю защищенности – очистка памяти:

Шестой класс:

Нет.

Пятый класс:

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

Четвертый класс:

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.

Третий класс:

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).

Второй класс:

Данные требования полностью совпадают с аналогичным требованием третьего класса.

Первый класс:

Данные требования полностью совпадают с аналогичным требованием второго класса.

3. Задание на практическую работу

Задача 1.

Для показателя защищенности – дискреционный принцип контроля доступа выполнить следующие действия:

1. Разбить содержание показателей защищенности на терминальные множество.
2. Определить число всевозможных подмножеств.
3. Выделить подмножества по классам.
4. Записать формулу включения классов.

Задача 2.

Для показателя защищенности – идентификация и аутентификация выполнить следующие действия:

1. Разбить содержание показателей защищенности на терминальные множество.
2. Определить число всевозможных подмножеств.
3. Выделить подмножества по классам.
4. Записать формулу включения классов.

Задача 3.

Для показателя защищенности – очистка памяти выполнить следующие действия:

1. Разбить содержание показателей защищенности на терминальные множество.
2. Определить число всевозможных подмножеств.
3. Выделить подмножества по классам.
4. Записать формулу включения классов.

Задача 4.

Для показателя защищенности – дискреционный принцип контроля доступа идентификация и аутентификация выполнить следующие действия:

1. Разбить содержание показателей защищенности на терминальные множество.
2. Определить число всевозможных подмножеств.
3. Выделить подмножества по классам.
4. Записать формулу включения классов.

4. Контрольные вопросы

1. Что такое очистка памяти?
2. Содержание показателя защищённости: очистка памяти?
3. Чем характеризуется шестой класс защищенности СВТ?
4. Чем характеризуется пятый класс защищенности СВТ?
5. Чем характеризуется четвертый класс защищенности СВТ?
6. Чем характеризуется третий класс защищенности СВТ?
7. Чем характеризуется второй класс защищенности СВТ?
8. Чем характеризуется первый класс защищенности СВТ

Методические указания к самостоятельной работе

В рамках курса самостоятельная работа включает в себя (табл. 1):

Таблица 1

Самостоятельная работа

№	Тематика самостоятельной работы	Часы	Контроль выполнения работы
1	Изучение дополнительного материала к лекциям	10	Рефераты
2	Изучение документов и законодательства по защите информации	12	Опрос
3	Подготовка к практическим занятиям	10	Решения задач
4	Изучение материалов лекций	14	Экзамен
	ИТОГО	46	

Изучение дополнительного материала к лекциям предполагает написание реферата.

Реферат – это самостоятельная научно-методическая работа студента, выполняемая без непосредственного руководства преподавателя. Главной целью, преследуемой при выполнении данной работы, является развитие у студентов навыков самостоятельной исследовательской работы.

Структура самостоятельной работы должна способствовать раскрытию темы и отдельных ее вопросов. Отчет по самостоятельной работе должен включать в себя введение, основную часть, заключение. Основная часть должна разбиваться на отдельные разделы. Все части должны быть изложены в строгой логической последовательности и

взаимосвязи. Содержание работы следует иллюстрировать схемами, таблицами, диаграммами, графиками, фотографиями, рисунками и т. д. Графическому материалу по тексту необходимо давать пояснения.

В ведении описывается проблематика задачи, которая должна быть
решена в ходе выполнения работ, актуальность данного вопроса.

В основной части дается обзор предметной области, изучается круг
проблем, связанных с темой самостоятельной работы. Рассматриваются
методы, используемые при решении проблем, связанных с данной темой.
Предлагается метод решения проблемы.

В заключении констатируется результат, полученный в ходе выполнения самостоятельной работы и изучения материалов по теме самостоятельной работы. Указываются области применения полученных
решений и прогнозируются перспективы развития данной тематики.

Темы для данной работы рекомендуются преподавателем и приведены ниже. Студент вправе взять другую тему, которая должна соответствовать дисциплине программно-аппаратные средства обеспечения информационной безопасности. В таком случае тема должна быть согласована с преподавателем.

К самостоятельному изучению и проработке предполагаются следующие темы:

1. Методика оценки профиля защиты изделия ИТ.
2. Методика оценки задания по безопасности изделия ИТ.
3. Обеспечение безопасности в жизненном цикле изделий ИТ.

4. Обзор структуры и содержания типичного профиля защиты.
5. Обзор структуры и содержания типичного задания по безопасности.
6. Обзор профилей защиты изделий ИТ прошедших оценку.
7. Обзор заданий по безопасности защиты изделий ИТ прошедших оценку.
8. Обзор функциональных компонентов безопасности для изделий ИТ.
9. Обзор класса функциональных требований: аудит безопасности
10. Обзор класса функциональных требований: связь и криптографическая поддержка.
11. Обзор класса функциональных требований: защита данных пользователя.
12. Обзор класса функциональных требований: идентификация и аутентификация.
13. Обзор класса функциональных требований: управление безопасностью.
14. Обзор класса функциональных требований: приватность.
15. Обзор класса функциональных требований: защита функций безопасности объекта.
16. Обзор классов функциональных требований: использование ресурсов и доверенный маршрут.
17. Обзор класса функциональных требований: доступ к объекту оценки.

В ходе изучения документов и законодательства по защите информации предполагается изучение национального стандарта безопасности ГОСТ/ИСО МЭК 15408-2002 "Общие критерии оценки безопасности информационных

технологий", а также иные законодательные акты, связанные с защитой информации.

Подготовка к практическим занятиям осуществляется по данному методическому пособию.

В рамках изучения материалов лекций подразумеваются вопросы,
изучаемые в ходе изучения материалов лекций и приведены в списке вопросов для экзамена.

Материалы для контроля знаний

1. Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.
2. Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.
3. Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.
4. Лицо или процесс, действия которого регламентируются правилами разграничения доступа.
5. Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации.
6. Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.
7. Процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных
требований по защите.
8. 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.

9. Предотвращение или существенное затруднение несанкционированного доступа:
10. Процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие.
11. Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.
12. 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.
13. Разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту.
14. Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.
15. Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте.
16. Проверка принадлежности субъекту доступа, предъявленного им идентификатора. подтверждение подлинности.
17. 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.

18. Информация, требующая защиты.
19. Субъект доступа, осуществляющий несанкционированный доступ к информации.
20. Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.
21. Доступ к информации, не нарушающий правил разграничения доступа.
22. Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.
23. Идентификатор субъекта доступа, который является его (субъекта) секретом.
24. Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.
25. Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).
26. Совокупность прав доступа субъекта доступа.
27. Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.
28. Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого

идентификатора с перечнем присвоенных идентификаторов.

29. Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
30. Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.
31. Таблица, отражающая правила разграничение доступа.
32. Комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах.
33. Уникальный признак субъекта или объекта доступа.
34. Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.
35. Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам.
36. Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.
37. Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники.

Приложение А
(справочное)
Требования к показателям защищенности

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 не идентифицированных 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 ввода 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).

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).

Приложение Б
(справочное)
Оценка класса защищенности 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.

Таблица Б.1

Оценка класса защищенности

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	+	+	+	+	+	+

Литература

1. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва : Горячая линия-Телеком, 2011. — 558 с.

2. Технология разработки программных систем: Учебное пособие / И. Г. Боровской - 2012. 260 с.

3. Основы информационной безопасности: Учебное пособие / А. М. Голиков - 2007. 201 с.