РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

Митюшин Дмитрий
Алексеевич

Защита информации от несанкционированного доступа

Тема 1. Требования к защите информации от несанкционированного доступа

Вопросы:

1. *Показатели защищённости от НСД средств вычислительной техники*
2. *Показатели защищённости АС*

Литература

1. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от НСД к информации. — Москва, 1992.
2. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Москва, 1992.

1. Показатели защищённости от НСД средств вычислительной техники.

Данные показатели устанавливаются в РД Гостехкомиссии от 30 марта 1992 г, который так и называется «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации».

Данный документ устанавливает классификацию СВТ по уровню защищённости от НСД на базе перечня показателей защищённости и совокупности описывающих их требований.

Показатели защищённости СВТ применяются к общесистемным программным средствам и операционным системам (с учётом архитектуры ЭВМ).

Конкретные перечни показателей определяют классы защищённости СВТ.

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

Каждый показатель описывается совокупностью требований.

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

1. Показатели защищённости от НСД средств вычислительной техники.

Требования к показателям реализуются с помощью программно–технических средств.

Совокупность всех средств защиты составляет комплекс средств защиты (КСЗ). Документация **КСЗ** должна быть **неотъемлемой** частью **конструкторской** документации на СВТ.

На прошлой лекции мы говорили, что устанавливается семь классов защищённости СВТ от НСД. Самый низкий класс – седьмой, самый высокий – первый, и классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты.
Выбор класса защищённости СВТ для автоматизированных систем, создаваемых на базе защищённых СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

Применение в комплекте СВТ средств криптографической защиты информации по ГОСТ 28147–89 может быть использовано для повышения гарантий качества защиты.
Перечень показателей по классам защищённости СВТ приведён в таблице.
Обозначения:
«–» – нет требований к данному классу;

1. Показатели защищённости от НСД средств вычислительной техники.

Наименование показателя	Класс защищённости					
	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	–	–	–	+	=	=
Надёжное восстановление	–	–	–	+	=	=
Целостность КСЗ	–	+	+	+	=	=
Контроль модификации	–	–	–	–	+	=
Контроль дистрибуции	–	–	–	–	+	=
Гарантии архитектуры	–	–	–	–	–	+
Тестирование	+	+	+	+	+	=
Руководство для пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

1. Показатели защищённости от НСД средств вычислительной техники.

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

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

1. Показатели защищённости от НСД средств вычислительной техники.

1.1. Требования к показателям защищённости шестого класса

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.) для данного субъекта 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.

1. Показатели защищённости от НСД средств вычислительной техники.

1.1. Требования к показателям защищённости шестого класса

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

2. Идентификация и аутентификация.

КСЗ должен:

- требовать от пользователей идентифицировать себя при запросах на доступ;
- осуществлять аутентификацию, т.е. проверять подлинность идентификации;
- должен располагать необходимыми данными для идентификации и аутентификации;
- препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых не подтвердилась.

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.

4. Руководство для пользователя.

В документации на СВТ должно быть краткое руководство пользователя с описанием способов использования КСЗ и его интерфейса с пользователем.

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.

6. Тестовая документация.

Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с п.3.) и результатов тестирования.

1. Показатели защищённости от НСД средств вычислительной техники.

1.1. Требования к показателям защищённости шестого класса

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.

1. Показатели защищённости от НСД средств вычислительной техники.

1.2. Требования к показателям пятого класса защищённости.

1. Дискреционный принцип контроля доступа.

Так же как у шестого класса, плюс дополнительно должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

2. Очистка памяти.

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

3. Идентификация и аутентификация.

Требования полностью совпадают с требованиями шестого класса.

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.

1. Показатели защищённости от НСД средств вычислительной техники

1.2. Требования к показателям пятого класса защищённости.

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 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.

1. Показатели защищённости от НСД средств вычислительной техники.

1.2. Требования к показателям пятого класса защищённости.

6. Целостность КСЗ.

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

7. Тестирование.

В СВТ пятого класса защищённости 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; (как у 6-го)
- очистка памяти в соответствии с п. 2.;
- регистрация событий в соответствии с п. 5, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней;
- работа механизма, осуществляющего контроль за целостностью КСЗ.

8. Руководство пользователя аналогично требованиям шестого класса.

1. Показатели защищённости от НСД средств вычислительной техники

1.2. Требования к показателям пятого класса защищённости.

9. Руководство по КСЗ. Требования что и для 6-го класса.

10. Тестовая документация. Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с требованиями п. 7), и результатов тестирования.

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.

1. Показатели защищённости от НСД средств вычислительной техники

1.3. Требования к показателям четвёртого класса защищённости.

1. Дискреционный принцип контроля доступа.

Данные требования аналогичны пятому 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.

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

1. Показатели защищённости от НСД средств вычислительной техники

1.3. Требования к показателям четвёртого класса защищённости.

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

1. Показатели защищённости от НСД средств вычислительной техники

1.3. Требования к показателям четвёртого класса защищённости.

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.

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 её очистку.

1. Показатели защищённости от НСД средств вычислительной техники

1.3. Требования к показателям четвёртого класса защищённости.

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.

5. Маркировка документов.

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

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.

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 надёжно сопоставляется выделенному устройству.

8. Идентификация и аутентификация.

Полностью совпадают с требованиями 6-го класса. Кроме того, КСЗ должен обладать способностью надёжно связывать полученную идентификацию со всеми действиями данного пользователя.

1. Показатели защищённости от НСД средств вычислительной техники

1.3. Требования к показателям четвёртого класса защищённости.

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.

10. Регистрация.

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

11. Целостность КСЗ.

В СВТ четвёртого класса защищённости должен осуществляться периодический контроль за целостностью КСЗ.

Программы КСЗ должны выполняться в отдельной части оперативной памяти.

1. Показатели защищённости от НСД средств вычислительной техники

1.3. Требования к показателям четвёртого класса защищённости.

12. Тестирование.

В четвёртом классе защищённости 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. 10, средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией.

1. Показатели защищённости от НСД средств вычислительной техники

1.3. Требования к показателям четвёртого класса защищённости.

13. Руководство для пользователя.

Совпадает с требованием шестого и пятого классов.

14. Руководство по КСЗ.

Данные требования полностью совпадают с аналогичными требованиями пятого класса.

15. Тестовая документация.

Должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с п. 12) и результатов тестирования.

1. Показатели защищённости от НСД средств вычислительной техники

1.3. Требования к показателям четвёртого класса защищённости.

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.

1. Показатели защищённости от НСД средств вычислительной техники

1.4. Требования к показателям третьего класса защищённости

1. Дискреционный принцип контроля доступа.

Данные требования полностью совпадают с требованиями 5-го и 4-го классов.

2. Мандатный принцип контроля доступа.

Данные требования полностью совпадают с аналогичным требованием 4-го класса.

3. Очистка памяти.

КСЗ должен осуществлять очистку оперативной и внешней памяти путём записи маскирующей информации в память при её освобождении (перераспределении).

4. Изоляция модулей.
5. Маркировка документов.
6. Защита ввода и вывода на отчуждаемый физический носитель информации.
7. Сопоставление пользователя с устройством.
8. Идентификация и аутентификация.

1. Показатели защищённости от НСД средств вычислительной техники

1.4. Требования к показателям третьего класса защищённости

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.

10. Регистрация. Требования полностью совпадают с аналогичными требованиями четвёртого класса.

1. Показатели защищённости от НСД средств вычислительной техники

1.4. Требования к показателям третьего класса защищённости

11. Взаимодействие пользователя с КСЗ.

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

12. Надёжное восстановление

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

13. Целостность КСЗ.

Необходимо осуществлять периодический контроль целостности КСЗ. Программы должны выполняться в отдельной части оперативной памяти. Это требование должно подвергаться верификации.

1. Показатели защищённости от НСД средств вычислительной техники

1.4. Требования к показателям третьего класса защищённости

14. Тестирование.

СВТ то же тестированию, что и СВТ четвёртого класса. Дополнительно должны тестироваться:

- очистка памяти;
- работа механизма надёжного восстановления.

15. Руководство для пользователя. Полностью совпадают с аналогичным требованием четвёртого класса.

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 надёжного восстановления.

1. Показатели защищённости от НСД средств вычислительной техники

1.4. Требования к показателям третьего класса защищённости

17. Тестовая документация

В документации должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (п.14), а также результатов тестирования.

18. Конструкторская (проектная) документация.

Требуется такая же документация, что и для СВТ четвёртого класса. Дополнительно необходимы:

- высокоуровневая спецификация КСЗ и его интерфейсов;
- верификация соответствия высокоуровневой спецификации КСЗ модели защиты.

1. Показатели защищённости от НСД средств вычислительной техники.

1.5. Требования к показателям второго класса защищённости

1. Дискреционный принцип контроля доступа.

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).

2. Мандатный принцип контроля доступа.

3. Очистка памяти.

Данные требования (2-3) полностью совпадают с аналогичным требованием третьего класса.

4. Изоляция модулей.

При наличии в СВТ мультипрограммирования в КСЗ программы разных пользователей в оперативной памяти ЭВМ должны быть изолированы друг от друга. Гарантии изоляции должны быть основаны на архитектуре СВТ.

1. Показатели защищённости от НСД средств вычислительной техники.

1.5. Требования к показателям второго класса защищённости

5. Маркировка документов.
6. Защита ввода и вывода на отчуждаемый физический носитель информации.
7. Сопоставление пользователя с устройством.
8. Идентификация и аутентификация.

Требование (5-8) полностью совпадает с аналогичным требованием четвёртого и третьего классов.

9. Гарантии проектирования.

Требования включают аналогичные требования третьего класса.

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.

1. Показатели защищённости от НСД средств вычислительной техники.

1.5. Требования к показателям второго класса защищённости

СХЕМА МОДЕЛИ ЗАЩИТЫ (к п.2.6.9)

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, изображённой на чертеже (см. рис. Схема модели защиты)

1. Показатели защищённости от НСД средств вычислительной техники.

1.5. Требования к показателям второго класса защищённости

10. Регистрация.

Данные требования полностью совпадают с аналогичным требованием четвёртого и третьего классов.

11. Взаимодействие пользователя с КСЗ.
12. Надёжное восстановление.
13. Целостность КСЗ.

Данные требования полностью совпадают с аналогичным требованием третьего класса.

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.

1. Показатели защищённости от НСД средств вычислительной техники.

1.5. Требования к показателям второго класса защищённости

15. Контроль дистрибуции.

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

16. Тестирование.

СВТ второго класса должны тестироваться так же, как и СВТ третьего. Дополнительно должен тестироваться контроль дистрибуции.

17. Руководство для пользователя.

Полностью совпадают с аналогичным требованием четвёртого и третьего классов.

18. Руководство по КСЗ.

Включают аналогичные требования третьего класса. Дополнительно должны быть представлены руководства по надёжному восстановлению, по работе со средствами контроля модификации и дистрибуции.

19. Тестовая документация.

Описание тестов и испытаний, которым подвергалось СВТ (п. 16), а также результатов тестирования.

20. Конструкторская (проектная) документация.

Такая же документация, что и для СВТ третьего класса. Дополнительно должны быть описаны гарантии процесса проектирования и эквивалентность дискреционных (п. 1) и мандатных (п. 2) ПРД.

1. Показатели защищённости от НСД средств вычислительной техники

1.6. Требования к показателям первого класса защищённости

1. Дискреционный принцип контроля доступа.
2. Мандатный принцип контроля доступа.
3. Очистка памяти.
4. Изоляция модулей.
5. Маркировка документов.
6. Защита ввода и вывода на отчуждаемый физический носитель информации.
7. Сопоставление пользователя с устройством.
8. Идентификация и аутентификация.

Данные требования полностью совпадают с аналогичным требованием второго класса.

9. Гарантии проектирования.

Включают аналогичные требования второго класса. Дополнительно требуется верификация соответствия объектного кода тексту КСЗ на языке высокого уровня.

10. Регистрация.
11. Взаимодействие пользователя с КСЗ.
12. Надёжное восстановление.
13. Целостность КСЗ.
14. Контроль модификации

1. Показатели защищённости от НСД средств вычислительной техники

1.6. Требования к показателям первого класса защищённости

16. Гарантии архитектуры.

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

17. Тестирование.
18. Руководство пользователя.
19. Руководство по КСЗ
20. Тестовая документация
Требования полностью совпадают с аналогичными требованиями второго класса.

21. Конструкторская (проектная) документация

Требуется такая же документация, что и для СВТ второго класса. Дополнительно разрабатывается описание гарантий процесса проектирования (п. 9).

2. Показатели защищённости АС

Рассмотрим формализованные требования к защите компьютерной информации АС в соответствии с документом [2]. При этом будем рассматривать первую группу АС, как включающую в себя наиболее распространённые многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности. Причём не все пользователи имеют право доступа ко всей информации АС.

Первая группа АС содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А. Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты. Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, а также различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала [2].

Требования к АС первой группы сведены в табл. 1.1. При этом используются следующие обозначения:
« – » нет требований к данному классу;
« + » есть требования к данному классу. (либо это дать на практике)

2. Показатели защищённости АС

Рассмотрим формализованные требования к защите компьютерной информации АС в соответствии с документом [2]. При этом будем рассматривать первую группу АС, как включающую в себя наиболее распространённые многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности. Причём не все пользователи имеют право доступа ко всей информации АС.

Первая группа АС содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А. Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты. Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, а также различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала [2].

Требования к АС первой группы сведены в табл. 1.1. При этом используются следующие обозначения:
« – » нет требований к данному классу;
« + » есть требования к данному классу. (либо это дать на практике)

2. Показатели защищённости АС

Подсистемы и требования	Классы				
	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом					
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:					
• в систему	+	+	+	+	+
• к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	–	+	+	+	+
• к программам	–	+	+	+	+
• к томам, каталогам, файлам, записям, полям записей	–	+	+	+	+
1.2. Управление потоками информации	–	–	+	+	+
2. Подсистема регистрации и учёта					
2.1. Регистрация и учёт:					
• входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+	+
• выдачи печатных (графических) выходных документов	–	+	+	+	+
• запуска (завершения) программ и процессов (заданий, задач)	–	+	+	+	+
• доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	–	+	+	+	+
• доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	–	+	+	+	+
• изменения полномочий субъектов доступа	–	–	+	+	+
• создаваемых защищаемых объектов доступа	–	–	+	+	+

2. Показатели защищённости АС

Подсистемы и требования	Классы				
	1Д	1Г	1В	1Б	1А
2.2. Учёт носителей информации	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	–	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	–	–	+	+	+
3. Криптографическая подсистема					
3.1. Шифрование конфиденциальной информации	–	–	–	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	–	–	–	–	+
3.3. Использование аттестованных (сертифицированных) криптографических средств	–	–	–	+	+
4. Подсистема обеспечения целостности					
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	–	–	+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	–	–	+	+	+

2. Показатели защищённости АС

Как видим, рассматриваемыми требованиями выделяются следующие основные группы механизмов защиты:

- механизмы управления доступом;
- механизмы регистрации и учёта;
- механизмы криптографической защиты;
- механизмы контроля целостности.

Отметим, что первая группа «Подсистема управления доступом» является основополагающей для реализации защиты от НСД, т.к. именно механизмы защиты данной группы призваны непосредственно противодействовать НСД к компьютерной информации.

2. Показатели защищённости АС

Остальные же группы механизмов реализуются в предположении, что механизмы защиты первой группы могут быть преодолены злоумышленником. В частности они могут использоваться:

- для контроля действий пользователя – группа «Подсистема регистрации и учёта»;
- для противодействия возможности прочтения похищенной информации (например, значений паролей и данных) – группа «Криптографическая подсистема»;
- для контроля осуществлённых злоумышленником изменений защищаемых объектов (исполняемых файлов и файлов данных) при осуществлении к ним НСД и для восстановления защищаемой информации из резервных копий – группа «Подсистема обеспечения целостности».

Кроме того, эти группы механизмов могут использоваться для проведения расследования по факту НСД.

Рассмотрим более подробно требования различных групп (согласно [2]), а также соответствующие им основные подходы к защите компьютерной информации, реализуемые на сегодняшний день на практике.

2. Показатели защищённости АС

При этом имеет смысл остановиться лишь на двух классах:

- 1Г, задающим необходимые (минимальные) требования для обработки конфиденциальной информации;
- 1В, задающим необходимые (минимальные) требования для обработки информации, являющейся собственностью государства и отнесённой к категории секретной.

2. Показатели защищённости АС

2.1. Требования к защите конфиденциальной информации

Подсистема управления доступом должна удовлетворять следующим требованиям:

1. Идентифицировать и проверять подлинность субъектов доступа при входе в систему. Причём это должно осуществляться по идентификатору (коду) и паролю условно–постоянного действия длиной не менее **шести** буквенно-цифровых символов.

2. Идентифицировать терминалы, ЭВМ, узлы компьютерной сети, каналы связи, внешние устройства ЭВМ по их логическим адресам (номерам).

3. По именам идентифицировать программы, тома, каталоги, файлы, записи и поля записей.

4. Осуществлять контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

2. Показатели защищённости АС

2.1. Требования к защите конфиденциальной информации

Подсистема регистрации и учёта должна:

1. Регистрировать вход (выход) субъектов доступа в систему (из системы), либо регистрировать загрузку и инициализацию операционной системы и её программного останова. При этом в параметрах регистрации указываются:
- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа – успешная или неуспешная (при НСД);
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке.

Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

2. Регистрировать выдачу печатных (графических) документов на «твёрдую» копию. При этом в параметрах регистрации указываются:
- дата и время выдачи (обращения к подсистеме вывода);
- краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности;
- спецификация устройства выдачи (логическое имя (номер) внешнего

2. Показатели защищённости АС

2.1. Требования к защите конфиденциальной информации

3. Регистрировать запуск (завершение) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов.

При этом в параметрах регистрации указывается:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный – НСД).

4. Регистрировать попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указывается:

- дата и время попытки доступа к защищаемому файлу с указанием её результата (успешная, неуспешная – несанкционированная);
- идентификатор субъекта доступа;
- спецификация защищаемого файла.

5. Регистрировать попытки доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам;

2. Показатели защищённости АС

2.1. Требования к защите конфиденциальной информации

При этом в параметрах регистрации указывается:

- дата и время попытки доступа к защищаемому файлу с указанием её результата: успешная, неуспешная, несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)].

6. Проводить учёт всех защищаемых носителей информации с помощью их маркировки и с занесением учётных данных в журнал (учётную карточку).

7. Регистрировать выдачу (приёмку) защищаемых носителей.

8. Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. При этом очистка должна производиться **однократной** произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

2. Показатели защищённости АС

2.1. Требования к защите конфиденциальной информации

Подсистема обеспечения целостности должна:

1. Обеспечивать целостность программных средств системы защиты информации от НСД (СЗИ НСД), обрабатываемой информации, а также неизменность программной среды. При этом:
   - целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
   - целостность программной среды обеспечивается использованием трансляторов с языка высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.
2. Осуществлять физическую охрану СВТ (устройств и носителей информации). При этом должны предусматриваться контроль доступа в помещение АС посторонних лиц, а также наличие надёжных препятствий для несанкционированного проникновения в помещение АС и хранилище носителей информации. Особенно в нерабочее время.
3. Проводить периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест–программ, имитирующих попытки НСД.
4. Иметь в наличии средства восстановления СЗИ НСД. При этом предусматривается ведение двух копий программных средств СЗИ НСД, а также их периодическое обновление и контроль работоспособности.

2. Показатели защищённости АС

2.2. Требования к защите секретной информации

Подсистема управления доступом должна:

Пп.1–4 как для класса 1 Г.

5. Управлять потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителя должен быть **не ниже** уровня конфиденциальности записываемой на него информации.

Подсистема регистрации и учёта должна:

1. как для класса 1 Г.

2. Регистрировать выдачу печатных (графических) документов на «твёрдую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учётными реквизитами АС с указанием на последнем листе документа общего количества страниц. В параметрах регистрации указываются:

- то же, что для 1Г;
- объём фактически выданного документа (количество страниц, листов, копий) и результат выдачи (успешный – весь объём, неуспешный).

2. Показатели защищённости АС

2.2. Требования к защите секретной информации

3. как для класса 1 Г.

4. как для класса 1 Г. В параметрах регистрации указывается:
- как для класса 1 Г;
- имя программы (процесса, задания, задачи), осуществляющих доступ к файлам;
- вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.).

5. как для класса 1 Г. В параметрах регистрации указывается:
- как для класса 1 Г.;
- имя программы (процесса, задания, задачи), осуществляющих доступ к файлам;
- вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.).

6. Регистрировать изменения полномочий субъектов доступа, а также статуса объектов доступа. В параметрах регистрации указывается:
- дата и время изменения полномочий;
- идентификатор субъекта доступа (администратора), осуществившего изменения.

2. Показатели защищённости АС

2.2. Требования к защите секретной информации

7. Осуществлять автоматический учёт создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта.

8. Проводить учёт всех защищаемых носителей информации с помощью их маркировки и с занесением учётных данных в журнал (учётную карточку).

9. Проводить учёт защищаемых носителей с регистрацией их выдачи (приёма) в специальном журнале (картотеке).

10. Проводить несколько видов учёта (дублирующих) защищаемых носителей информации.

11. Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Причём очистка должна осуществляется **двукратной** произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

12. Сигнализировать о попытках нарушения защиты.

2. Показатели защищённости АС

2.2. Требования к защите секретной информации

Подсистема обеспечения целостности должна:

1. как для класса 1 Г.

2. Осуществлять физическую охрану СВТ (устройств и носителей информации). При этом должно предусматриваться постоянное наличие охраны на территории здания и помещений, где находится АС.

Охрана должна производиться с помощью технических средств охраны и специального персонала, а также с использованием строгого пропускного режима и специального оборудования в помещении АС.

3. Предусматривать наличие администратора или целой службы защиты информации, ответственных за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС.

4. Проводить периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью специальных программных средств не реже одного раза в год.

2. Показатели защищённости АС

2.2. Требования к защите секретной информации

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

6. Использовать только сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.