Практическая работа №5

Определение класса защиты информации в соответствии с Руководящими документами Гостехкомиссии России

Система защиты информации — совокупность взаимосвязанных средств, методов и мероприятий, направленных на предотвращение уничтожения, искажения, несанкционированного получения конфиденциальных сведений, отображенных полями, электромагнитными, световыми и звуковыми волнами или вещественно-материальными носителями в виде сигналов, образов, символов, технических решений и процессов.

Руководящий документ, подписанный по решению председателя Гостехкомиссии России 30 марта 1992 г. устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в ПК различных классов.

**Концепция защиты от несанкционированного доступа к информации**

Идейной основой набора "Руководящих документов" является "Концепция защиты СВТ и АС от *НСД* к информации". Концепция "излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от *НСД*, являющейся частью общей проблемы безопасности информации".

В "Концепции" различаются понятия средств вычислительной техники и автоматизированной системы, аналогично тому, как в "Европейских Критериях" проводится деление на продукты и системы. Более точно, "Концепция предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от *НСД*. Это - направление, связанное с СВТ, и направление, связанное с АС. Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации.

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

Существуют различные способы покушения на информационную безопасность: радиотехнические, акустические, программные и т.п. Среди них *НСД* выделяется как "доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС."

В "Концепции" формулируются следующие основные принципы защиты от *НСД* к информации:

"...Защита СВТ обеспечивается комплексом программно-технических средств.

Защита АС обеспечивается комплексом программнотехнических средств и поддерживающих их организационных мер.... Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

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

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

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

"Концепция" ориентируется на физически защищенную среду, проникновение в которую посторонних лиц считается невозможным, поэтому нарушитель определяется как "субъект, имеющий доступ к работе с штатными средствами АС и СВТ как части АС.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

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

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

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

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

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

В качестве главного средства защиты от *НСД* к информации в "Концепции" рассматривается система разграничения доступа (СРД) субъектов к объектам доступа. Основными функциями СРД являются:

* "реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;
* реализация ПРД субъектов и их процессов к устройствам создания твердых копий;
* изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
* управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;
* реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам."

Кроме того, "Концепция" предусматривает наличие обеспечивающих средств для СРД, которые выполняют следующие функции:

* "идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
* регистрацию действий субъекта и его процесса;
* предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
* реакцию на попытки *НСД*, например, сигнализацию, блокировку, восстановление после *НСД,* тестирование;
* очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
* учет выходных печатных и графических форм и твердых копий в АС;
* контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств."

Видно, что функции системы разграничения доступа и обеспечивающих средств, предлагаемые в "Концепции", по своей сути близки к аналогичным положениям "Оранжевой книги". Это вполне естественно, поскольку близки и исходные посылки - защита от несанкционированного доступа к информации в условиях физически безопасного окружения.

Технические средства защиты от *НСД*, согласно "Концепции", должны оцениваться по следующим основным параметрам:

* "степень полноты охвата ПРД реализованной СРД и ее качество;
* состав и качество обеспечивающих средств для СРД;
* гарантии правильности функционирования СРД и обеспечивающих ее средств."

Примечание. Средства СВТ могут рассматриваться как объекты НСД только при записи и хранении в них информации. "Голое" железо интерес для хакеров, как правило, не представляет.

**"Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности."**

Краткое содержание важнейшего документа "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности." В этом документе определены семь классов защищенности СВТ от НСД к информации. Самый низкий класс - седьмой, самый высокий первый. Каждый класс наследует требования защищенности предыдущего класса.

Изложенные ниже требования к показателям защищенности предъявляются к общесистемным программным средствам и операционным системам.

Совокупность всех средств СВТ защиты образует комплекс средств защиты (КСЗ).

В зависимости от реализованных моделей защиты и надежности их проверки классы подразделяются на четыре группы. Первая группа включает только один седьмой класс (минимальная защищенность).

Вторая группа характеризуется избирательной защитой и включает шестой и пятый классы. Избирательная защита предусматривает контроль доступа поименованных субъектов к поименованным объектам системы. При этом для каждой пары "субъект-объект" должны быть определены разрешенные типы доступа. Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

Третья группа характеризуется полномочной защитой и включает четвертый, третий и второй классы. Полномочная защита предусматривает присвоение каждому субъекту и объекту системы классификационных меток, указывающих место субъекта (объекта) в соответствующей иерархии. Классификационные метки на объекты устанавливаются пользователем системы или специально выделенным субъектом. Обязательным требованием для классов, входящих в эту группу, является реализация диспетчера доступа (в иностранной литературе - reference monitor, монитор ссылок). Контроль доступа должен осуществляться применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов. Решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и избирательными и полномочными правилами разграничения доступа (ПРД).

Четвертый класс характеризуется верифицированной защитой и содержит только первый класс.

Для присвоения класса защищенности система должна содержать руководство администратора по системе, руководство пользователя, тестовую и конструкторскую (проектную) документацию.

Перечень показателей по классам защищенности СВТ приведен в таблице 1. Их краткое описание приведено ниже.

Таблица 1. Показатели по классам защищенности СВТ Гостехкомиссии РФ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| №№ п/п | Наименование  Показателя | Класс защищенности | | | | | |
| C6 (С1) | C5 (С2) | 4 (B1) | 3 (В2) | 2 (В3) | 1 (А1) |
| Политика безопасности | | | | | | | |
| 1 | Избирательная политика безопасности | + | + | + | = | + | = |
| 2 | Полномочная политика безопасности | - | - | + | = | = | = |
| 3 | Повторное использование объектов | - | + | + | + | = | = |
| 4 | Изоляция модулей | - | - | + | = | + | = |
| 5 | Маркировка документов | - | - | + | = | = | = |
| 6 | Защита ввода и вывода на отчуждаемый физический носитель информации | - | - | + | = | = | = |
| 7 | Сопоставление пользователя с устройством | - | - | + | = | = | = |
| Учет | | | | | | | |
| 8 | Идентификация и аутентификация | + | = | + | = | = | = |
| 9 | Регистрация | - | + | + | + | = | = |
| 10 | Взаимодействие пользователя с КСЗ | - | - | - | + | = | = |
| Гарантии | | | | | | | |
| 11 | Гарантии проектирования | - | + | + | + | + | + |
| 12 | Гарантии архитектуры | - | - | - | - | - | + |
| 13 | Надежное восстановление | - | - | - | + | = | = |
| 14 | Целостность КСЗ | - | + | + | + | = | = |
| 15 | Контроль модификации | - | - | - | - | + | = |
| 16 | Контроль дистрибуции | - | - | - | - | + | = |
| 17 | Тестирование | + | + | + | + | + | = |
| Документация | | | | | | | |
| 18 | Руководство пользователя | + | = | = | = | = | = |
| 19 | Руководство по КСЗ | + | + | = | + | + | = |
| 20 | Тестовая документация | + | + | + | + | + | = |
| 21 | Конструкторская (проектная) документация | + | + | + | + | + | + |

Обозначения:

"-" - нет требований к данному классу;

"+" - новые или дополнительные требования,

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

Шестой класс защищенности

КСЗ этого класса должен предоставлять возможности санкционированного изменения ПРД, списка пользователей я и списка защищаемых объектов. Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.).

Перед работой пользователь должен пройти процедуру проверки подлинности (аутентификацию). По ее результатам ему присваиваются определенные права по доступу к объектам в системе (авторизация пользователя). Неавторизованный пользователь не должен иметь доступа к защищаемым ресурсам.

Пятый класс защищенности

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

В КСЗ этого класса должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

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

КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

* использование идентификационного и аутентификационного механизма;
* запрос на доступ к защищаемому объекту ;
* создание и уничтожение объекта;
* действия по изменению ПРД.

Для каждого из регистрируемых событий должны

* регистрироваться:
* 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.

Периодическому контролю целостности должны быть подвержены программная и информационная части КСЗ.

Четвертый класс защищенности

Проектирование КСЗ должно начинаться с построения модели защиты, включающей в себя непротиворечивые ПРД, непротиворечивые правила изменения ПРД и правила работы с устройствами ввода и вывода информации и каналами связи.

Защита должна осуществляться не только от "явных" (осуществляемых при помощи системных средств, языков высокого уровня), но и от скрытых (осуществляемых другим путем, в т.ч. и с использованием собственных программ работы с устройствами) запросов на получение доступа .

Кроме внешней памяти очистке должны быть подвержена и оперативная память при ее перераспределении.

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).

При выводе защищаемой информации на документ в начале и конце КСЗ должен проставить штамп установленного образца.

КСЗ должен различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные ("помеченные"). При вводе с "помеченного" устройства (выводе 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.

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

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

Для СВТ данного класса защищенности требования по регистрации дополнительно включают регистрацию попыток доступа, и всех действий оператора и выделенных пользователей (администраторов защиты и т.п.).

Программы КСЗ должны выполняться в отдельной части оперативной памяти.

Третий класс защищенности

На начальном этапе проектирования КСЗ должна строиться модель защиты, содержащая непротиворечивые правила изменения ПРД, правила работы с устройствами ввода и вывода и формальную модель механизма управления доступом.

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

Для обеспечения возможности изучения, анализа, проверки и модификации КСЗ должен быть хорошо структурирован, его структура должна быть модульной и четко определенной.

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

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

Необходимо осуществлять периодический контроль за целостностью КСЗ. Программы должны выполняться в отдельной части оперативной памяти.

Второй класс защищенности

ПРД избирательной защиты должны быть эквивалентны ПРД полномочной защиты.

Гарантии изоляции модулей различных субъектов должны быть основаны на архитектуре СВТ.

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.

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. Оригиналы программ должны быть защищены.

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

Первый класс защищенности

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

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

**Классификация автоматизированных систем по уровню защищенности от НСД**

Для автоматизированных систем как объединений средств СВТ ГТК РФ разработала специальную классификацию автоматизированных систем по уровню защищенности от НСД

Классификация автоматизированных систем устроена иначе. Снова обратимся к соответствующему "Руководящему документу".

"...устанавливается девять классов защищенности АС от *НСД* к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

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

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

... Третья группа классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - ЗБ и ЗА.

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

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А." В таблице 2 собраны требования ко всем девяти классам защищенности АС.

Таблица 2. Требования к защищенности автоматизированных систем.

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

Обозначения:

"- " - нет требований к данному классу;

"+" - есть требования к данному классу;

"СЗИ *НСД*" - система защиты информации от несанкционированного доступа.

Ниже приведено подробное изложение требований к достаточно представительному классу защищенности - 1В. По существу, перед нами - минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность защищаемой информации (реальные АС часто не соответствуют данному классу).

ТРЕБОВАНИЯ К КЛАССУ ЗАЩИЩЕННОСТИ 1В

Подсистема управления доступом:

должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов; должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и/или адресам; должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам; должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа; должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Подсистема регистрации и учета:

должна осуществляться регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова; должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию; должна осуществляться регистрация запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов; должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей; должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа; должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта; должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки; должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двухкратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации; должна осуществляться сигнализация попыток нарушения защиты.

Подсистема обеспечения целостности:

должна быть обеспечена целостность программных средств СЗИ *НСД*, а также неизменность программной среды, при этом: целостность СЗИ *НСД* проверяется при загрузке системы по контрольным суммам компонент СЗИ, целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке и (или) хранении защищаемой информации; должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС; должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ *НСД*. Администратор должен иметь свой терминами и необходимые средства оперативного контроля и воздействия на безопасность АС; должно проводиться периодическое тестирование всех функций СЗИ *НСД* с помощью специальных программных средств не реже одного раза в год; должны быть в наличии средства восстановления СЗИ *НСД*, предусматривающие ведение двух копий программных средств СЗИ НОД и их периодическое обновление и контроль работоспособности; должны использоваться сертифицированные средства защиты."

**Пример**

Категория информации, обрабатываемой в информационных системах аэропорта практически во всех случаях относится к служебной тайне. Такая информация принадлежит грифу конфиденциально и предназначена для служебного пользования.

Помимо важности обрабатываемой информации, важную роль в определение класса защищенности играют последствия от ее утечки или кражи. Кража такой информации может привести к финансовым потерям, нарушения юридических прав клиентов данной организации и даже катастрофам.

АСУ аэропорта является многопользовательской, существует раздельный контроль доступа к различным уровням системы и имеет выход в интернет.

Исходя из определяющих признаков можно отнести рассматриваемую информационную систему к первой группе. Первая группа включает многопользовательские ИС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АСУ.

Информационная система аэропорта имеет класс защищенности 1Г.

**Практическая часть**

Прежде чем приступать к определению класса защиты информации в соответствии с Руководящими документами Гостехкомиссии России необходимо четко определиться является ли ваш объект защиты – СВТ или АС, и обосновать это. Только потом переходить к определению класса защиты информации