Тесты кафедры анатомии человека МГМСУ им. А.И. Евдокимова

Министерство образования и науки Российской Федерации
Пермский национальный исследовательский политехнический университет
Кафедра информационные технологии и автоматизированные системы
Контрольная работа
по дисциплине «Основы автоматизированного управления»
«Защита информации в автоматизированных системах»
Выполнил:
студент группы АСУ-11-2бзу
Моздоков Дмитрий Сергеевич
Проверил: профессор кафедры ИТАС
Файзрахманов Рустам Абубакирович
Пермь 2013
Оглавление

Введение

Информационная безопасность - сравнительно молодая, быстро развивающаяся область информационных технологий. Словосочетание информационная безопасность в разных контекстах может иметь различный смысл. Состояние защищенности национальных интересов в информационной сфере определяется совокупностью сбалансированных интересов личности, общества и государства. Под информационной безопасностью понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.
Вместе с тем, защита информации - это комплекс мероприятий направленных на

обеспечение информационной безопасности.
Не стоит, однако, забывать об экономической целесообразности применения тех или иных мер обеспечения безопасности информации, которые всегда должны быть адекватны существующим угрозам.
В данном реферате необходимо отобразить :
1. Классификацию автоматизированных систем
2. Причины защиты информации
3. Меры защиты информации
4. Требования по защите информации
5. Технологии администрирования защиты информации.
1. Классификация автоматизированных систем

1.1. Классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.
1.2. Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.
1.3. Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.
1.4. Основными этапами классификации АС являются:
1. разработка и анализ исходных данных;
2. выявление основных признаков АС, необходимых для классификации;
3. сравнение выявленных признаков АС с классифицируемыми;
4. присвоение АС соответствующего класса защиты информации от НСД.
1.5. Необходимыми исходными данными для проведения классификации конкретной АС являются:
1. перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
2. перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
3. матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
4. режим обработки данных в АС.
1.6. Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.
1.7. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:
1. наличие в АС информации различного уровня конфиденциальности;
2. уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

3. режим обработки данных в АС - коллективный или индивидуальный.
1.8. Устанавливается девять классов защищенности АС от НСД к информации.
1. Каждый класс характеризуется определенной минимальной совокупностью требований по защите.
2. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.
3. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.
1.9. Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.
Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.
Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А. [5,6,7,8]
2. Причины защиты информации в автоматизированных системах

Состояние защищённости информации с помощью совокупности программных, аппаратно-программных средств и методов, а также организационных мер с целью сохранения таких ее качественных характеристик (свойств), как секретность (конфиденциальность), целостность и доступность. Секретность (конфиденциальность) информации заключается в предотвращении несанкционированного ознакомления с ней или документирования (снятия копий). Целостность информации при ее обработке техническими средствами АСУ состоит в предотвращении ее несанкционированной модификации или уничтожения. Доступность информации - это возможность беспрепятственного доступа к информации для проведения санкционированных операций по ознакомлению с ней, документированию, модификации и уничтожению.
Безопасность информации в АСУ обеспечивается способностью этой системы сохранять конфиденциальность информации при ее вводе, выводе, передаче, обработке и хранении, а также противостоять ее разрушению, хищению или искажению. Объектом защиты в АСУ являются данные, содержащие конфиденциальные (секретные) сведения, которые хранятся, обрабатываются и передаются между элементами автоматизированной системы управления. Основными факторами опасности для информации, обрабатываемой техническими средствами АСУ, являются: побочные электромагнитные излучения и наводки, возникающие в результате нелинейных процессов в электрических цепях; несанкционированный доступ (НСД) к информации штатными техническими

средствами с нарушением установленных правил; специальные электронные закладные устройства - электронные устройства, несанкционированно установленные в технические средства; внешние воздействия на информационный ресурс (стихийные бедствия, электромагнитное излучение, диверсионные акты и т.п.).

Для защиты информации создается организационно-техническая система обеспечения безопасности информации (ОБИ), которая включает комплекс организационных мероприятий, а также технические, программные и криптографические средства защиты. Функционирование системы обеспечения безопасности информации регламентируется правовыми и законодательными актами РФ.

Защита информации осуществляется с помощью средств, методов и организационных мероприятий, исключающих несанкционированный доступ к конфиденциальной информации, ее раскрытие, изменение, уничтожение или хищение. Для защиты информации создается система защиты информации, которая включает: физические и технические (программные и аппаратные) средства защиты; организационные мероприятия; совокупность (комплекс) специальных мер правового (законодательного) и административного характера; специальный персонал, выполняющий функции обеспечения безопасности автоматизированных систем (АС) (циркулирующей в АС информации). Система должна предупреждать несанкционированный доступ к хранящейся, обрабатываемой или передаваемой информации с целью ее неразрешенного использования, преднамеренного искажения, или уничтожения.

Как правило, обеспечение безопасности информации достигается созданием административно-технической службы ОБИ (службы защиты), которая должна осуществлять такие функции, как: идентификация и установление подлинности пользователей (доступ в информационную систему только авторизованных лиц); управление доступом (использование ресурсов информационной системы разрешенным способом); обеспечение конфиденциальности данных и сообщений. С этой целью в службе ОБИ организуются подсистемы управления доступом, регистрации и учета, обеспечение целостности и др. Каждая из этих подсистем представляет собой совокупность механизмов, проце-дур и других управляющих воздействий для сокращения риска, связанного с угрозой искажения или уничтожения информации.

Эффективность ОБИ в АСУ зависит от того, насколько действенны и всеобъемлющи применяемые в системе методы и средства. [1,3]

3. Меры защиты информации

Физическая система защиты системы и данных может осуществляться только в отношении рабочих ЭВМ и узлов связи и оказывается невозможной для средств передачи, имеющих большую протяженность. По этой причине в ИВС должны использоваться средства, исключающие несанкционированный доступ к данным и обеспечивающие их секретность.

Неизбежным средством борьбы с этой опасностью стали постоянно увеличивающиеся расходы на защиту информации. Например, по оценке немецких экспертов лишь в 1987 году в промышленности и учебных заведениях Западной Европы потрачено
1 к 7 млрд марок на обеспечение безопасности компьютеров.
Исследования практики функционирования систем обработки информации и вычислительных систем доказали, что существует достаточно много возможных направлений утечки информации и путей несанкционированного доступа в системах и сетях.
В их числе:
— чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
— копирование носителей и файлов информации с преодолением мер защиты;
— маскировка под зарегистрированного пользователя;
— маскировка под запрос системы;
— использование программных ловушек;
— использование недостатков операционной системы;
— незаконное подключение к аппаратуре и линиям связи;
— злоумышленный вывод из строя механизмов защиты;
— внедрение и использование компьютерных вирусов.
Обеспечение безопасности информации в ИВС и в автономно работающих ПЭВМ достигается комплексом организационных, организационно-технических, технических и программных мер.
К организационным мерам защиты информации относятся:
— ограничение доступа в помещения, в которых происходит подготовка и обработка информации;
— доступ к обработке и передаче конфиденциальной информации только проверенных должностных лиц;
— хранение магнитных носителей и регистрационных журналов в закрытых для доступа посторонних лиц сейфах;
— исключение просмотра посторонними лицами содержания обрабатываемых материалов через дисплей, принтер и т.д.;
— использование криптографических кодов при передаче информации по каналам связи ценной информации;
— уничтожение красящих лент, бумаги и иных материалов, содержащих фрагменты ценной информации.
Организационно-технические меры зашиты информации включают:
— осуществление питания оборудования, обрабатывающего ценную информацию от независимого источника или через специальные фильтры;
— установку на дверях помещений кодовых замков;
— использование для отображения информации при вводе- выводе жидкокристаллических или плазменных дисплеев, а для получения твердых копий -- струйных принтеров и термопринтеров, поскольку дисплей дает такое

высокочастотное электромагнитное излучение, что изображение с его экрана можно принимать на расстоянии нескольких сотен километров;
— уничтожение информации, хранящейся в ОЗУ и на «винчестере» при списании или отправке ПЭВМ в ремонт;
— установка клавиатуры и принтеров на мягкие прокладки с целью снижения возможности снятия информации акустическим способом;
— ограничение электромагнитного излучения путем экранирования помещений, где происходит обработка информации, листами из металла или специальной пластмассы.
Технические средства защиты информации -- это системы охраны территорий и помещений с помощью экранирования машинных залов и организация контрольно-пропускных систем.
Защита информации в сетях и вычислительных средствах с помощью технических средств реализуется на основе организации доступа к памяти с помощью:
— контроля доступа к различным уровням памяти компьютера;
— блокировки данных и ввода ключей;
— выделения контрольных битов для записей с целью идентификации и др.
Архитектура программных средств защиты информации включает:
— контроль безопасности, в том числе и контроль регистрации вхождения в систему, фиксацию в системном журнале, контроль действий пользователя;
— реакцию, в том числе звуковую, на нарушение системы защиты контроля доступа к ресурсам сети;
— контроль мандатов доступа;
— формальный контроль защищенности операционных систем (базовой операционной и сетевой);
— контроль алгоритмов защиты;
— проверку и подтверждение правильности функционирования технического и программного обеспечения.
Для надежной защиты информации и выявления случаев неправомочных действий проводится регистрация работы системы: создаются специальные дневники и протоколы, в которых фиксируются все действия, имеющие отношение к защите информации в системе. Фиксируются время поступления заявки, ее тип, имя пользователя и терминала, с которого инициализируется заявка. При отборе событий, подлежащих регистрации, необходимо иметь в виду, что с ростом количества регистрируемых событий, затрудняется просмотр дневника и обнаружение попыток преодоления защиты. В этом случае можно применять программный анализ и фиксировать сомнительные события.
Используются также специальные программы для тестирования системы защиты. Периодически или в случайно выбранные моменты времени они проверяют работоспособность аппаратных и программных средств защиты.
К отдельной группе мер по обеспечению сохранности информации и выявлению несанкционированных запросов относятся программы обнаружения нарушений в режиме реального времени. Программы данной группы формируют специальный

сигнал при регистрации действий, которые могут привести к неправомерным действиям по отношению к защищаемой информации. Сигнал может содержать информацию о характере нарушения, месте его возникновения и другие характеристики. Кроме того, программы могут запретить доступ к защищаемой информации или симулировать такой режим работы (например, моментальная загрузка устройств ввода-вывода), который позволит выявить нарушителя и задержать его соответствующей службой.

Один из распространенных способов защиты -- явное указание секретности выводимой информации. В системах, поддерживающих несколько уровней секретности, вывод на экран терминала или печатающего устройства любой единицы информации (например, файла, записи или таблицы) сопровождается специальным грифом с указанием уровня секретности. Это требование реализуется с помощью соответствующих программных средств.

В отдельную группу выделены средства зашиты от несанкционированного использования программного обеспечения. Они приобретают особое значение вследствие широкого распространения персональных компьютеров. Исследования, проведенные зарубежными исследователями, свидетельствуют, что на одну проданную копию оригинальной программы приходится минимум одна нелегальная. А для особо популярных программ это соотношение достигает 1:7.

Особое внимание уделяется законодательным средствам, регулирующим использование программных продуктов. В соответствии с Законом Российской Федерации об информации, информатизации и защите информации от 25 января 1995 года предусматриваются санкции к физическим и юридическим лицам за нелегальное приобретение и использование программных продуктов.

Большую опасность представляют компьютерные вирусы.

Компьютерный вирус -- это специально написанная небольшая по размерам программа, которая может приписывать себя к другим программам (т.е. «заражать» их), а также выполнять различные нежелательные действия. Программа, внутри которой находится компьютерный вирус, называется зараженной. Когда такая программа начинает работу, то сначала управление получает вирус, который находит и заражает другие программы, а также выполняет ряд вредных действий, в частности «засоряет» активную память, портит файлы и т. д.

Для маскировки вируса его действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении каких-либо условий. После того, как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает как обычно, т. е. внешне работа зараженной программы какое-то время не отличается от работы незараженной программы.

Действия вируса могут выполняться достаточно быстро и без выдачи сообщений, поэтому пользователь часто и не замечает, что компьютер работает несколько странно. Однако по прошествии некоторого времени, на компьютере может происходить следующее:

— некоторые программы перестают работать или работают неправильно;

— на экран выводятся посторонние сообщения, символы, рисунки и т. д.;
— работа на компьютере существенно замедляется;
— некоторые файлы оказываются испорченными и т.д.
Многие вирусы устроены так, что при запуске зараженной программы они остаются постоянно (точнее, до перезагрузки ОС) в памяти компьютера и время от времени заражают программы. Кроме того, зараженные программы с данного компьютера могут быть перенесены с помощью дискет или по локальной сети на другие компьютеры.
Если не принимать мер по защите от вируса, то последствия заражения вирусом компьютера могут быть серьезными. В число средств и методов защиты от компьютерных вирусов входят:
— общие средства защиты информации, которые полезны так же, как и страховка от физической порчи машинных дисков, неправильно работающих программ или ошибочных действий пользователя;
— профилактические меры, позволяющие уменьшить вероятность заражения вирусов;
— специализированные программы для защиты от вирусов.
Комплексное решение вопросов безопасности ИВС принято именовать архитектурой безопасности, где выделяются угрозы безопасности, службы безопасности и механизмы обеспечения безопасности.
Под угрозой безопасности понимается событие или действие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую и обрабатываемую информацию, а также программные и аппаратные средства.
Угрозы распределяются на случайные (непреднамеренные) и умышленные. Источником первых могут быть ошибки в ПО, неправильные действия пользователей, выход из строя аппаратных средств и др.
Умышленные угрозы преследуют цель нанесения ущерба пользователям (абонентам) вычислительной сети и подразделяются на активные и пассивные. Пассивные угрозы не разрушают информационные ресурсы и не оказывают влияния на функционирование ИВС. Их задача -- несанкционированно получить информацию. Активные угрозы преследуют цель нарушить процесс функционирования ИВС путем разрушения или радиоэлектронного подавления линий связи ИВС, вывода из строя ЭВМ или ее операционной системы, искажения баз данных и т. д. Источником активных угроз могут быть непосредственные действия людей -- злоумышленников, компьютерные вирусы и т. д.
Служба безопасности вычислительной сети призвана обеспечить:
— подтверждение подлинности того, что объект, который предлагает себя в качестве отправителя информации в сети, действительно им является;
— целостность информации, выявляя искажения, вставки, повторы и уничтожение данных, передаваемых в сетях, а также последующее восстановление данных;
— секретность всех данных, передаваемых по сетям;
— нейтрализацию всех попыток несанкционированного использование ресурсов

ЭВМ. При этом контроль доступа может быть избирательным, т.е. распространяться только на некоторые виды доступа к ресурсам, например, на обновление информации в базе данных, либо полным;
— получателя информации доказательствами, что информация получена от данного отправителя, несмотря на попытки отправителя отрицать факт отправления;
К механизмам обеспечения безопасности относятся:
— идентификация пользователей;
— шифрование данных;
— электронная подпись;
— управление маршрутизацией и др.
Идентификация пользователей позволяет устанавливать конкретного пользователя, работающего за терминалом и принимающего или отправляющего сообщения. Право доступа к определенным вычислительным и информационным ресурсам, программам и наборам данных, а также ВС в целом предоставляется ограниченному контингенту лиц, и система должна распознавать пользователей, работающих за терминалами. Идентификация пользователей чаще всего производится с помощью паролей.
Пароль -- это совокупность символов, известных подключенному к сети абоненту, вводится в начале сеанса взаимодействия с сетью, а иногда и в конце сеанса (в особо ответственных случаях пароль выхода из сети может отличаться от входного). Система может предусматривать ввод пароля для подтверждения правомочия пользователя через определенные интервалы времени.
Для защиты средств идентификации пользователей от неправомочного использования, пароли передаются и сравниваются в зашифрованном виде, а таблицы паролей хранятся в зашифрованном виде, что исключает возможность прочтения паролей без знания ключа.
Для идентификации пользователей могут применять и физические методы: например, карточка с магнитным покрытием, на котором записывается персональный идентификатор пользователя или карточка со встроенным чипом. Наиболее надежным, хотя и наиболее сложным является способ идентификации пользователя на основе анализа его индивидуальных параметров: отпечатков пальцев, рисунков линий руки, радужной оболочки глаз и др.
Шифрование данных -- это обеспечение секретности методами криптографии, т. е. методами преобразования данных из общепринятой формы в кодированную (шифрование) и обратного преобразования (дешифрования) на основе правил, известных только взаимодействующим абонентам сети. Криптография применяется для защиты передаваемых данных, а также информации, хранимой в базах данных, на магнитных и оптических дисках и т. д.
К криптографическим средствам предъявляются требования сохранения секретности, даже когда известна сущность алгоритмов шифрования -- дешифрования. Секретность обеспечивается введением в алгоритмы специальных ключей (кодов). Зашифрованный текст превращается в исходный только в том случае, когда в процессе шифрования и дешифрования используется один и тот же

ключ. Область значений ключа выбирается столь большой, что практически исключается возможность его определения путем простого перебора.[4 стр. 595]
4. Требования по защите информации от несанкционированного доступа для автоматизированных систем
4.1. Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.
4.2. В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:
управления доступом;
регистрации и учета;
криптографической;
обеспечения целостности.
5. Технологии администрирования
Часть угроз безопасности информации возникает из-за непреднамеренных (или преднамеренных) ошибок на этапах жизненного цикла АИС -- при разработке программного обеспечения СУБД; при проектировании и создании на базе СУБД конкретной АИС, и, в том числе, при проектировании системы разграничения доступа; при администрировании и сопровождении системы и, в том числе, при реагировании и действиях пользователей во внештатных ситуациях; при технологических операциях по резервированию, архивированию и восстановлению информации после сбоев; при выводе АИС из эксплуатации. С целью нейтрализации или снижения вероятности данных угроз применяются ряд организационно-технологических и технических средств, решений, объединяемых в общую группу технологий надежного проектирования и администрирования. Их также условно можно разделить на следующие подгруппы:
• технологии надежной разработки программного обеспечения;
• технологии надежного проектирования и создания АИС;
• технические средства и специальный инструментарий администрирования АИС;
• протоколирование и аудит процессов безопасности.
Технологии надежной разработки программного обеспечения включают общие подходы к снижению ошибок при разработке программного кода и ряд более специфических аспектов, основанных на изначальном учете в концепции и структуре ядра системы (подсистема представления данных и подсистема доступа к данным) той или иной модели и технологий безопасности данных. Как показывает анализ выявленных уязвимостей в системах безопасности компьютерных систем, вероятность наличия и нахождения злоумышленниками брешей существенно выше в тех случаях, когда системы защиты реализуются в виде надстройки или внешней оболочки над ядром и интерфейсом исходных незащищенных систем.

Технологии надежного проектирования и создания на базе программного обеспечения СУБД конкретных АИС направлены на предотвращение логических ошибок в информационной инфраструктуре систем и в подсистемах разграничения доступа, строящихся на основе поддерживаемой СУБД модели и технологий безопасности данных. В этом отношении основным и широко распространенным является структурно-функциональный подход.

При наличии большого количества пользователей (субъектов) и объектов информационных систем (баз данных) схема разграничения доступа может быть очень сложной и запутанной, что создает трудности для администрирования и порождает предпосылки для логических ошибок. Для преодоления этой угрозы в рамках структурно-функционального подхода применяют технику рабочих групп. Рабочая группа объединяет пользователей, имеющих какое-либо общее технологическое отношение к базе данных (выполняющих похожие операции) и близкие параметры конфиденциальности по отношению к общим данным. Администратор системы может создавать рабочие группы, рассматривая их как коллективных пользователей, с определенной идентификацией и набором полномочий, т.е. с созданием специальных учетных записей для рабочих групп. Каждый пользователь обязательно должен являться членом какой-либо рабочей группы. Полномочия, определенные для рабочей группы, автоматически распространяются на всех пользователей -- членов группы, что является отражением некоторых элементов зонально-функционального принципа разграничения доступа. Дополнительно для каждого пользователя в его личной учетной записи могут быть уточнены и конкретизированы его полномочия.

Такой подход позволяет в большинстве случаев существенно уменьшить количество субъектов доступа в системе, сделать схему разграничения доступа более простой, «прозрачной» ч управляемой, и тем самым снизить вероятность таких логических ошибок как неправильное предоставление доступа конкретного пользователя к конкретному объекту, превышение полномочий конкретного пользователя по доступу к ряду объектов, предоставление избыточных прав доступа и т.п. Процессы в базе данных в технологиях рабочих групп помечаются как меткой пользователя, так и меткой рабочей группы, и, соответственно ядро безопасности СУБД проверяет подлинность обеих меток.

Проектирование системы доступа на основе технологии рабочих групп может проводиться «сверху» (дедуктивно) и «снизу» (индуктивно).

В первом способе сначала на основе анализа функциональной структуры и организационной иерархии пользователей (субъектов) формируются рабочие группы и осуществляются групповые назначения доступа. Далее каждый пользователь при его регистрации в системе включается в состав одной или нескольких групп, отвечающих его функциям. И, наконец, в заключение для каждого пользователя анализируются особенности его функциональных потребностей и доверительных характеристик и при необходимости осуществляются индивидуальные дополнительные назначения доступа. Формирование групп, групповые и индивидуальные установки доступа при этом осуществляются

администратором системы, что соответствует принудительному способу управления доступом.
Такой подход позволяет снизить вероятность ошибочных назначений доступа и обеспечивает жесткую централизованную управляемость системой доступа, но может порождать, в свою очередь, дублирование групповых и индивидуальных полномочий доступа субъектов к объектам (проблема дублирования), а также избыточность доступа субъекта к одним и тем же объектам через участие в разных группах (проблема пересечения групп или в более широком смысле проблема оптимизации групп).
При втором (индуктивном) способе проектирования рабочих групп первоначально осуществляются индивидуальные назначения доступа субъектов (пользователей) к объектам. Назначения производятся на основе опроса и анализа функциональных потребностей и доверительных характеристик пользователей, и могут осуществляться администратором системы (принудительный способ управления доступом) или через индивидуальные запрашивания субъектами доступа владельцев объектов (принцип добровольного управления доступом). Далее, уже администратором системы, производится анализ общих или схожих установок доступа у различных субъектов, на основе которого они объединяются в рабочие группы. Выделенные общие установки доступа используются в качестве групповых назначений доступа. При этом анализ схожести доступа при большом количестве субъектов и объектов представляет непростую задачу и решается администратором системы в значительной степени эвристически.
Дополнительным организационным способом повышения надежности и безопасности в процессе администрирования и сопровождения системы является разделение общего администрирования и администрирования безопасности. Общий администратор строит, поддерживает и управляет информационной инфраструктурой системы -- информационно-логическая схема, категорирование конфиденциальности объектов (ресурсов и устройств), интерфейсные и диалоговые элементы, формы, библиотеки запросов, словарно-классификационная база, резервирование и архивирование данных. Администратор безопасности организует и управляет системой разграничения доступа -- доверительные характеристики (допуска) пользователей, конкретные назначения доступа, регистрация и формирование меток доступа пользователей.
Доступ к массиву учетных записей пользователей имеет только администратор безопасности. Совмещение функций общего администрирования и администрирования безопасности одновременно одним пользователем не допускается, что объективно повышает надежность системы. автоматизированный безопасность несанкционированный
Протоколирование и аудит событии безопасности являются важным средством обеспечения управляемости состоянием и процессами безопасности, создают условия для расследования фактов нарушения информационной безопасности, анализа и исключения их причин, снижения отрицательных последствий и ущерба от них.

Документированию подлежат все события, критичные с точки зрения безопасности в системе:
• вход/выход пользователей;
• регистрация новых пользователей, смена привилегий и назначений доступа (все обращения к массивам учетных записей);
• все операции с файлами (создание, удаление, переименование, копирование, открытие, закрытие);
• обращения к/из удаленной системе(ы).
При этом по каждому такому событию устанавливается минимально необходимый перечень регистрируемых параметров, среди которых:
• дата и время события;
• идентификатор пользователя-инициатора;
• тип события;
• источник запроса (для распределенных систем -- сетевое имя терминала, рабочей станции и т. п.);
• имена затронутых объектов;
• изменения, внесенные в учеты в системы, в том числе в массивы учетных записей;
• метки доступа субъектов и объектов.
В СУБД такой подход хорошо вписывается в событийно-процедурную технологию с использованием техники журнализации. При этом доступ к журналу событий имеет только администратор безопасности, который при обнаружении фактов или признаков нарушений безопасности имеет возможность восстановления хода событий, анализа и устранения источников и причин нарушения безопасности системы.
В этом отношении журнал событий безопасности является необходимым средством аудита безопасности. Аудит безопасности заключается в контроле и отслеживании событий в системе с целью выявления, своевременного обнаружения проблем или нарушений безопасности и сигнализации об этом администратору безопасности. Ввиду того что процессы доступа, различных процедур, операций, информационных потоков в компьютерных системах являются многоаспектными, не строго детерминированными, т. е. частично или полностью стохастическими, разработка аналитических, алгоритмических или иным образом аналитических автоматизированных процедур обнаружения фактов и признаков нарушений информационной безопасности является чрезвычайно сложной и неопределенной задачей. Поэтому в настоящее время разрабатывается ряд эвристических и нейросетевых технологий, которые в некоторых случаях с успехом воплощаются в специальном программном инструментарии администратора безопасности, обеспечивая автоматизированный аудит безопасности системы. [2 стр 159]
Заключение

Мы рассмотрели поставленные задачи :
1. Классификацию автоматизированных систем
2. Причины защиты информации

3. Меры защиты информации
4. Требования по защите информации
5. Технологии администрирования защиты информации.
Изучили основные проблемы безопасности автоматизированных систем и их классы.
Проанализировали ГОСТы и руководящие документы по стандартизации АСУ.
Список литературы

1. Гайдамакин Н. А. Автоматизированные информационные системы, базы и банки данных. Вводный курс: Учебное пособие. -- М.: Гелиос АРВ, 2002.
2. Герасименко В.А.. Защита информации в автоматизированных системах обработки данных. В 2-х кн.: Кн. 1. - М.: Энергоатомиздат, 1994
3. Ларин А.А. Теоретические основы управления. Часть 6. Автоматизация управленческой деятельности. - М.: РВСН, 2000
4. Меньков А.В. Теоретические основы автоматизированного управления/ А.В. Меньков, В.А.Острейковский. - Учебник для вузов. - М.: Издательство Оникс, 2005.
5. ГОСТ 34.003-90
6. ГОСТ 34.601-90
7. РД 50-680-88
8. РД 50-34.680-90...