3. ПРИМЕНЕНИЕ СЗИ ОТ НСД ДЛЯ ОРГАНИЗАЦИИ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

3.1. Меры противодействия несанкционированному доступу

В пункте 1.2 пособия были перечислены основные меры по защите информации в компьютерной системе. Большинство из них направлено на обеспечение безопасности КИ от несанкционированного доступа. Эти меры можно назвать каноническими, они в той или иной мере реализованы в распространенных универсальных и специализированных операционных системах. Для неискушенных читателей, прежде чем перейти к изучению аппаратно-программных средств защиты от НСД, дополняющих классические компьютерные системы, целесообразно познакомиться с некоторыми теоретическими и практическими правилами предотвращения несанкционированного доступа.

3.1.1. Идентификация и аутентификация пользователей

Для гарантии того, чтобы только зарегистрированные в АС пользователи могли включить компьютер (загрузить операционную систему) и получить доступ к его ресурсам, каждый доступ к данным в защищенной АС осуществляется в три этапа: идентификация — аутентификация — авторизация.

Идентификация — присвоение субъектам и объектам доступа зарегистрированного имени, персонального идентификационного номера (PIN-кода), или идентификатора, а также сравнение (отождествление) предъявляемого идентификатора с перечнем присвоенных (имеющихся в АС) идентификаторов. Основываясь на идентификаторах, система защиты «понимает», кто из пользователей в данный момент работает на ПЭВМ или пытается включить компьютер (осуществить вход в систему). *Аутентификация* определяется как проверка принадлежности субъекту доступа предъявленного им идентификатора, либо как подтверждение подлинности субъекта. Во время выполнения этой процедуры АС убеждается, что пользователь, представившийся каким-либо легальным сотрудником, таковым и является. *Авторизация* — предоставление пользователю полномочий в соответствии с политикой безопасности, установленной в компьютерной системе.

Процедуры идентификации и аутентификации в защищенной системе осуществляются посредством специальных программных (программно-аппаратных) средств, встроенных в ОС или СЗИ. Процедура идентификации производится при включении компьютера и заключается в том, что сотрудник «представляется» компьютерной системе. При этом АС может предложить сотруднику выбрать свое имя из списка зарегистрированных пользователей или правильно ввести свой идентификатор. Далее пользователь должен убедить АС в том, что он действительно тот, кем представился. Аутентификация в защищенных АС может осуществляться несколькими методами:

- парольная аутентификация (ввод специальной индивидуальной для каждого пользователя последовательности символов на клавиатуре);

- на основе биометрических измерений (наиболее распространенными методами биометрической аутентификации пользователей в СЗИ являются чтение папиллярного рисунка и аутентификация на основе измерений геометрии ладони, реже встречаются голосовая верификация и считывание радужной оболочки или сетчатки глаз);
- с использованием физических носителей аутентифицирующей информации.

Наиболее простым и дешевым способом аутентификации личности в АИС является ввод пароля (трудно представить себе компьютер без клавиатуры). Однако существование большого количества различных по механизму действия атак на систему парольной защиты делает ее уязвимой перед подготовленным злоумышленником. Биометрические методы в СЗИ пока не нашли широкого применения. Непрерывное снижение стоимости и миниатюризация, например, дактилоскопических считывателей, появление «мышек», клавиатур и внешних флеш-носителей со встроенными считывателями неминуемо приведет к разработке средств защиты с биометрической аутентификацией.

В настоящее время для повышения надежности аутентификации пользователей в СЗИ применяют внешние носители ключевой информации. В технической литературе производители этих устройств и разработчики систем безопасности на их основе пользуются различной терминологией. Можно встретить подходящие по контексту термины: *электронный идентификатор*, *электронный ключ*, *внешний носитель ключевой или кодовой (аутентифицирующей) последовательности*. Следует понимать, что это устройства внешней энергонезависимой памяти с различным аппаратным интерфейсом, работающие в режимах чтение или чтение/запись и предназначенные для хранения ключевой (для шифрования данных) либо аутентифицирующей информации. Наиболее распространенными устройствами являются электронные ключи «Touch Memory» на базе микросхем серии DS199X фирмы Dallas Semiconductors. Другое их название — «iButton» или «Далласские таблетки» (устройства выпускаются в цилиндрическом корпусе диаметром 16 мм и толщиной 3 или 5 мм, рис. 3.1).

Рис. 3.1. Внешний вид электронного ключа iButton и считывателя информации

В СЗИ активно используются пластиковые карточки различных технологий (чаще всего с магнитной полосой или проксими-карты, рис. 3.2). Пластиковые карточки имеют стандартный размер 54х85,7х0,9 — 1,8 мм.

Рис. 3.2. Пластиковая карта с магнитной полосой

Удобными для применения в СЗИ являются электронные ключи eToken (рис. 3.3), выполненные на процессорной микросхеме семейства SLE66C Infineon, обеспечивающей высокий уровень безопасности. Они предназначены для безопасного хранения секретных данных, например, криптографических ключей. eToken выпускается в двух вариантах конструктивного оформления: в виде USB-ключа и в виде смарт-карты стандартного формата.

В большинстве программно-аппаратных средств защиты информации предусмотрена возможность осуществлять аутентификацию личности пользователя комбинированным способом, т. е. по нескольким методам одновременно. Комбинирование способов аутентификации снижает риск ошибок, в результате которых злоумышленник может войти в систему под именем легального пользователя.

Рис. 3.3. Электронные ключи eToken

3.1.2. Ограничение доступа на вход в систему

Прежде всего, еще раз напомним, что ограничение доступа к ресурсам АС начинается с ограничения *физического* доступа сотрудников и «гостей» предприятия в помещение, в котором размещаются и функционируют элементы компьютерной системы. Этот рубеж защиты организуется путем установки средств инженерной укрепленности помещений, автономных устройств охранной сигнализации, телевизионных систем наблюдения, устройств защиты рабочего места и непосредственно ПЭВМ и к функционированию программных и аппаратных СЗИ отношения не имеет.

В практике защиты объектов информатизации под методом «ограничение доступа на вход в систему» имеют в виду целый комплекс мер, выполняемых в процессе загрузки операционной системы. Поэтому для описания процесса правильного и легального включения компьютера специалисты часто используют термин «доверенная загрузка ОС». Правильно организованная доверенная загрузка обеспечивает выполнение 1, 2 и отчасти третьего пунктов требований к системе защиты информации, сформулированных в п. 1.1. пособия.

Благодаря процедурам идентификации и аутентификации АС разрешает дальнейшую работу только зарегистрированным пользователям в именованном режиме. Однако для всецело доверенной загрузки этого не достаточно. Безопасный вход в компьютерную систему включает в себя также процедуру ограничения доступа по дате и времени, процедуру проверки целостности системного программного обеспечения и аппаратуры, а также защиту от загрузки ОС со съемных носителей и входа в АС в незащищенном режиме. Первая из этих мер помимо поддержания дисциплины (что необходимо на предприятии, где обрабатывается информация ограниченного доступа) обеспечивает дополнительную защиту от злоумышленников, пытающихся атаковать АС во внерабочее время.

Одной из встроенных в программно-аппаратную среду самого компьютера процедур ограничения *логического* доступа является операция ввода пароля BIOS при включении ПЭВМ. Чтобы понять, какое место в комплексе защитных мер занимает парольная защита, рассмотрим процесс загрузки персонального компьютера без использования СЗИ (рис. 3.4).

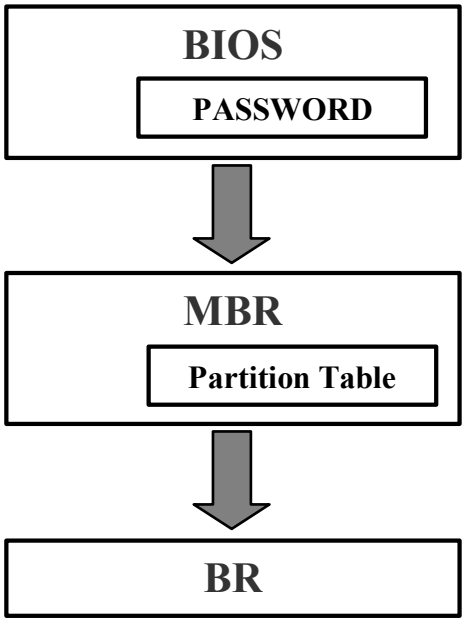


Рис. 3.4. Процесс стандартной загрузки персонального компьютера

При включении питания управление ПЭВМ берет на себя программа, записанная в ПЗУ BIOS, которая проводит процедуру самотестирования компьютера (Power-On Self-Test, POST). После тестирования из ПЗУ BIOS в оперативную память ПЭВМ загружается содержимое первого сектора нулевого цилиндра нулевой стороны накопителя на жестком магнитном диске (НЖМД). В данном секторе НЖМД находится главная загрузочная запись (Master Boot Record — MBR), на которую передается управление компьютером. Программа первоначальной загрузки (Non-System Bootstrap — NSB — несистемный загрузчик) является первой частью MBR. NSB анализирует таблицу разделов жесткого диска (Partition Table), являющуюся второй частью MBR, и определяет по ней расположение (номера сектора, цилиндра и стороны) активного раздела, содержащего рабочую версию ОС. Определив активный (загрузочный) раздел НЖМД, программа NSB считывает его нулевой сектор (Boot Record — BR — загрузочную запись) и передает ей управление ПЭВМ. Алгоритм работы загрузочной записи зависит от операционной системы, но обычно состоит в запуске непосредственно операционной системы или программы — загрузчика ОС.

Парольная система BIOS имеет только два варианта паролей с категориями «пользователь» и «суперпользователь». Ввод парольной информации выполняется (если функция активирована в соответствующих настройках BIOS) до обращения к жесткому диску компьютера, т. е. до загрузки операционной системы. Это только один из эшелонов защиты АС, который способен разде-

лить потенциальных пользователей на легальных (своих, знающих пароль пользователя) и нелегальных. Парольная система BIOS не обеспечивает идентификации конкретного пользователя.

Защита от входа в АС в незащищенном режиме является весьма серьезной мерой, обеспечивающей безопасность информации и противодействующей попыткам подготовленных нарушителей запустить компьютер в обход системы защиты. Целостность механизмов защиты может быть нарушена, если злоумышленник имеет возможность загрузить на компьютере какую-либо операционную систему с внешнего носителя либо установленную ОС в режиме защиты от сбоев. Опасность загрузки ОС в режиме защиты от сбоев заключается в том, что загружается лишь ограниченный перечень системных драйверов и приложений, в составе которых могут отсутствовать модули СЗИ. Конфиденциальные данные при неактивном СЗИ могут оказаться совершенно незащищенными, и злоумышленник может получить к ним неограниченный доступ.

Для противодействия подобной угрозе необходимо, во-первых, сделать недоступным для просмотра содержимое дисков при загрузке ОС с внешнего носителя. Данная задача может быть решена путем криптографического преобразования информации на жестком диске. Зашифрованным должно быть не только содержимое конфиденциальных файлов, но и содержимое исполняемых и иных файлов, а также служебные области машинных носителей.

Во-вторых, следует внести изменения в стандартный процесс загрузки компьютера, внедрив в него процедуры инициализации механизмов защиты еще до загрузки ОС. Запуск защитных механизмов СЗИ обычно выполняется по одному из следующих способов: с использованием собственного контроллера СЗИ либо путем модификации главной загрузочной записи.

При реализации первого способа СЗИ должно быть программно-*аппаратным* комплексом и содержать собственный контроллер, который обычно устанавливается в слот ISA или PCI. В процессе выполнения процедуры POST после проверки основного оборудования BIOS компьютера начинает поиск внешних ПЗУ в диапазоне адресов от C800:0000 до E000:0000 с шагом в 2Kb. Аппаратная часть СЗИ должна быть организована так, чтобы ее ПЗУ, содержащее процедуры идентификации и аутентификации пользователей, обнаруживалось компьютерной системой по одному из проверяемых системой адресов. При обнаружении внешнего ПЗУ POST BIOS передает управление программе, расположенной в найденном ПЗУ. Таким образом, защитные механизмы (процедуры идентификации и аутентификации, контроля целостности и т. п., записанные в ПЗУ контроллера СЗИ) начинают работать еще до загрузки ОС. И только после удачной отработки механизмов защиты средство защиты возвращает управление процедуре POST, либо непосредственно передает управление на MBR жесткого диска. Кроме ПЗУ, хранящего программы защитных механизмов, в составе СЗИ должны быть перепрограммируемые ПЗУ, в которые заносятся список зарегистрированных пользователей с образами аутентифицирующей их информации и временными рамками разрешения входа в АС. Одним из примеров подобной реализации доверенной загрузки является СЗИ НСД «Аккорд-АМДЗ» (рис. 3.5).

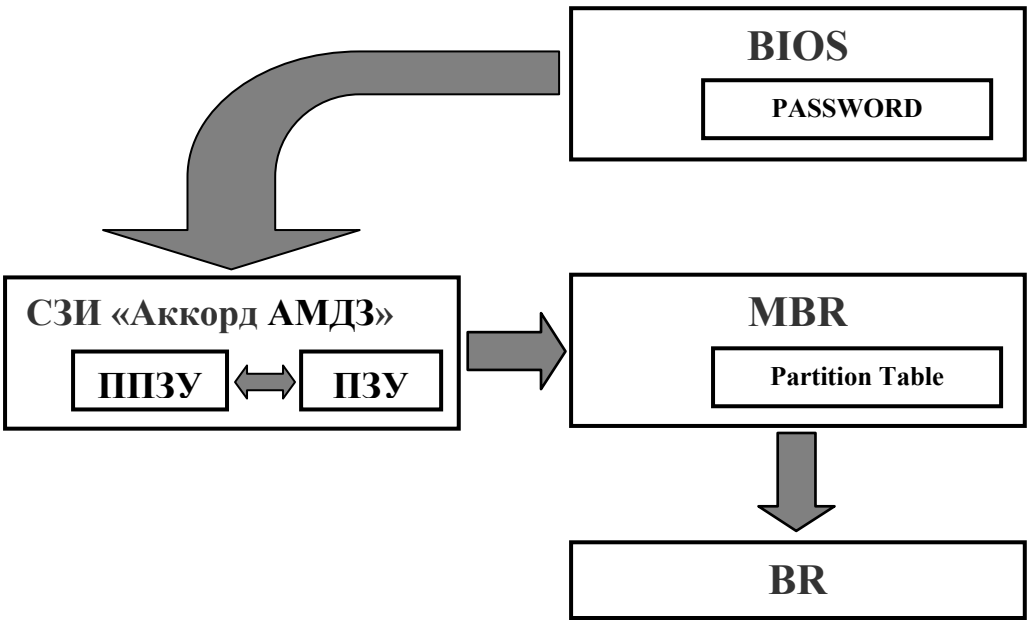


Рис. 3.5. Процесс загрузки персонального компьютера с использованием контроллера СЗИ

Второй способ запуска защитных механизмов применяется в программных СЗИ, примерами которых являются «Страж NT» и «Dallas Lock», которые не имеют собственных аппаратных контроллеров. Задача надежного запуска защитных механизмов (до загрузки ОС) решается здесь путем модификации главной загрузочной записи в *процессе установки* системы защиты. Обычно модификации подвергается только первая часть MBR — программа первоначальной загрузки. В процессе инициализации СЗИ программа первоначальной загрузки меняется на собственную программу средства защиты, задачей которой является передача управления на программный код, реализующий запуск и отработку защитных механизмов доверенной загрузки. После удачного выполнения всех предусмотренных СЗИ процедур управление ПЭВМ передается либо на штатную программу первоначальной загрузки ОС, которая при установке средства защиты копируется в некоторый сектор нулевой дорожки НЖМД, либо напрямую на загрузочную запись активного раздела жесткого диска (рис. 3.6).

В теории и практике обеспечения безопасности АС хорошо известен такой способ преодоления злоумышленником системы защиты, как подбор пароля. Он заключается в переборе всех возможных вариантов паролей («лобовая атака») или наиболее вероятных комбинаций (оптимизированный перебор). Для того чтобы исключить возможность осуществления штурма парольной системы защиты в СЗИ предусматривается режим блокировки компьютера после нескольких (обычно трех — пяти) неудачных попыток ввода пароля. Выход АС из этого режима возможен только после выключения питания (полной перезагрузки системы). Режим блокировки может быть запущен при обнаружении системой защиты любых нештатных действий пользователя как во время доверенной загрузки (например, если код, записанный в предъявляемую карту памяти, не соответствует введенным идентификатору и/или паролю), так и во

время последующей работы (например, при попытке обратиться к запрещенным для доступа портам, устройствам ввода-вывода). Естественно, все попытки неудачного входа в систему, приведшие к блокированию компьютера, должны быть зафиксированы в специальном журнале.

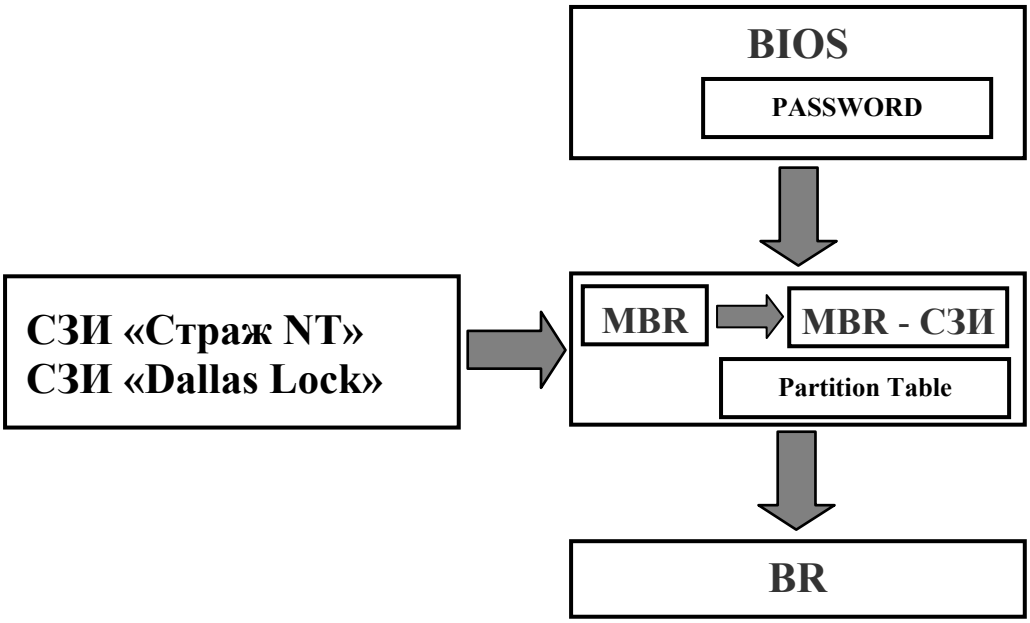


Рис. 3.6. Процесс загрузки персонального компьютера с использованием модификации MBR

Следует отметить, что при отсутствии в функциональном наборе СЗИ процедуры шифрования защищаемых данных, необходимо обеспечить надежную защиту самого компьютера от непосредственного физического доступа. Действительно, если злоумышленнику удастся извлечь контроллер СЗИ из слота ПЭВМ, процесс загрузки ОС перестанет носить защищенный характер, и будет осуществляться стандартно. При наличии физического доступа к элементам АС подготовленный злоумышленник может просто украсть жесткий диск и попытаться добыть интересующую его информацию путем анализа НЖМД с помощью различных низкоуровневых редакторов. Запрет входа в систему в обход механизмов защиты является необходимой составляющей частью процесса доверенной загрузки и обеспечивает выполнение 1, 2 и 3 пунктов требований к системе защиты информации.

3.1.3. Разграничение доступа

Одним из ключевых методов защиты информации от НСД является разграничение полномочий и прав доступа пользователей к ресурсам АС. Напомним, что под доступом к информации понимают [5] ознакомление с информацией, ее обработку, в частности, копирование модификация или уничтожение информации. Разграничение доступа — организация и осуществление доступа субъектов к объектам доступа в строгом соответствии с порядком, установленным политикой безопасности предприятия. Доступ к информации, не нару-

шающий правила разграничения доступа называется санкционированным. Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами, — несанкционированным.

Данное направление деятельности включает разработку организационной схемы функционирования АС, анализ потоков данных, уточнение задач и полномочий пользователей, создание функциональных групп работников на основе круга решаемых задач, построение схемы категорирования объектов АС по критерию доступа различных пользователей.

В своде *правил разграничения доступа* (ПРД) из множества элементов произвольной автоматизированной системы выделяют два подмножества: множество *объектов* и множество *субъектов* доступа. Объект доступа (диск, каталог, файл, системная служба) — любой элемент системы, доступ к которому может быть произвольно ограничен. Субъект доступа (пользователь) — любая сущность, способная инициировать выполнение операций над объектами. Для различных типов объектов вводятся различные операции или методы доступа. Некоторые методы доступа для удобства использования объединяются в группы, называемые правами доступа. Так, например, право доступа к файлу «изменение» подразумевает возможность доступа к нему по методам «чтение» и «запись». А право «полного» доступа — по всем существующим методам, включая «изменение прав доступа».

В качестве дополнительного множества иногда вводятся процессы, порождаемые (инициируемые) субъектами над объектами. Одной из важнейших задач разграничения доступа в АС является обязательная проверка полномочий любых процессов по отношению к обрабатываемым данным.

На этапах проектирования и эксплуатации защищенных АС возникает задача синтеза системы разграничения доступа пользователей информационной системы к ее ресурсам. Предельная открытость системы, когда максимальному числу пользователей предоставляются максимальные права на доступ ко всем ресурсам, приводит к максимальной эффективности ее функционирования, однако увеличивает риск возможных нарушений информационной безопасности. В то же время любые меры безопасности и ограничения объективно снижают отдельные характеристики эффективности функционирования системы. Наличие или отсутствие прав доступа определяется принятой в организации политикой безопасности, при разработке которой следует учитывать следующие принципы:

- доступ любого субъекта к любому объекту доступа может осуществляться только на основе явного или косвенного санкционирования администратором системы или владельцем объекта доступа;
- правила разграничения доступа не должны допускать изменения и удаления жизненно важных системных объектов;
- каждый объект должен иметь владельца;
- должна быть исключена возможность случайной (непреднамеренной) утечки конфиденциальной информации, включая так называемые скрытые каналы утечки информации [15].

Теория и практическая реализация механизмов разграничения доступа обсуждается во многих литературных источниках [10, 11, 15, 16, 17]. Механизмы разграничения доступа оперируют с множествами операций, которые субъекты могут инициировать над объектами. Для каждой пары «субъект — объект» вводится множество *разрешенных* операций, являющееся подмножеством всего множества *допустимых* операций [11]. Оставшиеся операции будут составлять подмножество запрещенных данному пользователю методов доступа к конкретному объекту.

Существуют две основных модели разграничения доступа: дискреционная (одноуровневая) и мандатная (многоуровневая). Большинство ОС, применяющихся в настоящее время на практике (ОС семейства MS Windows NT[1], Novell NetWare, UNIX), реализуют дискреционную модель разграничения доступа. Система правил дискреционной модели разграничения доступа формулируется следующим образом [13]:

1. У каждого объекта операционной системы существует владелец.
2. Владелец объекта может произвольно ограничивать (или разрешать) доступ других субъектов к данному объекту.
3. Для каждой тройки субъект-объект-метод возможность доступа определена однозначно (рис. 3.7).
4. Существует хотя бы один привилегированный пользователь, имеющий возможность обратиться к любому объекту по любому методу доступа.

Формально дискреционная модель разграничения доступа может быть представлена в виде матрицы доступа, строки которой соответствуют субъектам системы, а столбцы — объектам. Элементы матрицы характеризуют права доступа конкретного субъекта к конкретному объекту. Матрица доступа может формироваться на основе двух различных принципов: централизованного и децентрализованного. При реализации централизованного (принудительного) принципа возможность доступа субъектов к объектам определяется администратором. При реализации децентрализованного (добровольного) принципа доступом управляет владелец объекта. Первый принцип жесткого администрирования обеспечивает более четкий контроль над соблюдением ПРД. Второй принцип более гибкий, однако, труднее поддается контролю со стороны лиц, несущих ответственность за безопасность данных. На практике часто применяют принудительный принцип управления доступа с элементами добровольного подхода.

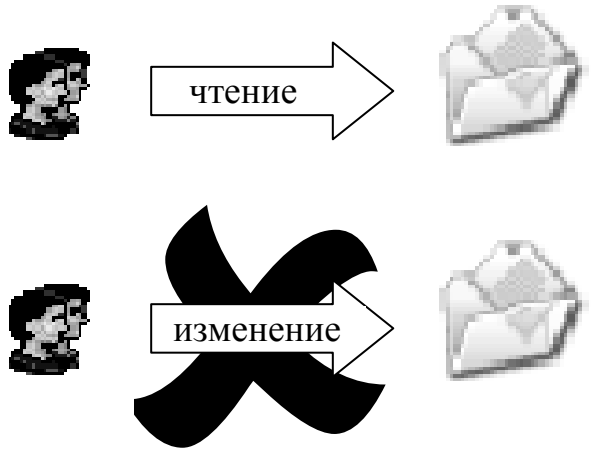
В большинстве случаев матрица доступа имеет весьма существенные размеры (в компьютерной системе присутствует множество различных субъектов и объектов) и является разреженной (субъектам необходим доступ только к небольшим подмножествам объектов). В целях экономии памяти матрица доступа может задаваться в виде списков прав субъектов (для каждого субъекта

[1] Под семейством ОС MS Windows NT авторы понимают известные на момент написания пособия системы Windows NT 4.0 Workstation, Windows NT 4.0 Server, Windows 2000 Professional, Windows 2000 Server, Windows XP Home Edition, Windows XP Professional, Windows Server 2003.

создается список доступных объектов) или в виде списков прав доступа (для каждого объекта создается список субъектов, имеющих права доступа к нему).

В практических реализациях используется хранение матрицы доступа в виде списков прав доступа, ассоциированных с каждым объектом. Известны два способа кодирования строки матрицы доступа: механизм битов защиты, применяемый в ОС семейства UNIX, и механизм списков прав доступа, применяемый, например, в ОС семейства MS Windows NT.

При реализации дискреционной модели в рамках определенной ОС применяются различные алгоритмы проверки прав доступа субъекта к объекту.



Субъект	Объект	Метод	Возможность
Ювченко	C:\ Приказы и распоряжения	Чтение	Разрешено
Ювченко	C:\ Приказы и распоряжения	Изменение	Запрещено

Рис. 3.7. Тройки субъект-объект-метод

Формализованный алгоритм проверки прав доступа при использовании механизма битов защиты, реализованный в ОС семейства Unix, приведен в [10]. С объектом (файлом) связываются биты защиты, указывающие права доступа для трех категорий субъектов: все пользователи, члены группы владельца и владелец объекта (рис. 3.8). Множество допустимых операций составляют три метода: чтение, запись и выполнение. При попытке доступа производится:

- проверка того, является ли субъект владельцем объекта;
- проверка вхождения субъекта в группу владельца;
- сравнение полномочий, предоставляемых всем пользователям системы, с запрашиваемым типом доступа.

При этом отсутствие разрешений для конкретного субъекта в приоритетной категории пользователей, к которой он принадлежит, приводит к отказу в доступе. Если, например, у владельца нет соответствующих прав, ему будет отказано в доступе к его объекту, и его права как члена своей группы и пользователя проверяться не будут. Пример реализации механизма битов защиты в ОС семейства Unix приведен на рис. 3.9.

Владелец			Группа владельца			Все зарегистрированные пользователи		
Чтение	Запись	Выполнение	Чтение	Запись	Выполнение	Чтение	Запись	Выполнение
*	*	*	*					

Рис. 3.8. Пример механизма битов защиты

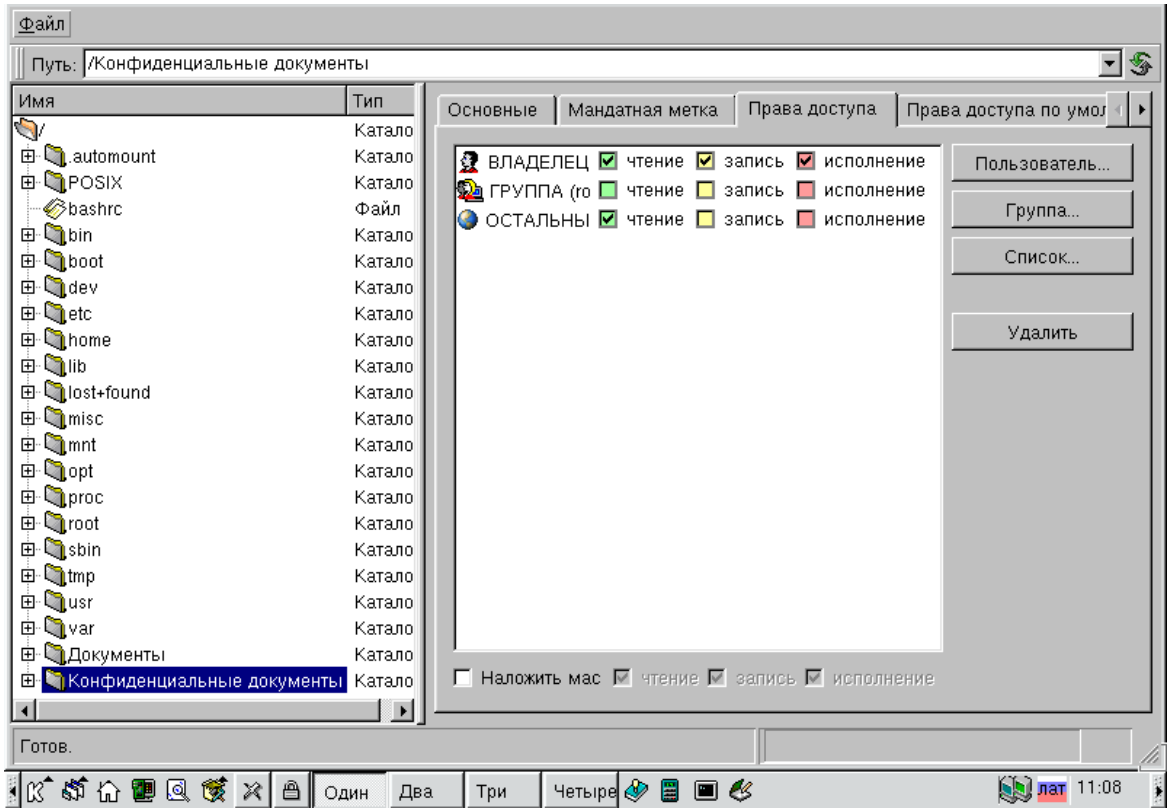


Рис. 3.9. Пример реализации механизма битов защиты в ОС семейства Linux

При использовании механизма списков прав доступа (Access Control List — ACL) не выделяют категорий пользователей (рис. 3.10). В то же время для удобства администрирования доступа пользователи могут объединяться в группы, например, по их функциональному признаку. Конкретный список субъектов (групп) доступа ассоциируется с каждым объектом с указанием прав доступа к нему для каждого пользователя (группы). Каждый список ACL состоит из так называемых записей управления доступом (Access Control Entries — ACE). Всего существует три типа записей. Два из них относятся к управлению доступом: первый разрешает указанный доступ и определяет метод доступа (ACE Allowed), а второй запрещает доступ (ACE Denied). Третий тип записей определяет настройки аудита доступа к объекту (ACE Audit).

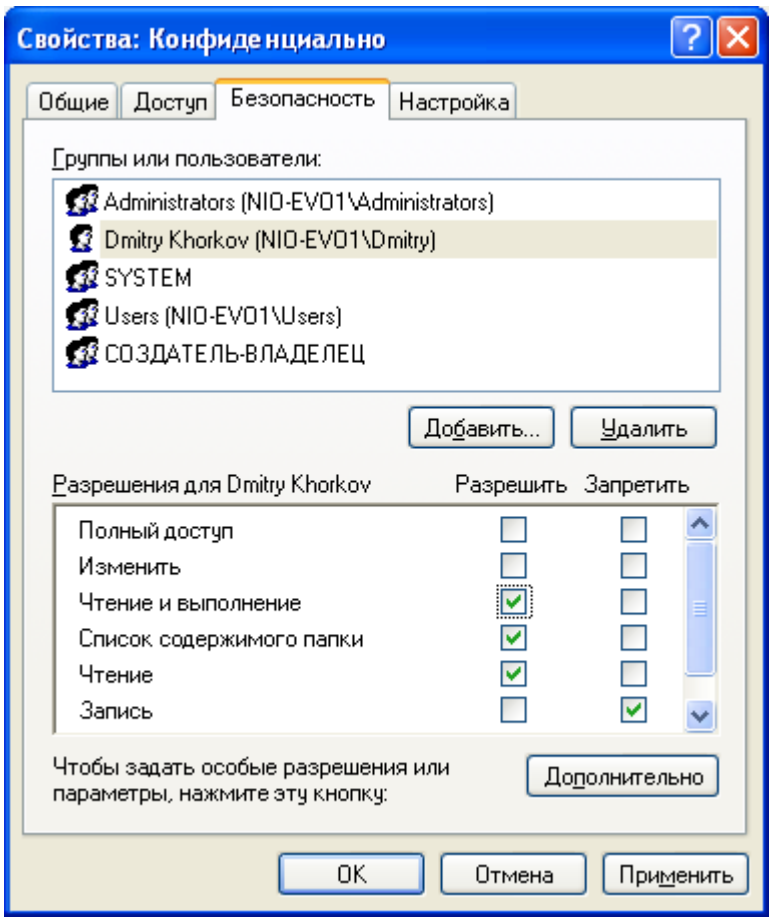


Рис. 3.10. Пример реализации механизма списки прав доступа в ОС MS Windows XP

Каждая запись управления доступом (ACE) состоит из идентификатора пользователя или группы пользователей и совокупности разрешенных методов доступа. При принятии решения о предоставлении доступа к объекту в ОС семейства MS Windows NT записи управления доступом обрабатываются с учетом иерархической структуры каталогов следующим образом ([12, 13]):

- система сравнивает идентификатор пользователя, запросившего доступ к объекту, а также идентификаторы всех групп, к которым он принадлежит, с идентификаторами, присутствующими в ACL объекта. Если в ACL отсутствует упоминание идентификаторов пользователя и его групп, то доступ запрещается;
- если идентификаторы присутствуют в ACL, то сначала обрабатываются ACE типа Denied (по запрещенным методам доступа). Для всех записей ACE типа Denied, идентификатор которых совпадает с идентификатором пользователя или его групп, запрашиваемый метод доступа сравнивается с указанным в ACE. Если метод (чтение, запись и т.д.) присутствует в ACE данного типа, то доступ запрещается, и дальнейшая обработка по данному методу не производится, и ACE типа Allowed не анализируются;

- если система не обнаруживает запрета на доступ по запрашиваемому методу в ACE типа Denied, она осуществляет анализ ACE типа Allowed (по разрешенным методам доступа). Для всех записей, имеющих тип Allowed, запрашиваемый метод доступа также сравнивается с указанным в ACE. По результатам сравнения отмечается, какие методы запрашиваемого доступа разрешены;
- если все методы доступа, которые указаны в запросе, встретились в ACE типа Allowed и не были обнаружены в ACE типа Denied, то запрашиваемый пользователем доступ будет удовлетворен системой полностью. В противном случае доступ разрешается только по тем методам, которые не запрещены в ACE типа Denied и разрешены в ACE типа Allowed [10].

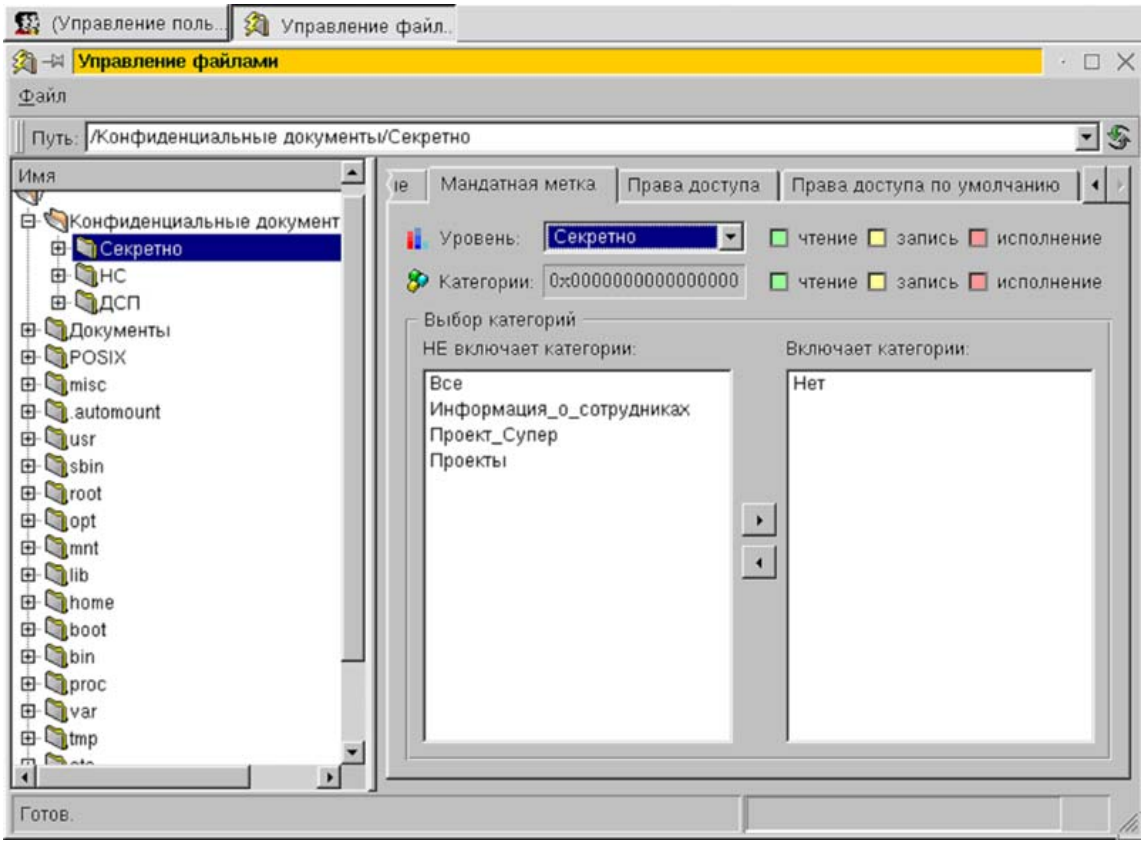


Рис. 3.11. Пример категорирования каталогов по уровню конфиденциальности в ОС семейства Linux

Многоуровневая (мандатная, полномочная) модель разграничения доступа подробно описана в [11, 13–17]. Мандатная модель предполагает категорирование объектов доступа по уровню конфиденциальности (рис. 3.11), а субъектов — по степени (уровням) допуска (рис. 3.12).

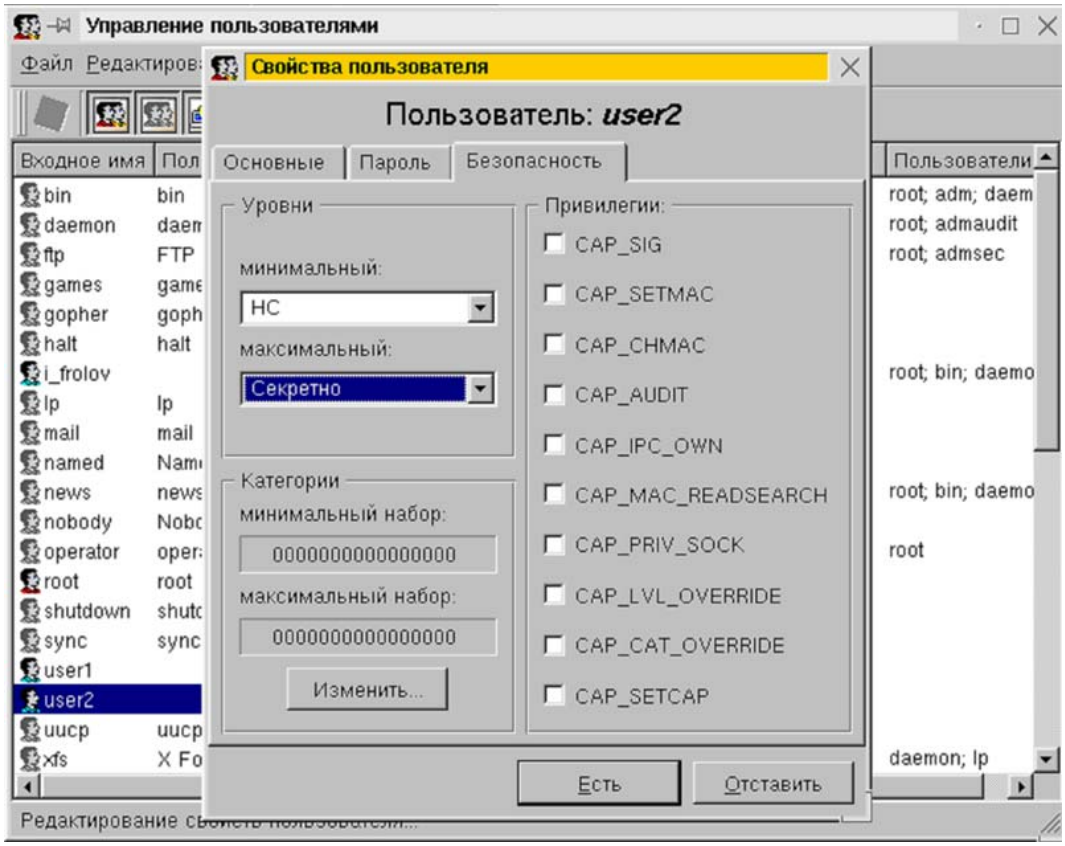


Рис. 3.12. Пример категорирования пользователей ОС семейства Linux по уровням допуска

Мандатная модель разграничения доступа обычно применяется в совокупности с дискреционной. Различают два способа реализации мандатной модели: с контролем информационных потоков и, более простой, без контроля потоков, который на практике встречается крайне редко. Правила мандатной модели разграничения доступа с контролем информационных потоков формулируются следующим образом [13].

1. У любого объекта операционной системы существует владелец.
2. Владелец объекта может произвольно ограничивать (или разрешать) доступ других субъектов к данному объекту.
3. Для каждой четверки субъект-объект-метод-процесс возможность доступа определена *однозначно в каждый момент времени.*
4. Существует хотя бы один привилегированный пользователь, имеющий возможность удалить любой объект.
5. Во множестве объектов выделяются множества объектов полномочного разграничения доступа. Каждый объект имеет свой уровень конфиденциальности.
6. Каждый субъект имеет уровень допуска.
7. Запрет чтения вверх (Not Read Up — NRU): запрет доступа по методу «чтение», если уровень конфиденциальности объекта выше уровня допуска субъекта, осуществляющего запрос.
8. Каждый процесс имеет уровень конфиденциальности, равный максимуму из уровней конфиденциальности объектов, открытых процессом.

9. Запрет записи вниз (Not Write Down — NWD): запрет доступа по методу «запись», если уровень конфиденциальности объекта ниже уровня конфиденциальности процесса, осуществляющего запрос.
10. Понизить гриф секретности объекта может субъект, который имеет доступ к объекту (по правилу 7) и обладает специальной привилегией.

Основная цель, которая достигается применением мандатной модели разграничения доступа с контролем информационных потоков, — это предотвращение *утечки информации* определенного уровня конфиденциальности к субъектам, чей уровень допуска ниже. Как известно, распространенные операционные системы не обеспечивают безопасности обрабатываемых данных на уровне приложений. Виной тому особенности механизма распределения памяти, использование буфера обмена данных, применение «свопирования» памяти, файлов подкачки и специфика самих приложений. Все это неизбежно приводит к тому, что при одновременной обработке файлов, имеющих различный уровень конфиденциальности, оберегаемая конфиденциальная информация или ее фрагменты могут попадать в документы с меньшим уровнем конфиденциальности. Неконтролируемое проникновение информации из одного документа в другой (с меньшим уровнем конфиденциальности) и принято называть ее утечкой. Выполнение 7, 8 и 9-го правил многоуровневой модели разграничения доступа гарантирует отсутствие утечки конфиденциальной информации.

Мандатная модель разграничения доступа *должна быть использована*, согласно руководящим документам Гостехкомиссии России [5, 6], в автоматизированных системах, начиная с класса 1В, предполагающего возможность обработки информации, составляющей государственную тайну. Таким образом, для обработки информации, составляющей государственную тайну в автоматизированных системах, в которых одновременно обрабатывается и (или) хранится информация различных уровней конфиденциальности, необходимо использовать компьютерные системы, в которых в обязательном порядке реализована мандатная модель разграничения доступа.

В широко распространенных ОС семейства MS Windows NT и Unix-подобных ОС реализована только дискреционная модель. Следовательно, для распространенных ОС, при условии обработки информации, составляющей государственную тайну, необходимо применение дополнительных средств, реализующих мандатную модель разграничения доступа. Программно-аппаратные средства защиты информации «Страж NT», «Dallas Lock», «Secret Net 2000» и «Аккорд-АМДЗ», обсуждаемые в данном пособии, являются надстройкой над существующей программной средой АС и предназначены, в частности, для внедрения мандатной модели в системы, работающие под управлением ОС семейства MS Windows NT.

Совокупность дискреционной и мандатной моделей разграничения доступа позволяет организовать выполнение сформулированного в п.1.1 требования 4: пользователи должны получать доступ только к той информации и с теми возможностями по ее обработке, которые соответствуют их функциональным обязанностям.

В дополнение к дискреционной и мандатной моделям в защищенных многопользовательских АС должен применяться режим изолированной или замкнутой программной среды. Данный режим целесообразно задействовать в тех случаях, когда для обработки информации применяется определенный перечень программных продуктов, и политикой безопасности запрещается использование других программ в целях, не имеющих отношение к выполнению функциональных обязанностей пользователями (см. требование 5). Также этот метод обеспечивает защиту компьютера от создания и запуска на нем вредоносного программного кода.

Суть метода заключается в том, что для каждого пользователя формируется перечень исполняемых файлов, которые могут быть им запущены. Реализация метода часто осуществляется формированием для каждого пользователя списка имен исполняемых файлов, иногда без указания полного пути. В более качественных системах для каждого исполняемого файла указывается признак возможности его запуска тем или иным пользователем. В том и в другом случаях целесообразно осуществлять проверку целостности исполняемых файлов при каждом их запуске.

Разграничение доступа пользователей к данным, программам и устройствам АИС является одним из важнейших методов обеспечения защиты информации и обеспечивает выполнение 2, 4–8 требований, приведенных в п. 1.1. пособия. Совместно с контролем целостности программного обеспечения (см. ниже) режим замкнутой программной среды обеспечивает «чистоту» компьютерной системы и затрудняет запуск в АИС вредоносных программ.

3.1.4. Регистрация событий (аудит)

Регистрация событий или аудит событий безопасности — фиксация в файле-журнале событий, которые могут представлять опасность для АС.

Регистрация событий как механизм защиты предназначена для решения двух основных задач: расследование инцидентов, произошедших с применением АС, и предупреждение компьютерных преступлений. При этом вторая задача может по степени важности выйти на первое место — если недобросовестный сотрудник организации знает о том, что все его действия в АС протоколируются, он воздержится от совершения действий, которые не входят в круг его функциональных обязанностей.

В связи с тем, что журналы аудита событий используются при расследовании происшествий, должна обеспечиваться полная объективность информации, фиксируемой в журналах. Для обеспечения объективности необходимо выполнение следующих требований к системе регистрации событий:

- только сама система защиты может добавлять записи в журнал;
- ни один субъект доступа, в том числе сама система защиты, не имеет возможности редактировать отдельные записи;
- в АС кроме администраторов, регистрирующих пользователей и устанавливающих права доступа, выделяется дополнительная категория — аудиторы;

- только аудиторы могут просматривать журнал;
- только аудиторы могут очищать журнал;
- полномочия администратора и аудитора в рамках одного сеанса несовместимы;
- при переполнении журнала система защиты аварийно завершает работу.

Средствами ОС семейства MS Windows NT могут регистрироваться следующие категории событий (рис. 3.13):

- вход/выход пользователей из системы;
- изменение списка пользователей;
- изменения в политике безопасности;
- доступ субъектов к объектам;
- использование опасных привилегий;
- системные события;
- запуск и завершение процессов.

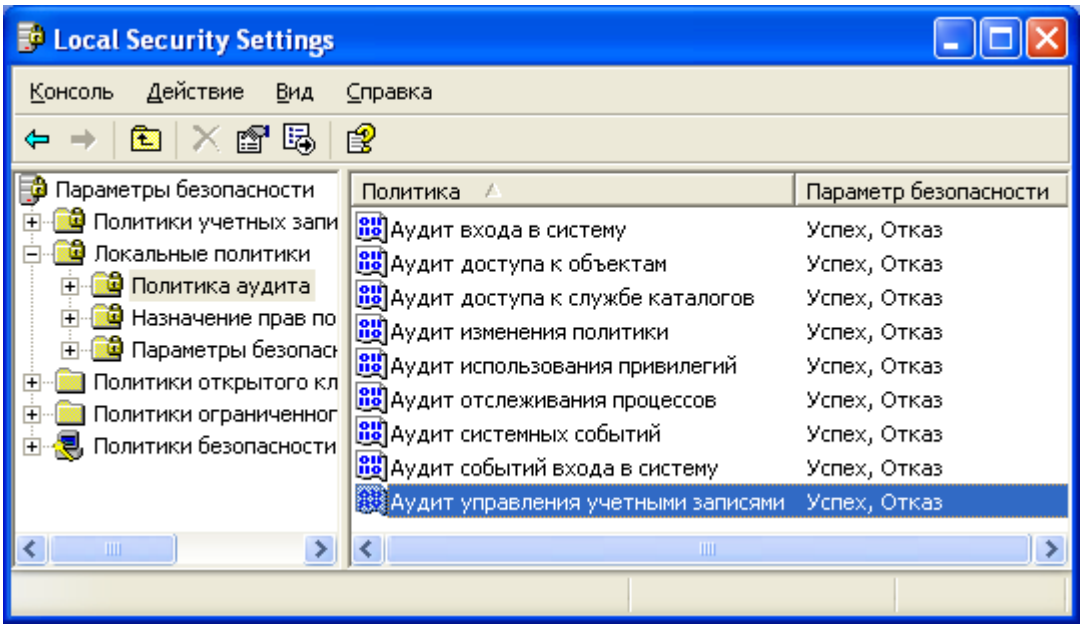


Рис. 3.13. Пример настройки политики аудита в ОС MS Windows XP

Вместе с тем при определении количества регистрируемых событий, следует вести речь об адекватной политике аудита, т. е. такой политике, при которой регистрируются не все возможные категории событий, а только действительно значимые и необходимые.

Так, на примере операционных систем семейства MS Windows NT, можно сформулировать следующую адекватную политику аудита [13, 16] (рис. 3.14):

- вход и выход пользователей регистрировать всегда;
- доступ субъектов к объектам регистрировать только в случае обоснованных подозрений злоупотребления полномочиями;
- регистрировать применение опасных привилегий;

- регистрировать только успешные попытки внесения изменений в список пользователей;
- регистрировать изменения в политике безопасности;
- не регистрировать системные события;
- не регистрировать запуск и завершение процессов, кроме случая обоснованных подозрений, например, вирусных атак.

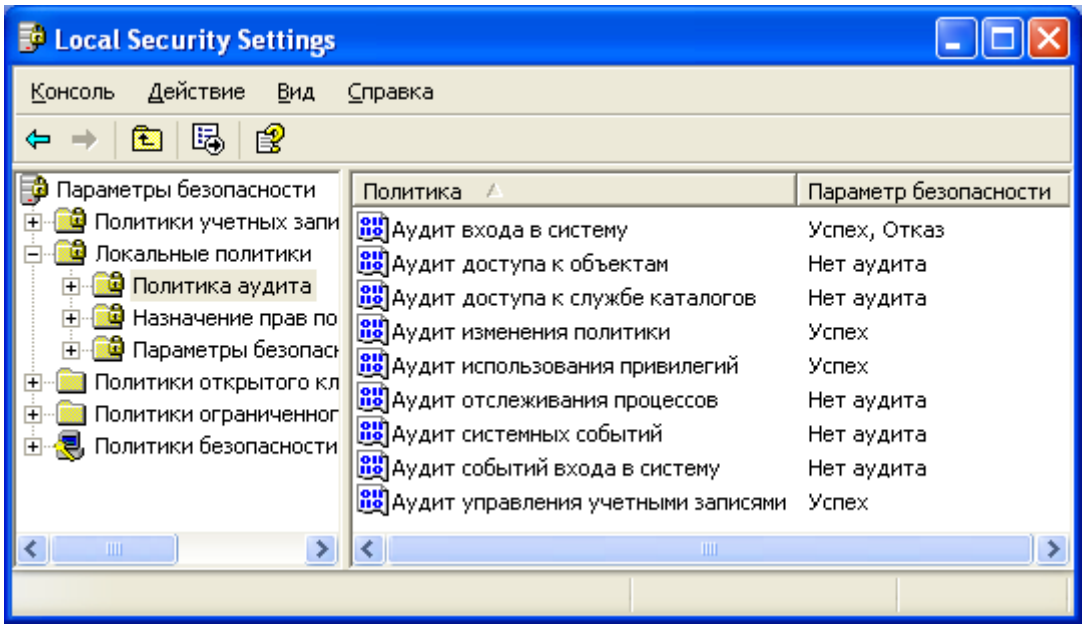


Рис. 3.14. Пример настройки адекватной политики аудита в ОС MS Windows XP

Механизм защиты *регистрация событий* позволяет организовать выполнение сформулированного в п.1.1 требования 8: в целях профилактики и расследования возможных инцидентов автоматически должна вестись регистрация в специальных электронных журналах наиболее важных событий, связанных с доступом пользователей к защищаемой информации и компьютерной системе в целом. Специальным образом организованная регистрация бумажных документов, распечатываемых в АИС, гарантирует выполнение требования 9.

3.2. Модель защищенной компьютерной системы

Для построения модели защищенной компьютерной системы, отвечающей перечисленным в главе 1 требованиям, рассмотрим некое предприятие НПО «Сигма», ведущее разработку проектно-конструкторской документации по различным инженерным направлениям. Несколько не связанных между собой групп специалистов ведут разработку самостоятельных инженерных проектов «Луна-1», «Юпитер-9», «Полет» и т. д. Сами проекты являются конфиденциальными программами (конфиденциальная информация — информация, требующая защиты [5]), а их документация — охраняемыми данными.

Рис. 3.15. Структура каталогов компьютерной системы предприятия

Документация проектов представляет собой ряд текстовых и графических электронных документов, обрабатываемых в единой компьютерной системе и имеющих различный уровень конфиденциальности: «открытые данные», «конфиденциально» и «строго конфиденциально». Уровней конфиденциальности может быть и больше: «ограниченного доступа», «особо конфиденциально» и т. д. Система уровней конфиденциальности определяется градацией информационных ресурсов в зависимости от величины и характера (качества) ущерба при неограниченном распространении соответствующей информации. В СЗИ различных производителей уровни конфиденциальности имеют различное наименование. Так, «открытые данные» иногда именуют «несекретными» или «общедоступными»; «конфиденциальные» называют «ДСП», «служебная тайна» или «конфиденциальные документы»; «строго конфиденциальные документы» — «секретными». В дальнейшем в пособии для обозначения уровней конфиденциальности будем пользоваться терминами «Несекретно», «ДСП», «Секретно» (рис. 3.15).

К документации каждого из инженерных проектов имеют доступ конкретные сотрудники предприятия, которые в рамках соответствующих проектов имеют различные уровни допуска к информации.

Руководит предприятием «Сигма» Клинов А.В., он имеет максимальный уровень допуска к информации и возможность работы с документацией любого проекта. Экономист Ювченко А.Н. работает над проектом «Продажи». Администратор компьютерной системы (администратор безопасности) Чистяков А.В. имеет полный доступ к любым документам, имеет возможность

управлять настройками компьютерной системы и реализует на практике политику безопасности предприятия, в части, касающейся информационных технологий. Для удобства работы всех пользователей АС в ее состав включена база данных, содержащая нормативно-правовые документы, требования ЕСПД, технические справочники. Администратор следит за состоянием базы данных, своевременно обновляет ее. Руководитель предприятия издает приказы и указания и размещает их в электронном виде в соответствующем каталоге. Сотрудники предприятия могут беспрепятственно знакомиться с содержимым базы данных и распоряжениями руководителя предприятия, копировать необходимую им информацию, но вносить изменения в эти каталоги они не имеют право.

Пусть к документации проекта «Полет» имеют доступ инженеры Свалов А.В., Савин П.А. и Соколов С.Ю., имеющие уровни допуска к секретной, ДСП, и несекретной информации соответственно (табл. 2.1).

Таблица 2.1

Уровни допуска сотрудников

Уровень допуска	Сотрудники
Несекретно	С.Ю. Соколов
ДСП	П.А. Савин, А.Н. Ювченко
Секретно	А.В. Свалов, А.В. Клинов, А.В. Чистяков

В зависимости от своих функциональных обязанностей сотрудники могут осуществлять различные действия с документами проекта (защищаемыми данными): редактировать, просматривать, удалять, копировать, распечатывать. В общем случае специалисты организации одновременно могут работать над несколькими проектами, но в нашем примере инженеры Свалов, Савин и Соколов заняты только проектом «Полет» и только к нему имеют доступ. В то же время они выполняют весь необходимый объем работы по данному проекту, поэтому доступ остальных инженеров предприятия к его документации запрещен. Для предварительной проработки проектной документации инженеры могут создавать черновики документов. Черновики создаются в специальном каталоге для индивидуального пользования, они доступны только авторам, администратору и руководителю предприятия.

Права доступа сотрудников к документации предприятия разрешенного уровня конфиденциальности находят свое отражение в матрице доступа, которая вместе с установленной системой допусков и уровней конфиденциальности информационных ресурсов формализует политику разграничения доступа. Возможный вариант матрицы, приведен в табл. 2.2, где буквой «П» обозначен тип доступа *полный доступ*, буквой «Ч» — *только чтение*, пробелом — *запрет доступа*.

Предполагается, что администратор системы Чистяков и руководитель предприятия Клинов имеют допуск в систему в любой день недели с 7.00 до 23.00. Остальные сотрудники могут регистрироваться в системе только в рабочие дни с 8.30 до 17.30.

Далее в пособии приводятся рекомендации по применению различных СЗИ для построения и эксплуатации защищенной компьютерной системы, базирующейся на предложенной политике безопасности, выполняющей перечисленные в главе 1 требования и использующей описанные методы защиты информации.

По каждому из СЗИ от НСД читателю предлагается реализовать предложенную политику безопасности на примере НПО «Сигма» и последовательно применить методы защиты:

- идентификацию и аутентификацию пользователей, создавая требуемые учетные записи и назначая им пароли;
- разграничение доступа, реализовывая мандатную и дискреционную модели, а также принцип замкнутой программной среды;
- контроль целостности, включая подсистемы контроля целостности для защиты конфиденциальных данных от несанкционированной модификации;
- регистрацию событий, настраивая политику аудита для выявления наиболее опасных действий нарушителя;
- уничтожение остаточной информации, выполняя гарантированное удаление конфиденциальных данных.

При изучении СКЗИ читателю предлагается применить метод криптографической защиты конфиденциальных данных путем создания защищенных виртуальных логических дисков.

Таблица 2.2

Матрица доступа предприятия

Каталог	Соколов (инженер)	Савин (инженер)	Свалов (инженер)	Чистяков (администра-тор)	Ювченко (экономист)	Клинов (начальник)
С:\Экономика\Канцелярские товары (НС)				П	П	П
С:\ Экономика\Продажи (ДСП)				П	П	П
С:\ Приказы и распоряжения	Ч	Ч	Ч	П	Ч	П
С:\ База данных (Консультант Плюс)	Ч	Ч	Ч	П	Ч	Ч
С:\Проекты\Полет\ Графические докумен-ты\Несекретно	П	П	П	П		П
С:\Проекты\Полет\ Графические документы\ДСП		П	П	П		П
С:\Проекты\Полет\ Графические докумен-ты\Секретно			П	П		П
С:\Проекты\Полет\ Текстовые докумен-ты\Несекретно	П	П	П	П		П
С:\Проекты\Полет\ Текстовые документы\ДСП		П	П	П		П
С:\Проекты\Полет\ Текстовые докумен-ты\Секретно			П	П		П
С:\Проекты\Полет\ Черновики\Соколов	П			П		П
С:\Проекты\Полет\ Черновики\Савин		П		П		П
С:\Проекты\Полет\ Черновики\Свалов			П	П		П