**Задание на 08.02.2022**

МДК 03.02 Программно-аппаратные средства защиты информации

1. **Сделать конспект лекции**
2. **Сделать практическую работу №17 Программно-аппаратные средства защиты информации**
3. **Сделать практическую работу №18 Интеграция защищенных операционных систем в защищенную сеть**
4. **Отчет отправить на почту** [**svebalch@mail.ru**](mailto:svebalch@mail.ru)
5. **СРС:** [**https://stepik.org/course/94299/promo**](https://stepik.org/course/94299/promo) **пройти онлайн курсы на платформе Степик. Тема: Кибербезопасность**

**Лекция 17**

**Комплекс КРИПТОН -ЗАМОК для ограничения доступа компьютеру**

Комплекс КРИПТОН-ЗАМОК предназначен для построения аппаратно-программных средств ограничения доступа к компьютеру с использованием УКЗД серии КРИПТОН . Комплекс позволяет организовать на базе персонального компьютера рабочее место с ограничением круга лиц, имеющих доступ к содержащейся в нем информации.

Для работы комплекса КРИПТОН -ЗАМОК необходим персональный компьютер IBM PC с процессором не ниже i386 и операционной системой-MS DOS, Windows 95/98/NT, UNIX и другими, для которых имеется соответствующий драйвер, позволяющий под управлением MS DOS понимать формат установленной на компьютере файловой системы.

Комплекс служит для защиты компьютеров с жесткими дисками, с файловыми системами в форматах FAT 12, FAT 16, FAT 32, NTFS, UNIX и т.д.

Работа с дисками с файловыми системами FAT 12, FAT 16 и FAT 32 обеспечивается средствами комплекса без дополнительных драйверов. Работа с дисками с нестандартными файловыми системами NTFS, HTFS, UNIX и т.д., не поддерживаемыми операционной системой MS-DOS, может производиться только при наличии на компьютере соответствующих DOS-драйверов. Комплекс КРИПТОН -ЗАМОК выпускается в двух исполнениях:

1. для жестких дисков объемом менее 8 Гбайт,
2. для жестких дисков объемом более 8 Гбайт.

В базовый состав аппаратно-программных средств ограничения доступа к компьютеру входят:

1. УКЗД серии КРИПТОН , поддерживающие режим работы комплекса ЗАМОК;
2. комплект драйверов и библиотек УКЗД;
3. комплекс ЗАМОК, включающий:

микросхему с программным обеспечением комплекса, устанавливаемую в УКЗД серии КРИПТОН;

инсталляционный дистрибутивный носитель с программным обеспечением, комплекса.

Установленный в персональный компьютер комплекс ограничения доступа КРИПТОН -ЗАМОК выполняет следующие функции:

1. ограничивает доступ пользователей к компьютеру путем их идентификации и аутентификации;
2. разделяет доступ пользователей к ресурсам компьютера в соответствии с их полномочиями;
3. контролирует целостность ядра комплекса, программ операционной среды, прикладных программ и областей памяти в момент включения компьютера до загрузки его операционной системы;
4. регистрирует события в защищенном электронном журнале;
5. передает управление и параметры пользователя программному обеспечению (RUN-файлам), указанному администратором (например, ПО защиты от несанкционированного доступа).

В соответствии с выполняемыми функциями комплекс КРИПТОН ЗАМОК содержит следующие основные подсистемы:

1. подсистему управления доступом, состоящую из устройства КРИПТОН и программы обслуживания CRLOCK.EXE;
2. подсистему регистрации и учета, включающую два журнала (аппаратный на устройстве КРИПТОН , фиксирующий попытки входа в компьютер до запуска его операционной системы, и полный-на жестком диске, в котором после удачного входа в комплекс отображаются все события, в том числе и содержимое аппаратного журнала), управление которыми осуществляется программой обслуживания комплекса CRLOCK.EXE;
3. подсистему обеспечения целостности, состоящую из устройства КРИПТОН и программы CHECKOS.EXE, проверяющей целостность главной ОС при работе комплекса.

При этом комплекс КРИПТОН -ЗАМОК обеспечивает выполнение следующих задач:

1. в компьютер может войти только санкционированный пользователь;
2. загружается достоверное ядро комплекса;
3. загружается достоверная операционная система;
4. проверяется целостность прикладного ПО , указанного администратором;
5. производится запуск программ, указанных администратором.

Рассмотрим штатную работу комплекса КРИПТОН -ЗАМОК. В начале работы с комплексом устройство КРИПТОН при инициализации его ключами с ключевого носителя (дискеты, смарт-карты или Touch Memory) загружает три файла: UZ.DB3 (УЗ, он один для всех пользователей данного компьютера); GK.DB3 (ГК, он уникален для каждого и может быть зашифрован на пароле пользователя) и файл-паспорт пользователя INIT.NSD.

Первые два файла обеспечивают выполнение устройством КРИПТОН криптографических процедур в соответствии с ГОСТ 28147-89 и формируются при помощи любой из программ генерации криптографических ключей, выпускаемых фирмой АНКАД для средств серии КРИПТОН (например, Crypton Soft, Crypton Tools или Сr Мng). Файл INIT.NSD уникален для каждого пользователя и используется при входе в комплекс для загрузки и проверки его ядра, поиска пользователя в файле полномочий, его аутентификации и расшифровки его записи. Файл INIT.NSD формируется на ключевом носителе пользователя: для администратора - автоматически программой INSTAL.EXE при установке комплекса на компьютер, а для всех остальных пользователей администратором при помощи программ CRLOCK.EXE.

Алгоритм работы комплекса КРИПТОН -ЗАМОК включает следующие шаги:

1. УКЗД КРИПТОН инициализируется файлами UZ.DB3 и GK.DB3.
2. КРИПТОН загружает файл INIT.NSD и проверяет его целостность по имитовставке. В случае нарушения целостности этого файла или при его отсутствии дальнейшая загрузка компьютера не производится.
3. КРИПТОН производит поиск имени вошедшего пользователя в списке пользователей. В случае отсутствия пользователя в списке дальнейшая загрузка компьютера не производится.
4. КРИПТОН производит аутентификацию пользователя-проверяет имитовставку его ключа. В случае несовпадения имитовставки пользователь считается несанкционированным и дальнейшая загрузка компьютера не производится.
5. КРИПТОН производит загрузку ОС комплекса ЗАМОК с Flash-диска. При загрузке автоматически стартует программа проверки целостности защищаемой ОС компьютера (далее "главной ОС")-CHECKOS.EXE.
6. CHECKOS.EXE получает параметры вошедшего пользователя от устройства КРИПТОН и:

− разблокирует клавиатуру;

− проверяет целостность файл-списка;

− проверяет целостность системных областей и файлов главной ОС;

− при наличии RUN-файлов проверяет их целостность и запускает на выполнение;

− по запросу пользователя меняет пароль ключей на его носителе; по запрос у администратора запускает программу обслуживания комплекса CRLOCK.EXE;

− при успешном завершении всех проверок CHECKOS.EXE запускает главную ОС.

После загрузки главной ОС компьютера комплекс ограничения доступа к компьютеру прекращает свою деятельность и не вмешивается в дальнейшую работу компьютера (до следующей загрузки).

Далее устройство КРИПТОН может использоваться как обычный шифратор.

Механизм RUN-файлов позволяет в процессе работы комплекса КРИПТОН -ЗАМОК запускать любые программы с предварительной проверкой их целостности. В частности, механизм RUN-файлов может быть использован при проверке файлов, находящихся на логических дисках с нестандартными файловыми системами (NTFS, HPFS, UNIX и т.д.). Другой вариант использования -запуск из под комплекса КРИПТОН -ЗАМОК любого другого программного обеспечения: системы ЗНСД, криптомаршрутизатора, операционной системы и т.д. На этой основе может быть построена система защиты персонального компьютера с требуемыми свойствами.

**Система защиты конфиденциальной информации Secret Disk.**

Система защиты конфиденциальной информации Secret Disk разработана компанией Aladdin при участии фирмы АНКАД и предназначена для широкого круга пользователей компьютеров: руководителей, менеджеров, бухгалтеров, аудиторов, адвокатов, т. е. всех тех, кто должен заботиться о защите личной или профессиональной информации.

При установке системы Secret Disk на компьютере создаются новые логические диски, при записи на которые информация автоматически шифруется, а при чтении-расшифровывается. Работа с секретными дисками совершенно незаметна и равносильна встраиванию шифрования во все запускаемые приложения (например, бухгалтерскую программу, Word, Excel и т.п.).

В системе Secret Disk используется смешанная программно-аппаратная схема защиты с возможностью выбора, соответствующего российским нормативным требованиям криптографического алгоритма ГОСТ 28147-89 с длиной ключа 256 бит (программный эмулятор платы КРИПТОН или криптоплата КРИПТОН фирмы АНКАД).

Следует отметить, что применяемая в этой версии системы Secret Disk плата КРИПТОН сертифицирована ФАПСИ для защиты государственной тайны и поставляется по отдельному запросу фирмой АНКАД.

Система Secret Disk допускает также подключение внешнего криптомодуля того стандарта и с той длиной ключа, которую пользователь считает возможной для своих приложений.

Важная особенность системы Secret Disk заключается в том, что для доступа к защищенной информации необходим не только вводимый пользователем пароль, но и электронный идентификатор. В качестве такого идентификатора может использоваться обычный электронный ключ для параллельного порта, карточка PCMCIA для ноутбуков или смарт-карта (в этом случае необходимо установить в компьютер специальный считыватель смарткарт).

Система Secret Disk подключается только после того, как пользователь введет пароль и система обнаружит соответствующий идентификатор. Поэтому , если пользователь вытащит из компьютера электронный ключ, злоумышленникам не поможет даже знание пароля.

При работе в критических ситуациях (например, под принуждением) система предоставляет пользователю специальный режим входа с помощью отдельного пароля и ряд блокировок, позволяющих не раскрывать информацию (т.е. доступ к диску будет открыт, но при попытке считать с него данные или переписать их на другой диск будут генерироваться системные ошибки Windows и будет разрушено содержимое памяти электронного идентификатора, без чего невозможно расшифровать содержимое секретного диска).

**Система защиты данных Crypton Sigma.**

Система Crypton Sigma-это программный комплекс, предназначенный для защиты данных на персональном компьютере. По своим возможностям он во многом аналогичен системе Secret Disk. Будучи установленной на компьютере, система Crypton Sigma хранит конфиденциальные данные в зашифрованном виде, не допуская несанкционированный доступ и утечку данных. Для шифрования данных в системе Crypton Sigma используется алгоритм шифрования ГОСТ 28147-89.

Система защиты конфиденциальных данных Crypton Sigma ориентирована на широкий круг пользователей компьютеров-бизнесменов, менеджеров, бухгалтеров, адвокатов и др., т.е. всех тех, кто нуждается в защите профессиональной и личной информации.

Система Crypton Sigma легко устанавливается, проста и надежна в использовании, а также полностью "прозрачна" для всех программ и системных утилит операционной системы. При установке системы Crypton Sigma на компьютере создаются новые логические диски. При записи на эти диски информация автоматически шифруется, а при считывании-расшифровывается. Этот метод прозрачного шифрования позволяет полностью снять с пользователя заботу о защите данных. Работа с защищенными дисками незаметна для пользователя и равносильна встраиванию процедур шифрования/расшифрования в запускаемые приложения. Защищенные системой диски на вид ничем не отличаются от обычных и могут использоваться в локальной или глобальной сети.

Поддерживаемые файловые системы-FAT 16, FAT 32 и NTFS. Система Crypton Sigma может работать как с УКЗД КРИПТОН , так и с его программным эмулятором. Криптографические ключи для защиты диска хранятся на съемном носителе (дискете), а при использовании УКЗД КРИПТОН возможно хранение ключевой информации на устройстве Touch Memory или смарт-карте. Кроме того, можно использовать устройство еТокеп (ключевой носитель для USBпорта). Применение УКЗД

КРИПТОН не позволит злоумышленнику перехватить ключи пользователя с помощью внедренных программ.

Для работы системы Crypton Sigma требуется следующая минимальная конфигурация.

Компьютер:

1. IBM PC/AT, PS/2 (с процессором Х486 или выше) или полностью совместимый;
2. минимум 8 Мбайт оперативной памяти;
3. минимум 3 Мбайт свободного дискового пространства для установки и запуска системы Crypton Sigma.

Программно -аппаратное обеспечение:

1. операционная система Windows 95/98 или Windows NT 4.0;
2. интерфейс Crypton API v.2.2 или выше;
3. УКЗД КРИПТОН с соответствующим драйвером или его программный эмулятор.

Система Crypton Sigma специально разрабатывалась так, чтобы сделать все процедуры управления максимально простыми и ясными. Все, что должен уметь пользователь,-это создать специальный файл (контейнер) для хранения зашифрованных данных и открыть его для доступа через логический диск системы Crypton Sigma.

Контейнер-это специальный файл, создаваемый при помощи Панели Управления системы Crypton Sigma. Контейнер можно открыть для доступа через логический диск, обслуживаемый драйвером системы Crypton Sigma. Все файлы, находящиеся на этом логическом диске, хранятся в зашифрованном виде. Пользователь может создать любое количество контейнеров. Каждый контейнер имеет собственный пароль. Пользователь должен ввести этот пароль при создании контейнера и использовать его для получения доступа к тем данным, которые будут храниться в данном контейнере. Используя Панель Управления Crypton Sigma, пользователь может сменить пароль для выбранного контейнера при условии, что ему известен прежний пароль.

Схема работы системы Crypton Sigma показана на рис. 10.3. Логический диск системы Crypton Sigma создается и управляется драйвером этой системы. Этот логический диск используется для записи (чтения) данных в контейнер. Работа пользователя с таким логическим диском не отличается от работы с любыми другими дисками компьютера.

Рисунок 7.3 – Схема выполнения операций чтения (записи) с логических дисков системой Crypton Sigma

wpgDAДрайвер системы Crypton Sigma обрабатывает запросы операционной системы на чтение (запись) с логических дисков, при этом драйвер автоматически производит шифрование/расшифрование данных. Следует отметить, что драйвер системы Crypton Sigma обрабатывает не все запросы на чтение/запись. Как уже упоминалось, система Crypton Sigma создает и обслуживает собственные логические диски. Драйвер системы обслуживает операции чтения (записи) только с этих логических дисков.

Эти диски доступны точно так же, как и остальные диски на компьютере, и могут обозначаться любыми незанятыми на данный момент буквами, например D:, Е:, К:, Z:.

Данные, записываемые на логический диск, фактически записываются драйвером системы в контейнер системы. Естественно, размер доступной памяти логического диска равен размеру соответствующего контейнера. Максимальный размер контейнера, создаваемого

1. на жестком диске с файловой системой FAT 16, равен 2 Гбайта;
2. на жестком диске с файловой системой FAT 32. равен 4 Гбайта;
3. на жестком диске с файловой системой NTFS, равен 512 Гбайт;
4. на сетевом диске, равен 2 Гбайта.

Минимальный размер контейнера системы равен 5 Кбайт.

Для доступа к зашифрованным данным, хранящимся в контейнере, следует присоединить этот контейнер к выбранному логическому диску, например Е:, и открыть его для доступа, введя соответствующий пароль. После завершения работы с данными следует закрыть этот логический диск для доступа. При этом данные, сохраненные в контейнере, станут недоступными.

Следует заметить, что если пользователь забудет пароль для доступа к данным, хранящимся в контейнере системы Crypton Sigma, то он полностью теряет возможность доступа к этим данным. Высокостойкие алгоритмы шифрования, используемые в системе Crypton Sigma, не позволяют восстановить информацию без знания пароля. Если существует опасность того, что пароль может быть забыт или утрачен, пользователь должен записать его и спрятать в надежном месте.

Отметим основные преимущества системы Crypton Sigma.

*Надежная защита.* Практически ни одна из существующих универсальных программ со встроенной защитой документов не имеет такой надежной защиты как Crypton Sigma. Компания Access Data (США) продает программный пакет, который вскрывает защиту данных в WordPerfect, Lotus 12-3, MS Excel, Symphony, Quattro Pro, Paradox, MS Word. Эта программа не просто перебирает все возможные комбинации паролей она проводит математически обоснованный криптографический анализ и тратит на вскрытие защищенных данных всего лишь несколько секунд. Система Crypton Sigma выгодна отличается использованием стойких и надежных алгоритмов шифрования и не содержит встроенных программных блоков, позволяющих злоумышленнику совершить несанкционированный доступ к зашифрованным данным.

*Высокая степень секретности .* После того как данные записываются на логический диск системы Crypton Sigma, они уже никогда не хранятся на компьютере в открытом (расшифрованном) виде. Расшифрование данных происходит только в момент доступа к ним пользователей, знающих пароль. Система Sigma нигде не хранит паролей, необходимых для доступа к данным. Она лишь проверяет, подходит ли пароль для расшифрования данных, на которые претендует пользователь, точно так же, как замок нигде не хранит дубликат ключа, а только "проверяет", может ли данный ключ открыть его или нет.

*Использование системы в локальных сетях.*

Программное обеспечение Crypton Sigma для Windows 95/98/NT позволяет использовать любой сетевой диск для создания на нем контейнеров и доступа к хранящимся на них данным. Эти сетевые диски могут быть выделены для доступа компьютерами с любой другой, отличной от Windows, операционной системой, например ОС семейства UNIX (OSF/1, LINUX, BSD, Sun OS, AIX и др.), а также Novell, Windows З.хх и др.

Логические диски Crypton Sigma с точки зрения операционной системы или любого другого программного обеспечения выглядят точно так же, как обыкновенные локальные диски компьютера. Поэтому логические диски Crypton Sigma могут быть открыты для доступа через

локальную компьютерную сеть. Таким образом, зашифрованная информация при необходимости может быть доступна для коллективного использования.

*Удобство в использовании.* Система Crypton Sigma проста в использовании и, следовательно, практически не позволяет совершать случайных действий, приводящих к появлению секретной информации на компьютере в открытом виде. Пользователю необходимо только ввести правильный пароль - об остальном позаботится система. После верификации пароля доступ к зашифрованной информации становится прозрачным для всех запускаемых пользователем программ. Все зашифрованные данные автоматически расшифровываются перед тем, как появиться перед пользователем, и автоматически зашифровываются перед записью их на диски, обслуживаемые системой Crypton Sigma.

**Лекция 18**

**Модель компьютерной системы. Методы и средства ограничения доступа к компонентам ЭВМ. Понятие изолированной**

**программной среды.**

**1. Понятие доступа и монитора безопасности**

В теории компьютерной безопасности практически всегда рассматривается модель произвольной КС в виде конечного множества элементов. Указанное множество можно разделить на два подмножества: множество объектов и множество субъектов, данное разделение основано на свойстве элемента «быть активным» или «получать управление» (применяются также термины «использовать ресурсы» или «пользоваться вычислительной мощностью»). Оно исторически сложилось на основе модели вычислительной системы, принадлежащей фон Нейману, согласно которой последовательность исполняемых инструкций (программа, соответствующая понятию «(субъект»)) находится в единой среде с данными, соответствующими понятию «объект».

Модели, связанные с реализацией политики безопасности, не учитывают возможности субъектов по изменению КС, которые могут привести к изменению ее свойств и, как предельный случай, к полной неприменимости той или иной модели к описанию отношений «субъект-объект» в измененной КС.

Этот факт не является недостатком политики безопасности. достоверность работы механизмов реализации политики безопасности считается априорно заданной, поскольку в противном случае невозможна формализация и анализ моделей. Однако вопрос гарантий политики безопасности является ключевым как в теории, так и в практике.

Рассматривая активную роль субъектов в КС, необходимо упомянуть о ряде важнейших их свойств, на которых базируется излагаемая ниже модель.

Во-первых, необходимо заметить, что человек-пользователь воспринимает объекты и получает информацию о состоянии КС через субъекты, которыми он управляет и которые производят отображение информации в воспринимаемом человеком виде.

Во-вторых, угрозы компонентам КС исходят от субъектов сак активной компоненты, порождающей потоки и изменяющей‚ состояние объектов в КС.

В-третьих, субъекты могут влиять друг на друга через изменяемые ими объекты, связанные с другими субъектами, порождая в конечном итоге в системе субъекты (или состояния системы), которые представляют угрозу для безопасности информации или для работоспособности самой системы.

Будем считать разделение КС на субъекты и объекты априорным. Будем считать также, что существует априорный безошибочный критерий различения субъектов и объектов в КС (по свойству активности). Кроме того, считаем в условиях всех утверждений, что декомпозиция КС на субъекты и объекты фиксирована.

Подчеркнем отличие понятия субъекта компьютерной системы от человека-пользователя следующим определением.

Пользователь — лицо (физическое лицо), аутентифицируемое некоторой информацией и управляющее субъектом компьютерной системы через органы управления ЭВМ. Пользователь КС является, таким образом, внешним фактором, управляющим состоянием субъектов. В связи с этим далее будем считать пользовательское управляющее воздействие таким, что свойства субъектов, сформулированные в ниже приводимых определениях, не зависят от него (т.е. свойства субъектов не изменяемы внешним управлением). Смысл данного условия состоит в предположении того факта, что пользователь, управляющий программой, не может через органы управления изменить ее свойства (условие неверно для систем типа компиляторов, средств разработки, отладчиков и др.).

Будем также полагать, что в любой дискретный момент времени множество субъектов КС не пусто (в противном случае соответствующие моменты времени исключаются из рассмотрения и рассматриваются отрезки с ненулевой мощностью множества субъектов).

Введем обозначения:

*O* — множество объектов;

*S*— множество субъектов ();

О*i*—объект ();

S*i* — субъект ().

Субъекты могут порождаться из объектов только активными компонентами, т.е. субъектами.

Объект О*i* — источник для субъекта S*k*, если существует субъект S*i*, в результате воздействия которого на объект О*i* в системе возникает субъект S*k*.

Объект О*i* в момент времени *t* ассоциирован с субъектом S*k,* если состояние объекта О*i* повлияло на состояние субъекта S*k* в момент времени *t*+1

Объекты:

— функционально ассоциированные объекты — те объекты, изменение которых меняет вид ассоциированных субъектов;

— ассоциированные объекты-данные — те объекты, которые ассоциированы с субъектами, но изменение которых не влияет на дальнейший вид ассоциированных субъектов.

Угрозы информации исходят от субъектов, порождающих потоки и изменяющих состояние объектов. Субъекты влияют друг на друга, изменяя объекты, связанные с другими субъектами или порождая субъекты, которые несут угрозу безопасности.

Потоком информации между объектами О*k* и О*j* называется произвольная операция над объектом О*j* ,реализованная в субъекте S*i* и зависящая от О*k*.

Потоки могут создавать или удалять объекты, также реализовывать операции чтения и записи.

Доступом субъекта S*k* к объекту О*i* называется порождение потока информации между некоторыми объектами и объектом О*i.*

Правило разграничения доступа субъектов к объектам — формально описанные потоки, принадлежащие множеству допустимых потоков *L*.

Объекты могут быть записаны в виде последовательности символов некоторого алфавита. Объекты можно сравнивать между собой на совпадение.

Монитор обращений (МО) — субъект, активизирующийся при возникновении потока от любого субъекта к любому объекту.

Можно выделить два вида МО:

— индикаторный МО — устанавливающий только факт обращения субъекта к объекту;

— содержательный МО — субъект, полностью участвующий в потоке от субъекта к объекту, при этом информация проходит через его ассоциированные объекты-данные и существует тождественное отображение объекта на какой-либо ассоциированый объект МО.

Монитор безопасности объектов (МБО) монитор обращений, который разрешает поток, принадлежащий только множеству легального доступа *L*. Разрешение потока в данном случае поyимается как выполнение операции над объектом-получателем потока, а запрещение — как невыполнение (т.е. неизменность объекта-получателя потока).

Монитор безопасности объектов фактически является механизмом реализации политики безопасности в компьютерной системе.

**2. Обеспечение гарантий выполнения политики безопасности**

При изменении функционально ассоциированных с субъектом реализации политики безопасности (МБО) объектов могут измениться и свойства самого МБО, заключающиеся в фильтрации потоков, и как следствие могут возникнуть потоки, принадлежащие множеству неразрешенных потоков *N*. Введем в Связи с этим понятие корректности субъектов.

**Субъекты** S*i* и S*j* называются **невлияющими** друг на друга (Или корректными относительно друг друга), если в любой момент времени отсутствует поток (изменяющий состояние объекта) между любыми объектами О*i* и О*j*, ассоциированными соответственно с субъектами S*i* и S*j*. Причем О*j* не является ассоциированным объектом S*i* а О*i* — ассоциированным объектом S*j*.

Смысл понятия корректности можно пояснить на примере: существующие в едином пространстве оперативной памяти программы не должны иметь функциональных возможностей изменения «чужого» вектора кода и состояния переменных.

**Субъекты** S*i* и S*j* называются абсолютно не влияющими друг на друга (или абсолютно корректными относительно друг друга), если в условиях предыдущего определения множества ассоциированных объектов указанных субъектов не имеют пересечения ().

Монитор безопасности объектов разрешает порождение потоков только из множества *L*, если все существующие в системе субъекты абсолютно корректны относительно него и друг друга.

Сформулированное утверждение накладывает весьма жест кие и трудноисполнимые условия на свойства субъектов.

**Монитор порождения субъектов** (МПС) — субъект, активизирующийся при любом порождении субъектов.

**Монитор безопасности субъектов** (МБС) — такой МПС, который разрешает порождение только фиксированного под- множества субъектов.

Обозначим через Е подмножество субъектов, порождения которых разрешены МБС.

Компьютерная система называется **замкнутой по порождению субъектов** (замкнутой программной средой), если в ней действует МБС.

Множество **субъектов** АС называется **изолированным (абсолютно изолированным)**, если в ней действует МБС и субъекты из порождаемого множества корректны (абсолютно корректны) относительно друг друга и МБС.

Любое подмножество субъектов (изолированная программная среда ИПС, абсолютно изолированная программная среда АИПС), включающее МБС, также составляет ИПС (АИПС).

Дополнение ИПС (АМПС) субъектом, корректным (абсолютно корректным) относительно других субъектов, является ИПС.

Теперь возможно переформулировать достаточное условие тированного выполнения политики безопасности следующим образом.

Если в абсолютно изолированной компьютерной системе существует МБО и порождаемые субъекты абсолютно корректен относительно МВО, а также МБС абсолютно корректен относительно МБО, то в такой КС реализуется только доступ, описанный правилами разграничения доступа (ПРД).

Легко видеть, что данное утверждение является более конструктивным, чем предыдущее достаточное условие гарантированной защищенности, поскольку ранее требовалась корректность МВО относительно произвольного субъекта, что практически невозможно. В данном же случае множество субъектов ограничено за счет применения механизма МБС, и возможно убедиться в попарной корректности порождаемых субъектов.

При рассмотрении операции порождения субъекта возникает весьма важная проблема, связанная с тем, что в реальных АС одинаково поименованные объекты могут иметь различное состояние в пространстве (например, быть размещенными в различных каталогах) или во времени. Предположим, что зафиксировано состояние объекта О*j* в некоторый момент времени *t*0. Будем обозначать состояние объекта О*j* в момент времени *t* как О*j*[*t*].

Операция порождения субъекта Сгеаtе >S*i*, называется **порождением с контролем неизменности объекта**, если для любого момента времени *t*> *t*0, в который активизирована операция порождения объекта Сгеаtе, порождение субъекта S*i* возможно только при тождественности объектов О*j*[*t*0] и О*j* [*t*].

Порожденные субъекты S*i* [*t*1] и S*i* [*t*2] тождественны, если выполняется операция порождения с контролем неизменности объектов.

Если в момент времени *t*0 в изолированной АС действует только порождение субъектов с контролем неизменности объекта и существуют потоки от любого субъекта к любому объекту, не противоречащие условию корректности (абсолютной корректности) субъектов, то в любой момент времени *t*> *t*0 АС также остается изолированной (абсолютно изолированной).

**3. Методология проектирования гарантированно защищенных КС**

Сущность данной методологии состоит в том, что при проектировании защитных механизмов КС необходимо опираться на совокупность приведенных выше достаточных условий, которые должны быть реализованы для субъектов, что гарантирует защитные свойства, определенные при реализации МБО в КС (т.е. гарантированное выполнение заданной МБО политики безопасности).

Рассмотренная концепция изолированной программной среды является расширением зарубежных подходов к реализации ядра безопасности.

Обычно модель функционирования ядра безопасности изображается в виде следующей схемы, представленной на рис. 8.1.

«База данных защиты» означает объект, содержащий в себе информацию о потоках множества *L* (защита по «белому списку» — разрешения на потоки) или *N* (защита по «черному списку» — запрещение на потоки).



*Рис. 8.1. Классическая модель ядра безопасности*

Для учета влияния субъектов в КС необходимо рассматривать расширенную схему взаимодействия элементов системы реализации и гарантирования ПБ.

В рис. 8.2 подчеркнута роль монитора безопасности субъектов при порождении субъектов из объектов. Взаимодействие субъектов и объектов при порождении потоков уточнено введением ассоциированных с субъектом объектов. Конструкция ОУ на схеме обозначает объект управления, т.е. объект, содержащий информацию о разрешенных значениях отображения Сгеаtе (об элементах множества L или N) и Сгеаtе. Объект управления может быть ассоциирован (ассоциированный объект - данные) как с МБО, так и с МБС.



*Рис. 8.2. Ядро безопасности с учетом контроля порождения субъектов*