Защита информации в КС от несанкционированного доступа

Система разграничения доступа к информации в КС

Для осуществления НСДИ злоумышленник не применяет никаких аппаратных или программных средств, не входящих в состав КС.

Он осуществляет НСДИ, используя:
• знания о КС и умения работать с ней;

• сведения о системе защиты информации;

• сбои, отказы технических и программных средств;

• ошибки, небрежность обслуживающего персонала и пользователей.

Для защиты информации от НСД создается система разграничения доступа к информации. Получить несанкционированный доступ к информации при наличии системы разграничения доступа (СРД) возможно только при сбоях и отказах КС, а также используя слабые места в комплексной системе защиты информации.

Чтобы использовать слабости в системе защиты, злоумышленник должен знать о них.

Одним из путей добывания информации о недостатках системы защиты является изучение механизмов защиты.

Злоумышленник может тестировать систему защиты путем непосредственного контакта с ней. В этом случае велика вероятность обнаружения системой защиты попыток ее тестирования. В результате этого службой безопасности могут быть предприняты дополнительные меры защиты.

Гораздо более привлекательным для злоумышленника является другой подход. Сначала получается копия программного средства системы защиты или техническое средство защиты, а затем производится их исследование в лабораторных условиях. Кроме того, создание неучтенных копий на съемных носителях информации является одним из распространенных и удобных способов хищения информации. Этим способом осуществляется несанкционированное тиражирование программ. Скрытно получить техническое средство защиты для исследования гораздо сложнее, чем программное, и такая угроза блокируется средствами и методами
обеспечивающими целостность технической структуры КС.

Для блокирования несанкционированного исследования и копирования информации КС используется комплекс средств и мер защиты, которые объединяются в систему защиты от исследования и копирования информации (СЗИК).

Таким образом, СРД и СЗИК могут рассматриваться как подсистемы системы защиты от НСДИ.

Управление доступом

Исходной информацией для создания СРД является решение владельца (администратора) КС о допуске пользователей к определенным информационным ресурс КС.

Так как информация в КС хранится, обрабатывается и передается файлами (частями файлов), то доступ к информации регламентируется на уровне файлов (объектов доступа).

Сложнее организуется доступ в базах данных, в которых он может регламентироваться к отдельным ее частям по определенным правилам. При определении полномочий доступа администратор устанавливает операции, которые разрешено выполнять пользователю (субъекту доступа).

Различают следующие **операции** с **файлами):**

• чтение (R);

• запись;

• выполнение программ (E).

Операция записи в файл имеет две модификации.

Субъекту доступа может быть дано право осуществлять запись с изменением содержимого файла (W).

Другая организация доступа предполагает разрешение только дописывания в файл, без изменения старого содержимого (A).

В КС нашли применение два подхода к организации разграничения доступа:

• матричный:

• полномочный (мандатный).

Матричное управление доступом предполагает использование матриц доступа.

Матрица доступа представляет собой таблицу, в которой объекту доступа соответствует столбец Oj, а субъекту доступа - строка Si. На пересечении столбцов и строк записываются операция или операции, которые допускается выполнять субъекту доступа i с объектом доступа j.

	O_1	O_2	...	O_j	...	0_m
S_i	R	R,W		E		R
S_2	R,A	–		R		E
...						
S_i	R	–		–		R
...						
S_n	R,W	–		E		E

Матричное управление доступом позволяет с максимальной детализацией установить права субъекта доступа по выполнению разрешенных операций над объектами доступа.

Такой подход нагляден и легко реализуем. Однако в реальных системах из-за большого количества субъектов и объектов доступа матрица доступа достигает таких размеров, при которых сложно поддерживать ее в адекватном состоянии.

Полномочный или *мандатный* метод базируется на многоуровневой модели защиты.

Такой подход построен по аналогии с ≪ручным≫ конфиденциальным (секретным) делопроизводством.

Документу присваивается уровень конфиденциальности (гриф секретности), а также могут присваиваться метки, отражающие категории конфиденциальности (секретности) документа.

Таким образом, конфиденциальный документ имеет гриф конфиденциальности (конфиденциально, строго конфиденциально, секретно, совершенно секретно и т. д.) и может иметь одну или несколько
меток, которые уточняют категории лиц, допущенных к этому документу (≪для руководящего состава≫, ≪для инженернотехнического состава≫ и т. д.).

Субъектам доступа устанавливается уровень допуска, определяющего максимальный для данного субъекта уровень конфиденциальности документа, к которому разрешается допуск. Субъекту доступа устанавливаются также категории, которые связаны с метками документа.

Правило разграничения доступа заключается в следующем:

лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

В КС все права субъекта доступа фиксируются в его мандате.

Объекты доступа содержат метки, в которых записаны признаки конфиденциальности. Права доступа каждого субъекта и характеристики конфиденциальности каждого объекта отображаются в виде совокупности уровня конфиденциальности и набора категорий конфиденциальности.

Мандатное управление позволяет упростить процесс регулирования доступа, так как при создании нового объекта достаточно создать его метку.

Однако при таком управлении приходится завышать конфиденциальность информации из-за невозможности детального разграничения доступа.

Если право установления правил доступа к объекту предоставляется владельцу объекта (или его доверенному лицу), то такой метод контроля доступа к информации называется *дискреционным.*

Состав системы разграничения доступа

Система разграничения доступа к информации должна содержать четыре функциональных блока:

• блок идентификации и аутентификации субъектов доступа;

• диспетчер доступа;

• блок криптографического преобразования информации при ее хранении и передаче;

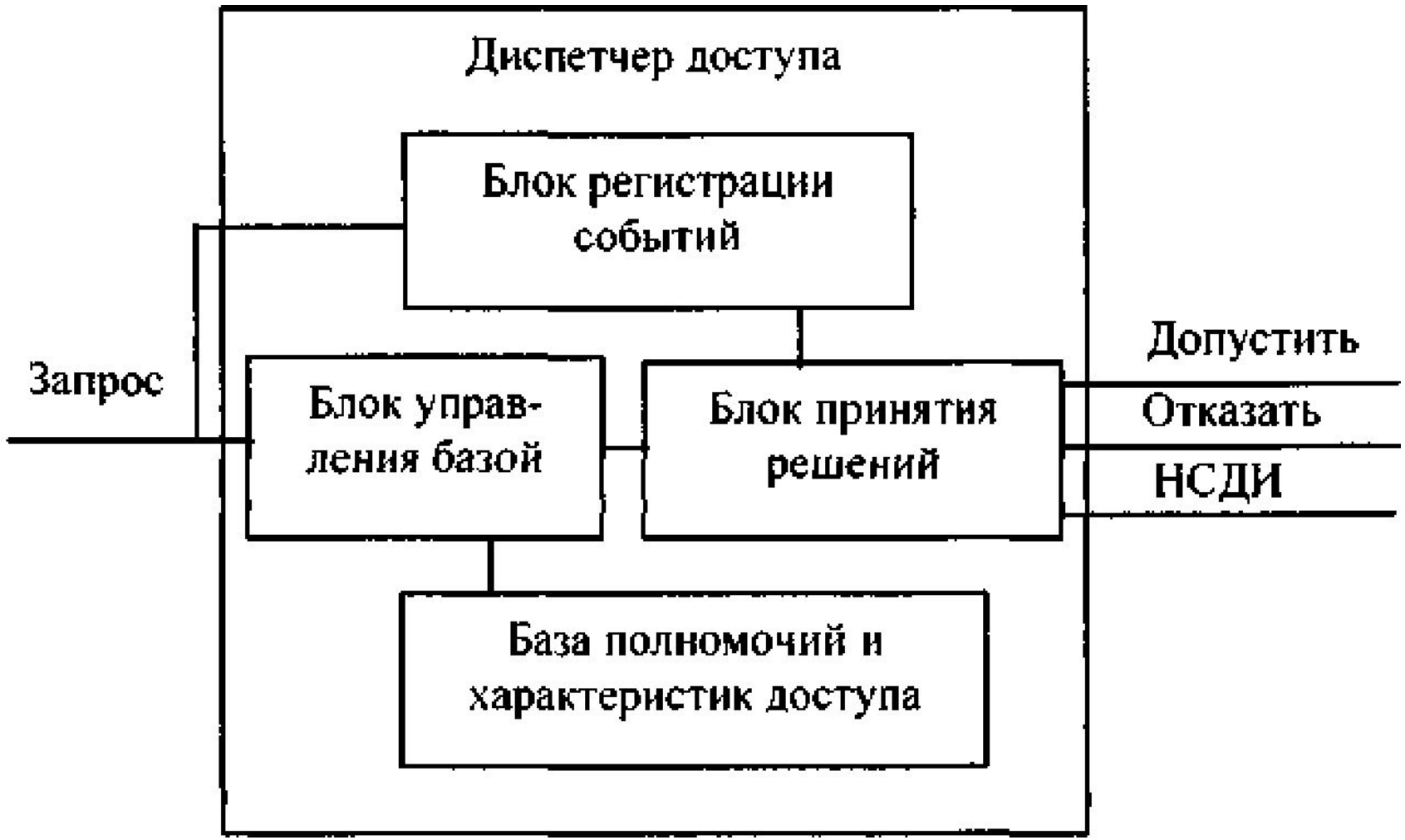
• блок очистки памяти.

Идентификация и аутентификация субъектов осуществляется в момент их доступа к устройствам, в том числе и дистанционного доступа.

Диспетчер доступа реализуется в виде аппаратно программных механизмов и обеспечивает необходимую дисциплину разграничения доступа субъектов к объектам доступа (в том числе и к аппаратным блокам, узлам, устройствам).
Диспетчер доступа разграничивает доступ к внутренним ресурсам КС субъектов, уже получивших доступ к этим системам. Необходимость использования диспетчера доступа возникает только в многопользовательских КС.

Запрос на доступ i-го субъекта и j-му объекту поступает в блок управления базой полномочий и характеристик доступа и в блок регистрации событий. Полномочия субъекта и характеристики объекта доступа анализируются в блоке принятия решения, который выдает сигнал разрешения выполнения запроса, либо сигнал отказа в допуске. Если число попыток субъекта допуска получить доступ к запрещенным для него объектам превысит определенную границу (обычно 3 раза), то блок принятия решения на основании данных блока регистрации выдает сигнал ≪НСДИ≫ администратору системы безопасности.

Администратор может блокировать работу субъекта, нарушающего правила доступа в системе, и выяснить причину нарушений. Кроме преднамеренных попыток НСДИ диспетчер фиксирует нарушения правил разграничения, явившихся следствием отказов, сбоев аппаратных и программных **средств,** а также вызванных ошибками персонала **и пользователей.**


Диспетчер доступа
Блок регистрации событий
Запрос
Блок управления базой
Блок принятия решений
Допустить
Отказать
НСДИ
База полномочий и характеристик доступа

Следует отметить, что в распределенных КС криптографическое закрытие информации является единственным надежным способом защиты от НСДИ.

В СРД должна быть реализована функция очистки оперативной памяти и рабочих областей на внешних запоминающих устройствах после завершения выполнения программы, обрабатывающей конфиденциальные данные.

Причем очистка должна производиться путем записи в освободившиеся участки памяти определенной последовательности двоичных кодов, а не удалением только учетной информации о файлах из таблиц ОС, как это делается **при** стандартном удалении средствами ОС.

Концепция построения систем разграничения доступа

В основе построения СРД лежит концепция разработки защищенной универсальной ОС на базе ядра безопасности.

Под **ядром безопасности** понимают локализованную, минимизированную, четко ограниченную и надежно изолированную совокупность программно-аппаратных механизмов, доказательно правильно реализующих функции диспетчера доступа.

Правильность функционирования ядра безопасности доказывается путем полной формальной верификации его программ и пошаговым доказательством их соответствия выбранной математической модели защиты.

Применение ядра безопасности требует провести изменения ОС и архитектуры ЭВМ.

Ограничение размеров и сложности ядра необходимо для обеспечения его верифицируемости.

Для аппаратной поддержки защиты и изоляции ядра в архитектуре ЭВМ должны быть предусмотрены:

• многоуровневый режим выполнения команд;

• использование ключей защиты и сегментирование памяти;

• реализация механизма виртуальной памяти с разделением адресных пространств;

• аппаратная реализация части функций ОС;

• хранение программ ядра в постоянном запоминающем устройстве (ПЗУ);

• использование новых архитектур ЭВМ, отличных от фоннеймановской архитектуры (архитектуры с реализацией абстрактных типов данных, архитектуры с привилегиями и др.).

Обеспечение многоуровневого режима выполнения команд является главным условием создания ядра безопасности.

Таких уровней должно быть не менее двух. Часть машинных командЭВМ должна выполняться только в режиме работы ОС.
Основной проблемой создания высокоэффективной защиты от НСД является предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние. Для современных сложных ОС практически нет доказательств отсутствия возможности несанкционированного получения пользовательскими программами статуса программ ОС.

Использование ключей защиты, сегментирование памяти и применение механизма виртуальной памяти предусматривает аппаратную поддержку концепции изоляции областей памяти при работе ЭВМ в мультипрограммных режимах.
Эти механизмы служат основой для организации работы ЭВМ в режиме виртуальных машин. Режим виртуальных машин позволяет создать наибольшую изолированность пользователей, допуская использование даже различных ОС пользователями в режиме разделения времени.

Аппаратная реализация наиболее ответственных функций ОС и хранение программ ядра в ПЗУ существенно повышают изолированность ядра, его устойчивость к попыткам модификации.

Аппаратно должны быть реализованы прежде всего функции идентификации и аутентификации субъектов доступа, хранения атрибутов системы защиты, поддержки криптографического закрытия информации, обработки сбоев и отказов и некоторые другие.

Универсальные ЭВМ и их ОС, используемые ранее, практически не имели встроенных механизмов защиты от НСД. Такие распространенные ОС как IBM System/370, MS-DOS и целый ряд других ОС не имели встроенных средств идентификации и аутентификации и разграничения доступа. Более современные универсальные ОС UNIX, VAX/VMS, Solaris и др. имеют встроенные
механизмы разграничения доступа и аутентификации. Однако возможности этих встроенных функций ограничены и не могут удовлетворять требованиям, предъявляемым к защищенным ЭВМ.

Имеется два пути получения защищенных от НСД КС:

• создание специализированных КС;

• оснащение универсальных КС дополнительными средствами защиты.

Первый путь построения защищенных КС пока еще не получил широкого распространения в связи с нерешенностью целого ряда проблем.
Основной из них является отсутствие эффективных методов разработки доказательно корректных аппаратных и программных средств сложных систем.
Среди немногих примеров специализированных ЭВМ можно назвать систему SCOMP фирмы ≪Honeywell≫, предназначенную для использования в центрах коммутации вычислительных сетей, обрабатывающих секретную информацию. Система разработана на базе концепции ядра безопасности. Узкая специализация позволила создать защищенную систему, обеспечивающую требуемую эффективность функционирования по прямому назначению.

Современные системы защиты ПЭВМ от несанкционированного доступа к информации

В качестве примеров отдельных программ, повышающих защищенность КС от НСД, можно привести утилиты из пакета Norton Utilities, такие как программа шифрования информации при записи на диск Diskreet или Secret disk, программа стирания информации с диска Wipelnfo, программа контроля обращения к дискам Disk Monitor и др.

Отечественными разработчиками предлагаются программные системы защиты ПЭВМ ≪Снег-1.0≫, ≪Кобра≫, ≪Страж-1.1≫ и др. В качестве примеров отечественных аппаратно-программных средств защиты, имеющих сертификат Гостехкомиссии, можно привести системы ≪Аккорд-4≫, ≪DALLAS LOCK 3.1≫, ≪Редут≫, ≪ДИЗ-1≫.

Аппаратно-программные комплексы защиты реализуют максимальное число защитных механизмов:

- идентификация и аутентификация пользователей;
- разграничение доступа к файлам, каталогам, дискам;
- контроль целостности программных средств и информации;
- возможность создания функционально замкнутой среды пользователя;
- защита процесса загрузки ОС;
- блокировка ПЭВМ на время отсутствия пользователя;
- криптографическое преобразование информации;
- регистрация событий;
- очистка памяти.

Программные системы защиты в качестве идентификатора используют, как правило, только пароль.

Пароль может быть перехвачен резидентными программами двух видов.

Программы первого вида перехватывают прерывания от клавиатуры, записывают символы в специальный файл, а затем передают управление ОС.
После перехвата установленного числа символов программа удаляется из ОП.

Программы другого вида выполняются вместо штатных программ считывания пароля. Такие программы первыми получают управление и имитируют для пользователя работу со штатной программой проверки пароля. Они запоминают пароль, имитируют ошибку ввода пароля и передают управление штатной программе парольной идентификации. Отказ при первом наборе пароля пользователь воспринимает как сбой системы или свою ошибку и осуществляет повторный набор пароля, который должен завершиться допуском его к работе.

При перехвате пароля в обоих случаях пользователь не почувствует, что его пароль скомпрометирован. Для получения возможности перехвата паролей злоумышленник должен изменить программную структуру системы.
В некоторых программных системах защиты (≪Страж-1.1≫) для повышения достоверности аутентификации используются съемные магнитные диски, на которых записывается идентификатор пользователя.

Значительно сложнее обойти блок идентификации и аутентификации в аппаратно-программных системах защиты от НСД.

В таких системах используются электронные идентификаторы, чаще всего - Touch Memory.

Для каждого пользователя устанавливаются его полномочия в отношении файлов, каталогов, логических дисков. Элементы, в отношении которых пользователю запрещены любые действия, становятся ≪невидимыми≫ для него, т. е. они не отображаются на экране монитора при просмотре содержимого внешних запоминающих устройств.

Для пользователей может устанавливаться запрет на использование таких устройств, как накопители на съемных носителях, печатающие устройства. Эти ограничения позволяют предотвращать реализацию угроз, связанных с попытками несанкционированного копирования и ввода информации, изучения системы защиты.

В наиболее совершенных системах реализован механизм контроля целостности файлов с использованием хэш-функции/

Причем существуют системы, в которых контрольная характеристика хранится не только в ПЭВМ, но и в автономном ПЗУ пользователя.

Постоянное запоминающее устройство, как правило, входит в состав карты или жетона, используемого для идентификации пользователя.

Так в системе ≪Аккорд-4≫ хэш-функции вычисляются для контролируемых файлов и хранятся в специальном файле в ПЭВМ, а хэш-функция, вычисляемая для специального файла, хранится в Touch Memory.

Очень эффективным механизмом борьбы с НСДИ является создание функционально-замкнутых сред пользователей. Суть его состоит в следующем.

Для каждого пользователя создается меню, в которое попадает пользователь после загрузки ОС. В нем указываются программы, к выполнению которых допущен пользователь. Пользователь может выполнить любую из программ из меню. После выполнения программы пользователь снова попадает в меню. Если эти программы не имеют возможностей инициировать выполнение других программ, а также предусмотрена корректная обработка ошибок, сбоев и отказов, то пользователь не сможет выйти за рамки установленной замкнутой функциональной среды.

Такой режим работы вполне осуществим во многих АСУ.

Защита процесса загрузки ОС предполагает осуществление загрузки именно штатной ОС и исключение вмешательства в ее структуру на этапе загрузки. Для обеспечения такой защиты на аппаратном или программном уровне блокируется работа всех ВЗУ, за исключением того, на котором установлен носитель со штатной ОС.

При организации многопользовательского режима часто возникает необходимость на непродолжительное время отлучиться от рабочего места, либо передать ЭВМ другому пользователю.

На это время необходимо блокировать работу ЭВМ. В этих случаях очень удобно использовать электронные идентификаторы, которые при работе должны постоянно находиться в приемном устройстве блока идентификации ЭВМ. При изъятии идентификатора гасится экран монитора и блокируются устройства управления.

При предъявлении идентификатора, который использовался при доступе к ЭВМ, осуществляется разблокировка, и работа может быть продолжена.
При смене пользователей целесообразно производить ее без выключения ЭВМ. Для этого необходим аппаратно-программный или программный механизм корректной смены полномочий. Если предыдущий пользователь корректно завершил работу, то новый пользователь получает доступ со своими полномочиями после успешного завершения процедуры аутентификации.

Одним из наиболее эффективных методов разграничения доступа является криптографическое преобразование информации.

Этот метод является универсальным. Он защищает информацию от изучения, внедрения программных закладок, делает операцию копирования бессмысленной.

Здесь необходимо лишь отметить, что пользователи могут использовать одни и те же аппаратно-программные или программные средства криптографического преобразования или применять индивидуальные средства.

Для своевременного пресечения несанкционированных действий в отношении информации, а также для контроля за соблюдением установленных правил субъектами доступа, необходимо обеспечить регистрацию событий, связанных с защитой информации.

Степень подробности фиксируемой информации может изменяться и обычно определяется администратором системы защиты. Информация накапливается на ВЗУ. Доступ к ней имеет только администратор системы защиты.

Важно обеспечивать стирание информации в ОП и в рабочих областях ВЗУ. В ОП размещается вся обрабатываемая информация, причем, в открытом виде. Если после завершения работы пользователя не осуществить очистку рабочих областей памяти всех уровней, то к ней может быть осуществлен несанкционированный доступ.