Методы и средства защиты компьютерной информации. Методы обеспечения информационной безопасности. Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта)

Методы и средства защиты

Проблему защиты информации в базах данных целесообразно рассматривать совместно с проблемой защиты вычислительной системы (ВС) в целом. Действительно, средой функционирования СУБД - основного инструмента управления данными, является среда вычислительной системы. Кроме того, известные из литературы методы и средства защиты программ и данных в равной мере относятся к программам (СУБД, приложения, хранимые процедуры и т. д.) и данным (базы данных, словари данных) из баз данных.

Методы и средства защиты

Знание принципов построения систем защиты и возможностей, предоставляемых различными компонентами вычислительной системы (операционной системой, программами обслуживания, СУБД, специализированными пакетами защиты и отдельными устройствами) позволяет оценить уязвимость ИС и грамотно организовать в ней защиту конфиденциальной информации.

Методы и средства защиты

Для организации комплексной защиты информации в ВС в общем случае может быть предусмотрено 4 защитных уровня.

1. Внешний уровень, охватывающий всю территорию расположения ВС.
2. Уровень отдельных сооружений или помещений расположения устройств ВС и линий связи с ними.
3. Уровень компонентов ВС и внешних носителей информации.
4. Уровень технологических процессов хранения, обработки и передачи информации.

Методы и средства защиты

Первые три уровня обеспечивают в основном физическое препятствие доступу путем ограждения, системы сигнализации, организации пропускного режима, экранирования проводов и т. д. Последний уровень предусматривает логическую защиту информации в том случае, когда физический доступ к ней имеется.

Существующие методы защиты можно разделить на четыре основных класса:

1. физические;
2. аппаратные;
3. программные;
4. организационные.

Физическая защита используется в основном на верхних уровнях защиты и состоит в физическом преграждении доступа посторонних лиц в помещения ВС на пути к данным и процессу их обработки. Для физической защиты применяются следующие средства:

- сверхвысокочастотные, ультразвуковые и инфракрасные системы обнаружения движущихся объектов, определения их размеров, скорости и направления перемещения;
- лазерные и оптические системы, реагирующие на пересечение нарушителями световых лучей;
- телевизионные системы наблюдения за охраняемыми объектами;
- кабельные системы, в которых небольшие объекты окружают кабелем, чувствительным к приближению нарушителя;
- системы защиты окон и дверей от несанкционированного проникновения, а также наблюдения и подслушивания;
- механические и электронные замки на двери и ворота;
- системы нейтрализации излучений.

Аппаратная защита реализуется аппаратурой в составе ЭВМ или с помощью специализированных устройств. Основными аппаратными средствами защиты являются средства защиты процессоров и основной памяти, устройств ввода-вывода, систем передачи данных по каналам связи, систем электропитания, устройств внешней памяти и т. д.

Аппаратные средства защиты процессоров производят контроль допустимости выдаваемых из программ команд. Средства защиты памяти обеспечивают режим совместного использования и разграничения оперативной памяти при выполнении программ. К аппаратным средствам защиты устройств ввода-вывода относятся различные схемы блокировки от несанкционированного использования. Средства защиты передачи данных по каналам связи представляют собой схемы засекречивания (шифрования) информации.

Программная защита реализуется с помощью различных программ: операционных систем, программ обслуживания, антивирусных пакетов, инструментальных систем (СУБД, электронных таблиц, текстовых процессоров, систем программирования и т. д.), специализированных программ защиты и готовых прикладных программ.

Организационная защита реализуется совокупностью направленных на обеспечение защиты информации организационно-технических мероприятий, разработкой и принятием законодательных актов по вопросам защиты информации, утверждением морально-этических норм использования информации в обществе и т.д.

Программно-аппаратные методы защиты

С помощью программно-аппаратных средств можно в определенной мере решать как основные задачи защиты ИПО в ВС (от хищения, от потери, от сбоев и отказов оборудования), так и защиту от ошибок в программах.

Решение этих задач в системах защиты обеспечивается следующими способами:

- защитой от несанкционированного доступа (НСД) к ресурсам со стороны пользователей и программ;
- защитой от несанкционированного использования (НСИ) ресурсов при наличии доступа;
- защитой от некорректного использования ресурсов;
- внесением структурной, функциональной и информационной избыточности;
- высоким качеством разработки программно-аппаратных средств.

Программно-аппаратные методы защиты

Для защиты от НСД прежде всего необходима эффективная система регистрации попыток доступа в систему со стороны пользователей и программ, а также мгновенная сигнализация о них отвечающим за безопасность ВС лицам. Именно отсутствие надежной системы регистрации и сигнализации при НСД, а также наличие обходных путей или «дыр» в ВС, является причиной незаконного проникновения в систему. Чтобы регистрировать события подключения к системе, в ВС обычно ведется специальный журнал или база данных.

Защита от НСД со стороны пользователей в современных системах в основном реализуется двумя основными способами: парольной защитой, а также путем идентификации и аутентификации.

Программно-аппаратные методы защиты

Простейшая парольная защита является достаточно слабым средством, особенно если пароль не шифруется. Основной ее недостаток состоит в том, что все пользователи, использующие одинаковый пароль, с точки зрения ВС неразличимы. Неудобство парольной защиты для пользователя состоит в том, что надо запоминать пароль. Если он простой и короткий, значит, его легко подобрать, если сложный - его нужно куда-нибудь записать. При небрежном отношении к записям пароль может стать достоянием других.

Более серьезный контроль доступа в систему получается, если каждого подключающегося пользователя сначала идентифицировать, затем убедиться, что это именно он, а не другой (аутентифицировать), и при запросе ресурсов контролировать полномочия (проверять право запрашивать ресурсы системы).

Программно-аппаратные методы защиты

Идентификация пользователей может выполняться, например, с помощью паролей. Для аутентификации, или проверки подлинности пользователя, часто используют следующие способы:

- запрос секретного пароля;
- запрос какой-либо информации сугубо индивидуального характера;
- проверка наличия физического объекта, представляющего собой электронный аналог обычного ключа (электронный ключ);
- применение микропроцессорных карточек;
- активные средства опознавания;
- биометрические средства.

Программно-аппаратные методы защиты

Более перспективными средствами аутентификации являются так называемые активные средства распознавания. Примером такого средства является система, состоящая из миниатюрного слабосигнального радиопередатчика и соответствующего радиоприемника.

Из множества существующих средств аутентификации наиболее надежными (но и дорогими) считаются биометрические средства. В них опознание личности осуществляется по отпечаткам пальцев, форме ладони, сетчатке глаза, подписи, голосу и другим физиологическим параметрам человека. Некоторые системы идентифицируют человека по манере работы на клавиатуре. Основным достоинством систем такого класса является высокая надежность аутентификации.

Программно-аппаратные методы защиты

Одной из разновидностей несанкционированных программ являются компьютерные вирусы. Количество известных компьютерных вирусов постоянно возрастает. Появилась даже новая инженерная дисциплина - **компьютерная вирусология**. Последствия воздействия компьютерных вирусов могут быть разнообразными: от внешне необычных эффектов на мониторе компьютера и простого замедления работы ЭВМ до краха вычислительной системы или сети. Отсюда возникает необходимость защиты от компьютерных вирусов на всех стадиях их развития и в особенности на стадиях их проникновения в систему и размножения. Для этого в систему защиты включают средства диагностирования состояния программно-аппаратных средств, локализации и удаления вирусов, устранения последствий их воздействия.

Программно-аппаратные методы защиты

Обеспечение защиты от НСИ ресурсов, как и от НСД, требует применения средств регистрации запросов защищаемых ресурсов ВС и сигнализации в случаях попыток незаконного их использования. Заметим, что речь ведется о важнейших с точки зрения защиты ресурсах. Если постоянно регистрировать все события обо всех запросах на ресурсы в ВС, на остальную работу не хватит процессорного времени.

Для защиты информационно-программных ресурсов ВС от несанкционированного использования применяются следующие варианты защиты: от копирования, исследования (программ), просмотра (данных), модификации и удаления.

Для защиты программы от несанкционированного копирования можно в исполняемом коде выполнить привязку к оборудованию. Тогда копия программы не будет работать на другом компьютере.

Программно-аппаратные методы защиты

Под защитой от исследования программ понимаются такие средства, которые не позволяют или затрудняют изучение системы защиты программы. Например, после нескольких неудачных попыток подключения к программе, имеющей парольную защиту, целесообразно блокировать дальнейшие попытки подключения к ней либо предусмотреть средства самоликвидации.

- Защиту файлов с исполняемыми программами или данными от модификации можно сделать путем сверки некоторой характеристики файла (контрольной суммы) с эталоном. Тогда, если кто-нибудь изменит содержимое файла, изменится его контрольная сумма, что сразу же обнаружится. Средства проверки контрольной суммы можно вставить в программу (для программных файлов) либо поместить в программную систему контроля модификации файлов (программ и данных).

Программно-аппаратные методы защиты

Достаточно мощным средством защиты данных от просмотра является их шифрование. Расшифровка информации требует знания ключа шифрования. Подбор последнего даже при современном уровне компьютерной техники представляет трудоемкую задачу.

- Шифрование незаменимо для защиты информации от раскрытия ее содержания при хранении информации в файлах или базах данных, а также при передаче по линиям связи: проводным, кабельным и радиоканалам.
- Шифрование данных осуществляется в темпе поступления информации (On-Line) и в автономном режиме (Off-Line). Первый способ применяется к основном в системах приема-передачи информации, а второй - для засекречивания хранимой информации.

Программно-аппаратные методы защиты

Защита от некорректного использования ресурсов традиционно выполняется программами ОС. Функции защиты от некорректного использования ресурсов ВС предусматривают, по крайней мере, следующие действия: изолирование друг от друга участков оперативной памяти, выделенных различным программам, защиту системных областей внешней памяти и контроль допустимости команд ЦП.

- В программном обеспечении на более высоком, чем ОС, уровне необходимо обеспечить корректность использования прикладных ресурсов: документов, изображений, баз данных, сообщений и т. п. На практике возможны ситуации, когда корректные с точки зрения операционной системы файлы содержат не совсем верную или противоречивую информацию из предметной области. Другими словами, прикладное программное обеспечение тоже должно обеспечивать целостность и непротиворечивость данных.

Одним из важнейших методов устранения или сведения к минимуму последствий сбоев и отказов в работе ВС является внесение структурной, функциональной и информационной избыточности (резервирования).

- **Структурная избыточность** означает резервирование аппаратных компонентов ВС на различных уровнях: ЭВМ (дублирование серверов обработки); отдельных устройств (дублирование процессоров или накопителей на магнитных дисках - зеркальные диски) и схем устройств (мажоритарные схемы выполнения операций).
- **Функциональное резервирование** означает организацию вычислительного процесса, при которой функции управления, хранения и обработки информации реализуются несколькими элементами системы. При отказе функционального элемента его заменяет другой элемент. Примером функциональной избыточности может служить запуск нескольких одинаковых программ в многозадачной операционной системе.
- **Информационное резервирование** используется для предотвращения полной потери информации и реализуется путем одноразового или периодического копирования и архивирования наиболее ценной информации. К ней прежде всего можно отнести прикладные программы пользователя, а также данные различных видов: документы, БД, файлы и т. д., а также основные программы ОС, типовое ПО (СУБД, текстовые, табличные и графические процессоры и т. п.).

Своевременное выявление сбоев и отказов оборудования, а также физических и логических дефектов на носителях информации невозможно без организации тестирования аппаратно-программных средств. **Тестирование** может выполняться в специально отведенное время и в процессе работы (например, в интервалы простоя оборудования).

Многие причины потери информации в процессе обычного функционирования системы, а также в результате происходящих в системе сбоев и отказов, кроются в наличии ошибок или неточностей, **заложенных на этапах проектирования ВС**.

Для устранения или сведения к минимуму ошибок, которые существенно снижают общую защищенность ВС, следует использовать современные методы защиты на всех этапах жизненного цикла аппаратно-программного обеспечения ВС: системного анализа, проектирования, эксплуатации и сопровождения.

Средства защиты БД

Средства защиты БД в различных СУБД несколько отличаются друг от друга. На основе анализа современных СУБД фирм Borland и Microsoft можно утверждать, что средства защиты БД условно делятся на две группы: основные и дополнительные.

К основным средствам защиты информации можно отнести следующие средства:

- парольной защиты;
- шифрования данных и программ;
- установления прав доступа к объектам БД;
- защиты полей и записей таблиц БД.

Средства защиты БД

Парольная защита представляет простой и эффективный способ защиты БД от несанкционированного доступа. Пароли устанавливаются конечными пользователями или администраторами БД. Учет и хранение паролей производится самой СУБД. Обычно пароли хранятся в определенных системных файлах СУБД в зашифрованном виде. Поэтому просто найти и определить пароль невозможно. После ввода пароля пользователю СУБД предоставляются все возможности по работе с защищенной БД. Саму СУБД защищать паролем большого смысла нет.

Шифрование данных (всей базы или отдельных таблиц) применяют для того, чтобы другие программы, «знающие формат БД этой СУБД»; не могли прочитать данные. Такое шифрование (применяемое в Microsoft Access), по-видимому, дает немного, поскольку расшифровать БД может любой с помощью «родной» СУБД. Если шифрация и дешифрация требуют задания пароля, то дешифрация становится возможной при верном вводе пароля.

Средства защиты БД

Шифрование исходных текстов программ позволяет скрыть от несанкционированного пользователя описание соответствующих алгоритмов.

В целях контроля использования основных ресурсов СУБД во многих системах имеются средства установления прав доступа к объектам БД. Права доступа определяют возможные действия над объектами. Владелец объекта (пользователь, создавший объект), а также администратор БД имеют все права. Остальные пользователи к разным объектам могут иметь различные уровни доступа.

По отношению к таблицам в общем случае могут предусматриваться следующие права доступа:

- просмотр (чтение) данных;
- изменение (редактирование) данных;
- добавление новых записей;
- добавление и удаление данных;
- все операции, в том числе изменение структуры таблицы.

Средства защиты БД

К дополнительным средствам защиты БД можно отнести такие, которые нельзя прямо отнести к средствам защиты, но которые непосредственно влияют на безопасность данных. Их составляют следующие средства:

- встроенные средства контроля значений данных в соответствии с типами;
- повышения достоверности вводимых данных;
- обеспечения целостности связей таблиц;
- организации совместного использования объектов БД в сети.

Редактируя БД, пользователь может случайно ввести такие значения, которые не соответствуют типу поля, в которое это значение вводится. Например, в числовое поле пытаться занести текстовую информацию. В этом случае СУБД с помощью средств контроля значений блокирует ввод и сообщает пользователю об ошибке звуковым сигналом, изменением цвета вводимых символов или другим способом.

Средства защиты БД

Блокировки могут действовать на различные объекты БД и на отдельные элементы объектов. Очевидной ситуацией блокировки объектов БД является случай одновременного использования объекта и попытки входа в режим разработки этого же объекта. Применительно к таблицам баз данных дополнительные блокировки могут возникать при работе с отдельными записями или полями.

Блокировки бывают явные и неявные. Явные блокировки накладываются пользователем или приложением с помощью команд. **Неявные** блокировки организует сама система, чтобы избежать возможных конфликтов. Например, в случае попытки изменения структуры БД во время редактирования информации устанавливается запрет реструктурирования БД до завершения редактирования данных.