Содержание:

Введение

В связи с все возрастающей ролью информации в жизни общества вопросы информационной безопасности занимают особое место и требуют к себе все большего внимания. Первичным является понятие информационной безопасности - это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации.

Безопасность данных - такое состояние хранимых, обрабатываемых и принимаемых данных, при которых невозможно их случайное или преднамеренное получение, изменение или уничтожение.

Защита данных- совокупность целенаправленных действий и мероприятий по обеспечению безопасности данных. Таким образом, защита данных есть процесс обеспечения безопасности данных, а безопасность - состояние данных, конечный результат процесса защиты. Защита данных осуществляется с использованием методов (способов) защиты.

Метод (способ) защиты данных - совокупность приемов и операций, реализующих функции защиты данных. Примерами их могут служить, например, методы шифрования и паролирования.

На основе методов защиты создаются средства защиты (например, устройства шифрации/дешифрации, программы анализа пароля, датчики охранной сигнализации и т.д.).

Механизм защиты - совокупность средств защиты, функционирующих совместно для выполнения определенной задачи по защите данных (криптографические протоколы, механизмы защиты операционных систем и т.д.). Система обеспечения безопасности данных (СОБД) - совокупность средств и механизмов защиты данных.

Основные угрозы безопасности данных

Для того чтобы сформулировать главную цель защиты данных, необходимо определить потенциально существующие возможности нарушения безопасности хранимых, обрабатываемых и передаваемых данных. Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно используют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения информационной безопасности.

Под угрозой безопасности данных будем понимать потенциально существующую возможность случайного или преднамеренного действия, или бездействия, в результате которого может быть нарушена безопасность данных. Несанкционированный доступ к данным (НСД) - злоумышленное или случайное действие, нарушающее технологическую схему обработки данных и ведущее к получению, модификации или уничтожению данных. НСД может быть пассивным (чтение, копирование) и активным (модификация, уничтожение).

Воздействия, в результате которых может быть нарушена безопасность данных, включают в себя:

- случайные воздействия природной среды (ураган, пожар и т.п.);

- целенаправленные воздействия нарушителя (шпионаж, разрушение компонентов информационной системы, использование прямых каналов утечки данных);

- внутренние возмущающие факторы (отказы аппаратуры, ошибки в математическом и программном обеспечении, недостаточная подготовка персонала и т.д.).

Под каналом утечки данных будем понимать потенциальную возможность нарушителю получить доступ к НСД, которая обусловлена архитектурой, технологической схемой функционирования информационной системы, а также существующей организацией работы с данными. Все каналы утечки данных можно разделить на косвенные и прямые.

Косвенными называются такие каналы утечки, использование которых для НСД не требует непосредственного доступа к техническим устройствам информационной системы. Они возникают, например, вследствие недостаточной изоляции помещений, просчетов в организации работы с данными и предоставляют нарушителю возможность применения подслушивающих устройств, дистанционного фотографирования, перехвата электромагнитных излучений, хищения носителей данных и отходов и т.п.).

Технические каналы утечки информации классифицируются по физической природе носителя. С учетом физической природы путей переноса информации каналы утечки данных можно классифицировать на следующие группы:

- визуально-оптические - источники информации здесь служит, как правило, непосредственное или удаленное наблюдение (в том числе и телевизионное);

- акустические - источником информации здесь служат речь и шумы, средой распространения звука являются воздух, земля, вода, строительные конструкции (кирпич, железобетон, металлическая арматура и др.);

- электромагнитные (включая магнитные и электрические) - источником информации здесь служат различные провода и кабели связи, создающие вокруг себя магнитное и электрическое поле, информацию с которых можно перехватить путем наводок на другие провода и элементы аппаратуры в ближней зоне их расположения;

- материально-вещественные (бумага, фото, магнитные носители и т.д.).

Наверное, потребность в защите информации появилась одновременно с самой информацией. И возможные методы защиты информации почти всегда определялись формой ее представления и предполагаемыми способами использования.

1. Система защиты информации

Система защиты информации - совокупность специальных мер правового и административного характера, организационных мероприятий, физических и технических средств защиты, а также специального персонала, предназначенного для обеспечения безопасности информации.

В первом приближении все методы защиты информации можно разделить на эти классы:

· Административные;

· Правовые меры защиты информации;

· Морально-этические меры защиты информации;

· Физические меры защиты;

· Технические (аппаратно-программные) средства защиты.

Организационные (административные) меры защиты - это меры, регламентирующие процессы функционирования АСОЭИ, использование ее ресурсов, деятельности персонала, а также порядок взаимодействия пользователей системой таким образом, чтобы максимально затруднить или исключить возможность реализации угроз безопасности информации.

Правовые меры защиты информации - действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.

Морально-этические меры защиты информации - традиционно сложившиеся в стране нормы поведения и правила обращения с информацией. Эти нормы не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет к падению авторитета, престижа человека, организации.

Физические меры защиты - различные механические, электро- или электронно-механические устройства, предназначение для создания физических препятствий на путях проникновения потенциальных нарушителей к абонентам АБС и защищаемой информации, а также техник визуального наблюдения, связи и охранной сигнализации.

Технические (аппаратно-программные) средства защиты - различные электронные устройства и специальные программы, выполняющие (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию пользователей, разграничение доступа к ресурсам, криптографическое закрытие информации и т.п.)

Наилучшие результаты по защите АСОЭИ достигаются при системном подходе к вопросам безопасности АСОЭИ и комплексном использовании различных мер защиты на всех этапах жизненного цикла системы начиная с ее проектирования.

Существуют следующие универсальные (общие) способы защиты информации от различных воздействий на нее:

1. Идентификация и аутентификация (пользователей процессов и т.д.);

2. Контроль доступа к ресурсам АСОЭИ (управление доступом);

3. Регистрация и анализ событий, происходящих в АСОЭИ;

4. Контроль целостности объектов АСОЭИ;

5. Шифрование данных;

6. Резервирование ресурсов и компонентов АСОЭИ.

Аутентификация - это процесс, в ходе которого на основании пароля, ключа или какой-либо иной информации, пользователь подтверждает, что является именно тем, за кого себя выдает.

Идентификация - это процесс, в ходе которого выясняются права доступа, привилегии, свойства и характеристики пользователя на основании его имени, логина или какой-либо другой информации о нем.

2. Система контроля и управления доступом

Система контроля и управления доступом (СКУД) -- совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через «точки прохода»: двери, ворота, КПП.

Основная задача - управление доступом на заданную территорию (кого пускать, в какое время и на какую территорию), включая так же:

· Ограничение доступа на заданную территорию;

· Идентификация лица, имеющего доступ на заданную территорию.

Важным компонентом в системе безопасности сетей передачи данных является цифровая подпись, позволяющая обмениваться юридически значимыми документами, проводить платежные операции, подтверждать целостность предаваемой и проверять целостность полученной информации.

Фирма IBM для целей защиты информации предлагает комплекс технических средств и программных продуктов для контроля доступа, наделения пользователей персональными полномочиями, установления подлинности передаваемой информации и секретности трансакций, действующий в диапазоне от уровня рабочих станций до уровня хост-ЭВМ.

Защита рабочей станции как составляющая часть единой системы защиты информации включает следующие функции:

· Идентификацию и проверку конечного пользователя;

· Наделение полномочиями конечного пользователя;

· Секретность трансакций;

· Целостность информации

и компоненты:

· Персональную карточку безопасности;

· Интерфейсное устройство безопасности;

· Криптографический адаптер;

· Процессор безопасности сети.

Идентификация и проверка конечного пользователя достигаются за счет применения персонального идентификатора. В качестве дополнительного средства проверки используется динамический метод проверки подписи конечным пользователем, основанный на измерении скорости движения ручки и давления при совершении подписи, показатели которых сравниваются с хранимыми в персональной карточке безопасности показателями.

Наделение полномочиями конечного пользователя, информация о которых хранится в персональной карточке безопасности. При положительном результате проверки доступ к прикладному программному продукту и наделение полномочиями выполнять те или иные трансакции контролируется на персональном уровне.

Секретность трансакций достигается путем включения криптографического (шифровального) процессора, реализующего алгоритм шифрования данных, в персональную карточку безопасности фирмы IBM , в интерфейсное устройство безопасности типа IBM 4754 и в криптографический адаптер типа IBM 4755 на уровне рабочих станций, а также в процессор безопасности сети типа IBM 4753 на уровне хост-ЭВМ.

Целостность информации обеспечивается применением кода подлинности передаваемой информации, формируемого путем реализации криптографического алгоритма данных в передающих и приемных устройствах.

Выполнение функций защиты информации реализуется с помощью комплекса технических средств и программных продуктов, разработанных фирмой IBM.

.

3. Целостность данных

Целостность данных -- свойство, при выполнении которого данные сохраняют заранее определённый вид и качество.

Методы и способы реализации требований, изложенных в определении термина, подробно описываются в рамках единой схемы обеспечения информационной безопасности объекта (защиты информации).

Основными методами обеспечения целостности информации (данных) при хранении в автоматизированных системах являются:

· Обеспечение отказоустойчивости (резервирование, дублирование, зеркалирование оборудования и данных, например через использование RAID-массивов);

· Обеспечение безопасного восстановления (резервное копирование и электронное архивирование информации).

Одним из действенных методов реализации требований целостности информации при ее передаче по линиям связи является криптографическая защита информации (шифрование, хеширование, электронная цифровая подпись).

При комплексном подходе к защите бизнеса, направление обеспечения целостности и доступности информации (ресурсов бизнес-процессов) перерастает в план мероприятий, направляемых на обеспечение непрерывности бизнеса.

Представленная система обеспечения защиты информации фирмы IBM опирается на различные компьютерные платформы и позволяет реализовать различные варианты банковских технологий и средств защиты информации.

Практика показывает, что введение паролей не защищает в достаточной степени от несанкционированного проникновения в коммуникационные сети. Наилучшим методом защиты компьютерной сети от несанкционированного проникновения является использование специальных компьютерных программ, постоянно сканирующих состояние сети, выявляющих попытки несанкционированного прорыва в них и подающих сигнал тревоги с одновременным блокированием канала связи, по которому пытается подключиться компьютер “хакера”.

По аналогичному принципу работают программы защиты компьютерных сетей от проникновения в них вирусов. Вирусы в настоящий момент представляют собой огромную опасность для успешного функционирования банковских компьютерных сетей.

К примеру, проникновение в такую сеть опасного вируса может привести не только к потере информации, но и блокировке всей сети в целом. Ущерб банку в таком случае может быть колоссальным, поскольку приостановка его работы хотя бы на один день приведёт к краху. Потеря же информации о счетах клиентов и перечислениях денежных средств вообще ведёт к катастрофе. Создание постоянно сканирующих систему программ, выявляющих и уничтожающих вирусы, является сейчас крупным бизнесом.

4. Шифрование и расшифрование

Предположим, что отправитель хочет послать сообщение получателю. Более того, отправитель желает засекретить это сообщение, чтобы никто, кроме получателя, не смог его прочитать.

Сообщение состоит из открытого текста. Процесс преобразования открытого текста с целью сделать непонятным его смысл для посторонних называется шифрованием. В результате шифрования сообщения получается шифр-текст. Процесс обратного преобразования шифртекста в открытый текст называется расшифрованием.

Наука, которая учит, как следует поступать, чтобы сохранить содержание сообщений в тайне, называется криптографией. Людей, занимающихся криптографией, зовут криптографами. Криптоаналитики являются специалистами в области криптоанализа -- науки о вскрытии шифров, которая отвечает на вопрос о том, как прочесть открытый текст, скрывающийся пол шифрованным. Раздел

науки, объединяющий криптографию и криптоанализ, именуется криптологией.

5. Учет реальных потребностей пользователей

Немало проблем, связанных с использованием криптографических средств, создают сами пользователи. Безопасность заботит их меньше всего. В первую очередь им требуются простота, удобство и совместимость с уже существующими (как правило, недостаточно защищенными) программными продуктами. Они выбирают легко запоминающиеся криптографические ключи, записывают их, где попало, запросто делятся ими с друзьями и знакомыми. Поэтому грамотно спроектированная криптографическая система обязательно должна принимать во внимание специфические особенности поведения людей.

Основная идея процедуры состоит в том, что каждому узлу сети вдоль маршрута следования потока задается вопрос, может ли этот узел обслужить некоторый новый поток с заданными характеристиками QoS, если известны предельные характеристики скорости потока, такие как средняя и пиковая скорости? Каждый узел при ответе на этот вопрос должен оценить свои возможности, то есть проверить, достаточно ли у него свободных ресурсов, чтобы принять на обслуживание новый поток и обслуживать его качественно. При положительном ответе узел должен некоторым образом зарезервировать часть своих ресурсов для данного потока, чтобы при поступлении пакетов потока на входные интерфейсы использовать эти ресурсы для их обслуживания с гарантированным уровнем качества.

Смысл резервирования состоит в том, чтобы ограничить уровень перегрузок определенного потока или нескольких потоков некоторой приемлемой величиной. Эта величина должна быть такой, чтобы механизмы QoS (управления очередями, кондиционирования трафика и обратной связи), применяемые в узлах сети, справлялись с кратковременными небольшими перегрузками и обеспечивали требуемые значения характеристик QoS.

В описанном примере не использован механизм профилирования трафика. При наличии отдельной взвешенной очереди для потока, зарезервировавшего пропускную способность, этот механизм не является обязательным, так как сам механизм взвешенных очередей ограничит пропускную способность потока в нужных пределах в периоды перегрузок, когда все взвешенные очереди заполняются полностью.

Использование взвешенных очередей -- не единственный вариант резервирования пропускной способности в пакетных сетях. Для той же цели можно задействовать приоритетные очереди. Применение приоритетной очереди может быть не только возможным, но и необходимым, если потоку помимо определенного уровня пропускной способности требуется обеспечить минимально возможный уровень задержек пакетов.

При использовании приоритетной очереди профилирование необходимо всегда, так как приоритетный механизм не обеспечивает ограничения скорости потока, как это делает механизм взвешенного обслуживания.

Нужно подчеркнуть, что резервирование приводит к ожидаемым результатам только в тех случаях, когда реальная скорость потоков, для которых было выполнено резервирование, оказывается не выше, чем пропускная способность, запрошенная при резервировании и реализованная при конфигурировании сетевых устройств. В противном случае результаты могут оказаться даже хуже, чем при наличии единственной очереди «по умолчанию» и обслуживании «по возможности». Так, если скорость потока окажется выше, чем предел, учитываемый механизмом профилирования, то часть пакетов будет отброшена даже в том случае, если устройство не перегружено и могло бы отлично справиться с предложенным трафиком без применения механизмов QoS.

Что же меняется в сети после резервирования? При поступлении на входной интерфейс коммутатора пакетов потока, для которых было выполнено резервирование, механизм классификации распознает пакеты, относящиеся к этому потоку, и направляет их в нужную очередь. При этом пакеты могут проходить через механизм профилирования, призванный предотвратить ситуацию обслуживания потока, скорость которого превышает оговоренную при резервировании.

В результате резервирования сеть оказывается загруженной рационально. В ней нет ресурсов, которые работают со значительной перегрузкой. Механизмы организации очередей по-прежнему обеспечивают временную буферизацию пакетов в периоды пульсаций. Так как мы планировали загрузку ресурсов из расчета средних скоростей передачи данных, то на периодах пульсаций в течение некоторого ограниченного времени скорости потоков могут превышать средние скорости, так что механизмы борьбы с перегрузками по-прежнему нужны. Для обеспечения требуемых средних скоростей потоков на периодах перегрузок соответствующие потоки могут обслуживаться с помощью взвешенных очередей.

Сохраняется также главное преимущество метода коммутации пакетов: если некоторый поток не расходует отведенной ему пропускной способности, то она может выделяться для обслуживания другого потока. Нормальной практикой является резервирование пропускной способности только для части потоков, в то время как другие потоки обслуживаются без резервирования, получая обслуживание по возможности (с максимальными усилиями). Временно свободная пропускная способность может для таких потоков выделяться динамически, без нарушения взятых обязательств по обслуживанию потоков, для которых ресурсы зарезервированы.

Заключение

Административные методы заключаются в определении процедур доступа к защищаемой информации и строгом их выполнении. Контроль над соблюдением установленного порядка возлагается на специально обученный персонал. Административные методы применялись многие века и диктовались здравым смыслом. Чтобы случайный человек не прочитал важный документ, такой документ нужно держать в охраняемом помещении. Чтобы передать секретное сообщение, его нужно посылать с курьером, который готов ценой собственной жизни защищать доверенную ему тайну. Чтобы из библиотеки не пропадали в неизвестном направлении книги, необходимо вести учет доступа к библиотечным ресурсам. Современные административные методы защиты информации весьма разнообразны. Например, при работе с документами, содержащими государственную тайну, сначала необходимо оформить допуск к секретным документам. При получении документа и возврате его в хранилище в журнал регистрации заносятся соответствующие записи. Работа с документами разрешается только в специально оборудованном и сертифицированном помещений. На любом этапе известно лицо, несущее ответственность за целостность и секретность охраняемого документа. Схожие процедуры доступа к информации существуют и в различных организациях, где они определяются корпоративной политикой безопасности. Например, элементом политики безопасности может являться контроль вноса и выноса с территории организации носителей информации (бумажных, магнитных, оптических и др.). Административные методы защиты зачастую совмещаются с законодательными и могут устанавливать ответственность за попытки нарушения установленных процедур доступа