Лекция 3 Построение систем защиты от угрозы нарушения целостности информации и отказа доступа. Политика и модели безопасности

План лекции:

1. Защита целостности информации при хранении, обработке, транспортировке.
2. Защита от угрозы нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита семантического анализа и актуальности информации.
3. Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности.
4. Политика и модели дискреционного доступа. Парольные системы разграничения доступа. Политика и модели мандатного доступа.
5. Теоретико-информационные модели.
6. Политика и модели тематического разграничения доступа. Ролевая модель безопасности.

1 Защита целостности информации при хранении, обработке, транспортировке

Защита целостности информации при хранении

В информационной системе основное место хранения информации — электронные носители, поэтому рассмотрим меры защиты применительно к этому классу носителей.

Определяя порядок хранения информации на электронных носителях, следует иметь в виду, что от состояния носителей зависит качество программ и защищаемых данных. Электронные носители являются устройствами, подвергавшимися интенсивному износу. Кроме того, в электронные носители могут быть внедрены закладки, поэтому используемые методы записи, хранения и считывания нельзя считать защищенными.

Организационно-технологические меры защиты целостности информации на электронных носителях можно разделить на две основные группы:

· организационные меры по поддержке целостности информации;

· технологические меры контроля целостности битовых последовательностей.

Организационные меры

Организационные меры защиты направлены на предупреждение хищения или утраты носителей, а вместе с ними и информации. Организационные меры излагаются в документах, описывающих режим хранения конфиденциальной информации.

Организационные меры разделяются на две группы:

· создание резервных копий информации, хранимой на электронных носителях;

· обеспечение правильных условий хранения и эксплуатации носителей.

Создание резервных копий Создание резервных копий информации, хранимой в информационной системе, должно быть обязательной регулярной процедурой, периодичность которой зависит от важности информации и технологии ее обработки, в частности от объема вводимых данных, возможности повторного ввода и т. д. Для создания резервных копий могут использоваться как стандартные утилиты, так и специализированные системы резервного копирования, адаптированные к конкретной системе. В последнем случае можно применять собственные методы «разностного» архивирования, когда на вспомогательный носитель записывается, а только та часть информации, которая была введена с момента последнего сохранения.

В качестве вспомогательных носителей для хранения архивных данных выбирают, как правило, те, которые оптимальны по цене единицы хранимой информации.

При ведении резервных копий необходимо регулярно проверять сохранность и целостность находящейся в них информации.

Обеспечение правильных условий хранения и эксплуатации Обеспечение правильных условий хранения и эксплуатации определяется конкретным типом носителя.

Регистрация и учет носителей производятся независимо от того, есть ли на них конфиденциальная информация или нет. Служебные носители должны иметь ясную, хорошо видимую этикетку, на которой проставлены гриф, номер, дата регистрации. Гриф секретности носителя может изменяться только в большую сторону, т. к. информация не может быть гарантированно удалена. Учет носителей по журналу ведется в течение всей «жизни» носителя. В помещении не должно быть личных носителей. Не допускается работа с непроверенными носителями. Должна проводиться систематическая комиссионная проверка наличия носителей и информации.

Хранение электронных носителей такое же, как обычных документов такого же уровня конфиденциальности. Основное требование при хранении — исключение НСД. Передача между подразделениями должна осуществляться под расписку и учитываться в журнале. Вынос за пределы помещения возможен только с разрешения уполномоченных лиц.

Жесткий диск регистрируется с грифом, соответствующим категории компьютера, независимо от целей его использования. На корпусе жесткого диска должна быть соответствующая этикетка. При передаче компьютера в ремонт необходимо либо изъять жесткий диск, либо гарантированно удалить с него информацию, либо присутствовать при ремонте.

Копирование файлов с зарегистрированных электронных носителей допускается только на компьютерах, категория которых не ниже грифа секретности носителя. Каждое копирование должно учитываться в обычном или электронном журнале.

Следует уделять особое внимание удалению информации с носителей. Обычные способы удаления файлов не приводят к удалению области данных, происходит стирание только на логическом уровне. Кроме того, при удалении следует учесть, что в современных средствах обработки информация существует в нескольких экземплярах, под разными именами.

Технологические меры

Рассмотрим теперь технологические меры контроля целостности битовых последовательностей, хранящихся на электронных носителях. Целостность информации в областях данных проверяется с помощью контрольного кода, контрольные числа которого записываются после соответствующих областей, причем в контролируемую область включаются соответствующие маркеры.

Для обеспечения контроля целостности информации чаще всего применяют циклический контрольный код. Этот метод, дающий хорошие результаты при защите от воздействия случайных факторов (помех, сбоев и отказов), совсем не обладает имитостойкостью, т. е. не обеспечивает защиту от целенаправленных воздействий нарушителя, приводящих к навязыванию ложных данных.

Для контроля целостности можно использовать методы имитозащиты, основанные на криптографических преобразованиях. Они обеспечивают надежный контроль данных, хранящихся в системе, но в то же время реализуются в виде объемных программ и требуют значительных вычислительных ресурсов.

Защита целостности информации при обработке

При рассмотрении вопроса целостности данных при обработке используется интегрированный подход, основанный на ряде работ Д. Кларка и Д. Вилсона, а также их последователей и оппонентов и включающий в себя девять теоретических принципов:

· корректность транзакций;
· аутентификация пользователей;
· минимизация привилегий;
· разграничение функциональных обязанностей;
· аудит произошедших событий;
· объективный контроль;
· управление передачей привилегий;

· обеспечение непрерывной работоспособности; · простота использования защитных механизмов.

Понятие *корректности транзакций* определяется следующим образом. Пользователь не должен модифицировать данные произвольно, а только определенными способами, т. е. так, чтобы сохранялась целостность данных. Другими словами, данные можно изменять только путем корректных транзакций и нельзя произвольными средствами. Кроме того, предполагается, что «корректность» каждой из таких транзакций может быть некоторым способом доказана.

Второй принцип гласит, что изменение данных может осуществляться только специально *аутентифицированными* для этой цели пользователями. Данный принцип работает совместно с последующими четырьмя, с которыми тесно связана его роль в общей схеме обеспечения целостности.

Идея *минимизации привилегий* появилась еще на ранних этапах развития информационной безопасности в форме ограничения, накладываемого на возможности выполняющихся в системе процессов и подразумевающего то, что процессы должны быть наделены теми и только теми привилегиями, которые естественно и минимально необходимы для выполнения процессов. Принцип минимизации привилегий распространяется и на программы, и на пользователей. Пользователи имеют, как правило, несколько больше привилегий, чем им необходимо для выполнения конкретного действия в данный момент времени. А это открывает возможности для злоупотреблений.

Разграничение функциональных обязанностей подразумевает организацию работы с данными таким образом, что в каждой из ключевых стадий, составляющих единый критически важный, с точки зрения целостности, процесс, необходимо участие различных пользователей. Это гарантирует невозможность выполнения одним пользователем всего процесса целиком (или даже двух его стадий) с тем, чтобы нарушить целостность данных. В обычной жизни примером воплощения данного принципа служит передача одной половины пароля для доступа к программе управления ядерным реактором первому системному администратору, а другой — второму.

Аудит произошедших событий, включая возможность восстановления полной картины происшедшего, является превентивной мерой в отношении потенциальных нарушителей.

Принцип *объективного контроля* также является одним из краеугольных камней политики контроля целостности. Суть данного принципа заключается в том, что контроль целостности данных имеет смысл лишь тогда, когда эти данные отражают реальное положение вещей. В связи с этим Кларк и Вилсон указывают на необходимость регулярных проверок, имеющих целью выявление возможных несоответствий между защищаемыми данными и объективной реальностью, которую они отражают.

Управление передачей привилегий необходимо для эффективной работы всей политики безопасности. Если схема назначения привилегий неадекватно отражает организационную структуру предприятия или не позволяет администраторам безопасности гибко манипулировать ею для обеспечения эффективности производственной деятельности, защита становится обременительной и провоцирует попытки обойти ее.

Принцип *обеспечения непрерывной работы* включает защиту от сбоев, стихийных бедствий и других форс-мажорных обстоятельств.

Простота использования защитных механизмов необходима, в том числе для того, чтобы пользователи не стремились обойти их как мешающих «нормальной» работе. Кроме того, как правило, простые схемы являются более надежными. Простота использования защитных механизмов подразумевает, что самый безопасный путь эксплуатации системы будет также наиболее простым, и наоборот, самый простой — наиболее защищенным.

Защита целостности информации при транспортировке

Средства контроля целостности должны обеспечивать защиту от несанкционированного изменения информации нарушителем при ее передаче по каналам связи.

При транспортировке информации следует защищать как целостность, так и подлинность информации.

Схема контроля целостности данных подразумевает выполнение двумя сторонами — *источником* и *приемником* — некоторых (возможно, разных) криптографических преобразований данных. Источник преобразует исходные данные и передает их приемнику вместе с некоторым приложением, обеспечивающим избыточность шифрограммы.

Приемник обрабатывает полученное сообщение, отделяет приложение от основного текста и проверяет их взаимное соответствие, осуществляя таким образом контроль целостности.

Контроль целостности может выполняться с *восстановлением* или *без восстановления* исходных данных.

Целостность отдельного сообщения обеспечивается имитовставкой, ЭЦП или шифрованием, целостность потока сообщений — соответствующим механизмом целостности.

Имитовставка

Для обеспечения целостности в текст сообщения часто вводится некоторая дополнительная информация, которая легко вычисляется, если секретный ключ известен, и является трудновычислимой в противном случае. Если такая информация вырабатывается и проверяется с помощью одного и того же секретного ключа, то ее называют *имитовставкой* (в зарубежных источниках используется термин *код аутентификации сообщений* — Message Authentication Code (MAC) — поскольку помимо целостности может обеспечиваться еще и аутентификация объекта). Имитовставкой может служить значение хэш-функции, зависящей от секретного ключа, или выходные данные алгоритма шифрования в режиме сцепления блоков шифра.

Шифрование Целостность данных можно обеспечить и с помощью их шифрования симметричным криптографическим алгоритмом при условии, что подлежащий защите текст обладает некоторой избыточностью. Последняя необходима для того, чтобы нарушитель, не зная ключа шифрования, не смог бы создать шифрограмму, которая после расшифрования успешно прошла бы проверку целостности.

Избыточности можно достигнуть многими способами. В одних случаях текст может обладать достаточной естественной избыточностью (например, в тексте, написанном на любом языке, разные буквы и буквосочетания встречаются с разной частотой).

В других можно присоединить к тексту до шифрования некоторое контрольное значение, которое, в отличие от имитовставки и цифровой подписи, не обязательно должно вырабатываться криптографическими алгоритмами, а может представлять собой просто последовательность заранее определенных символов.

Контроль целостности потока сообщений Контроль целостности потока сообщений помогает обнаружить их повтор, задержку, переупорядочение или утрату. Предполагается, что целостность каждого отдельного сообщения обеспечивается шифрованием, имитовставкой или цифровой подписью.

Для контроля целостности потока сообщений можно, например:

· присвоить сообщению *порядковый номер целостности*;

· использовать в алгоритмах шифрования *сцепление* с предыдущим сообщением.

При использовании порядкового номера целостности, который может включать в себя порядковый номер сообщения и имя источника, приемник хранит последний номер принятого сообщения каждого источника. Для контроля целостности приемник проверяет, например, что порядковый номер целостности текущего сообщения от данного источника на единицу больше номера предыдущего сообщения. Если в качестве порядкового номера целостности используется время отправки сообщения, то проверяется, действительно ли

время отправки и время приема близки друг к другу с точностью до задержки сообщения в канале связи и разности хода часов источника и приемника.

Электронная подпись Термин «электронная подпись» (ЭЦП) используется для методов, позволяющих устанавливать подлинность автора сообщения при возникновении спора относительно авторства этого сообщения. ЭЦП применяется в информационных системах, в которых отсутствует взаимное доверие сторон (финансовые системы, системы контроля за соблюдением международных договоров и др.).

Концепцию цифровой подписи для аутентификации информации предложили Диффи и Хеллман в 1976 г. Она заключается в том, что каждый абонент сети имеет личный секретный ключ, на котором он формирует подпись и известную всем другим абонентам сети проверочную комбинацию, необходимую для проверки подписи (эту проверочную комбинацию иногда называют открытым ключом). Цифровая подпись вычисляется на основе сообщения и секретного ключа отправителя. Любой получатель, имеющий соответствующую проверочную комбинацию, может аутентифицировать сообщение по подписи.

ЭЦП в цифровых документах играет ту же роль, что и подпись, поставленная от руки в документах, которые напечатаны на бумаге: это данные, присоединяемые к передаваемому сообщению и подтверждающие, что отправитель (владелец подписи) составил или заверил данное сообщение. Получатель сообщения или третья сторона с помощью цифровой подписи может проверить, что автором сообщения является именно владелец подписи (т. е. аутентифицировать источник данных) и что в процессе передачи не была нарушена целостность полученных данных.

Если пользователь ведет себя грамотно, с точки зрения соблюдения норм секретности (хранение секретных ключей подписи, работа с «чистым» программным продуктом, осуществляющим функции подписи), и тем самым исключает возможность похищения ключей или несанкционированного изменения данных и программ, то стойкость системы подписи определяется исключительно криптографическими качествами.

2 Защита от угрозы нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита семантического анализа и актуальности информации

Защита от угрозы нарушения целостности информации на уровне содержания

Защита от угрозы нарушения целостности информации на уровне содержания в обычной практике рассматривается как защита от дезинформации. Пусть у злоумышленника нет возможности воздействовать на отдельные компоненты системы, находящиеся в пределах контролируемой зоны, но, если источники поступающей в нее информации находятся вне системы, всег- да остается возможность взять их под контроль. При намеренной дезинформации применяют как заведомую ложь, так и полуправду, создающие искаженное представление о событиях.

Наиболее распространенные приемы дезинформации:

· прямое сокрытие фактов;

· тенденциозный подбор данных;

· нарушение логических и временных связей между событиями;

· подача правды в таком контексте (добавлением ложного факта или намека), чтобы она воспринималась как ложь;

· изложение важнейших данных на ярком фоне отвлекающих внимание сведений;

· смешивание разнородных мнений и фактов;

· изложение данных словами, которые можно истолковывать по-разному;

· отсутствие упоминания ключевых деталей факта.

В процессе сбора и получения информации могут возникнуть искажения.

Основные причины искажений информации:

· передача только части сообщения;

· интерпретация услышанного в соответствии со своими знаниями и представлениями; · пропуск фактуры через призму субъективно-личностных отношений.

Для успешности *борьбы с вероятной дезинформацией* следует:

· различать факты и мнения;

· применять дублирующие каналы информации;

· исключать все лишние промежуточные звенья и т. п.

В информационных системах необходимо предусматривать наличие подсистем, проводящих первичный смысловой анализ и в определенной степени контролирующих работу оператора. Наличие подобных подсистем позволяет защитить информацию не только от случайных, но и от преднамеренных ошибок.

Построение систем защиты от угрозы отказа доступа к информации

Поскольку одной из основных задач информационной системы является своевременное обеспечение пользователей системы необходимой информацией (сведениями, данными, управляющими воздействиями и т. п.), то угроза отказа доступа к информации может еще рассматриваться как угроза отказа в обслуживании или угроза отказа функционирования. Угроза отказа функционирования информационной системы может быть вызвана: · целенаправленными действиями злоумышленников; · ошибками в программном обеспечении; · отказом аппаратуры.

Часто невозможно бывает разделить причины отказа. В связи с этим вводят понятие надежности.

Надежность — свойство объекта сохранять во времени значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонта, хранения и транспортировки.

Для оценки надежности функционирования информационной системы не важно, вызваны ли отказы действиями злоумышленника или связаны с ошибками разработки, важно, как и в каком объеме произойдет их парирование.

Целесообразно проводить отдельно оценку надежности аппаратуры и программного обеспечения, так как подход к определению надежности здесь различен.

Оценка *надежности оборудования* основана на следующем подходе.

Элементная надежность любого устройства или системы в целом оценивается как произведение вероятности безотказной работы $P'(t)$ на коэффициент готовности

$$Kr : P_0(t) = P'(t)Kr .$$

Если надежность выступает в качестве одной из мер эффективности системы, то оптимальным ее значением является такое, при котором стоимость эксплуатации является минимальной. Оптимальное значение показателя надежности может быть оценено графически (рис.2.1).

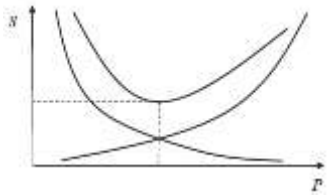

Рис. 2.1 - Зависимость затрат от надежности:
$S_э$ — эксплуатационные затраты; $S_р$ — затраты на разработку

В некоторых случаях решается задача достижения максимальной надежности при фиксированных затратах или других закрепленных условиях.

Для определения надежности существуют как теоретические методы расчета, так и рабочие методики. Именно на основе таких расчетов вырабатываются практические мероприятия

по повышению надежности работы как отдельных элементов, так и систем в целом.

На начальной стадии проектирования чаще всего используются рабочие методики, основанные на простых моделях, или элементарные методики расчета надежности, исходящие из предположения о самостоятельности отдельных элементов.

В теоретических методах расчета надежности наиболее широкое распространение получили методики расчета по элементам. При этом функциональные зависимости и параметры, характеризующие надежность работы отдельного элемента, могут быть выражены следующими формулами:

частота отказов

$$f(t) = dq(t)/dt = — dP(t)/dt;$$

интенсивность отказов

$$\lambda(t) = \frac{1}{P(t)} \frac{dq(t)}{dt} = -\frac{1}{P(t)} \frac{dP(t)}{dt}$$

среднее время безотказной работы

$$t_{cp} = \int_0^\infty t \cdot f(t)dt,$$

где P — вероятность безотказной работы элемента; q — вероятность отказа элемента.

Эти формулы применимы к системам с любым числом элементов и произвольным их отношением.

Вероятность безотказной работы системы является функцией вероятностей безотказной работы входящих в систему элементов

$$P_c = f_1 [P_1(t), P_2(t), \dots , P_n(t)].$$

Взаимосвязь функций для отдельных элементов может быть разной. В частности, вероятность безотказной работы или функция надежности системы, состоящей из n произвольно соединенных элементов, может быть выражена в виде полинома

$$P_c = \sum_{i=1}^{k} aiP_i$$

В случае независимого влияния отдельных элементов на работоспособность установки, если отказ каждого из элементов приводит к отказу всей системы, схема структурных надежных отношений представляется в виде последовательного соединения элементов. В этом случае вероятность безотказной работы системы определяется произведением вероятностей безотказной работы элементов

$$P_c(t) = \prod_{i=1}^{n} Pi\,(t)$$

Если же элементы влияют друг на друга, то схема структурных надежных отношений будет параллельной или смешанной.

Если отказ элемента не приводит к отказу системы, то в схеме структурных надежных отношений этот элемент включается параллельно, а при вычислении надежности системы перемножаются вероятности отказов параллельных элементов и полученное произведение вычитается из единицы:

$$P_c(t) = 1 - \prod_{j=1}^{n}(1 - P_j(t))$$

Надежность работы элементов не всегда удобно характеризовать вероятностью безотказной работы, так как для малых периодов времени работы элементов значения $Pi\,(t)$ будут близкими к единице. В этом случае лучше использовать интенсивность отказов, которая характеризует плотность вероятности появления отказа отдельно взятого элемента. Она определяется количеством отказов n_i в единицу времени Δt, отнесенных к количеству исправно работающих в данный момент однотипных элементов N, то есть

$$\lambda = n_i/N\Delta t$$

Вероятность безотказной работы связана с интенсивностью отказов следующим соотношением:

$$P(t) = \exp(-\int_0^\infty \lambda(t)dt).$$

Функция $\lambda(t)$ имеет вид, изображенный на рис. 2.2.

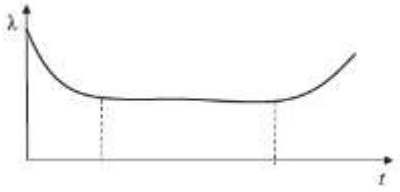

Рис. 2.2 - Изменение интенсивности отказов системы в течение срока службы

Первый участок повышенной интенсивности отказов характеризует период, отказы в котором возникают главным образом в результате скрытых неисправностей, допущенных при проектировании, нарушении технологии изготовления системы или связанных с трудностями освоения эксплуатации. Наиболее длительное время система эксплуатируется в нормальных условиях (участок II). Именно этот период работы системы принимается во внимание при расчете надежности в процессе проектирования. Участок III характеризует период увеличения интенсивности отказов вследствие износа оборудования и его старения.

Анализ работы многочисленных технических устройств показал: чем они проще, тем более надежны.

При обеспечении защиты информационной системы от угрозы отказа функционирования обычно считается, что надежность аппаратных компонентов достаточно высока и данной составляющей в общей надежности можно пренебречь. Это связано с тем, что темпы морального старения вычислительной техники значительно опережают темпы ее физического старения и замена вычислительной техники, как правило, происходит до ее выхода из строя.

Таким образом, на надежность функционирования информационной системы во многом влияет *надежность функционирования программного обеспечения,* входящего в ее состав.

Несмотря на явное сходство в определениях надежности для аппаратных средств и программного обеспечения, фактически последнее имеет принципиальные отличия:

· программа в большинстве случаев не может отказать случайно;

· ошибки в программном обеспечении, допущенные при его создании, зависят от технологии разработки, организации работ и квалификации исполнителей;

· ошибки не являются функцией времени; · причиной отказов является набор входных данных, сложившихся к моменту отказа.

Существует два основных подхода к обеспечению защиты программного обеспечения от угрозы отказа функционирования:

· обеспечение отказоустойчивости программного обеспечения;

· предотвращение неисправностей.

Отказоустойчивость предусматривает, что оставшиеся ошибки программного обеспечения обнаруживаются во время выполнения программы и парируются за счет использования программной, информационной и временной избыточности.

Предотвращение неисправностей связано с анализом природы ошибок, возникающих на разных фазах создания программного обеспечения, и причин их возникновения.

Защита семантического анализа и актуальности информации

На уровне представления информации защиту от угрозы отказа доступа к информации (защиту семантического уровня) можно рассматривать как противодействие сопоставлению используемым синтаксическим конструкциям (словам некоторого алфавита, символам и т.

п.) определенного смыслового содержания. В большей степени эта задача относится к области лингвистики, рассматривающей изменение значения слов с течением времени, переводу с иностранного языка и другим аналогичным научным и прикладным областям знаний.

Применительно к информационным системам защита содержания информации от угрозы блокировки доступа (отказа функционирования) означает юридическую обоснованность обработки и использования информации.

ВЫВОДЫ

· Эффективность методов контроля целостности определяется в основном характеристиками используемых криптографических средств шифрования — цифровой подписи, хэш-функций.

· Вопросы обеспечения своевременного беспрепятственного доступа к информации приобретают все большее значение с развитием распределенных систем обработки.

Усложнение топологии систем, применяемого оборудования и используемого программного обеспечения, а также задача сопряжения всех элементов требуют повышенного внимания к обеспечению работоспособности системы и доступности циркулирующей в ней информации.

· Отдельное направление защиты — обеспечение секретности параметров информационной системы, в которой циркулирует конфиденциальная информация. Методы защиты параметров такой системы аналогичны общим методам, применяемым для защиты конфиденциальности информации.

3 Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности

Политика безопасности

Технология защиты информационных систем начала развиваться относительно недавно, но уже сегодня существует значительное число теоретических моделей, позволяющих описывать различные аспекты безопасности и обеспечивать средства защиты с формальной стороны.

Под *политикой безопасности* понимается совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое условие безопасности системы. Формальное выражение политики безопасности называют *моделью безопасности*.

Основная цель создания политики безопасности — это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Кроме того, модели безопасности позволяют решить еще целый ряд задач, возникающих в ходе проектирования, разработки и сертификации защищенных систем, поэтому их используют не только теоретики информационной безопасности, но и другие категории специалистов, участвующих в процессе создания и эксплуатации защищенных информационных систем.

Модели безопасности обеспечивают системотехнический подход, включающий решение следующих задач:

· выбор и обоснование базовых принципов архитектуры защищенных систем, определяющих механизмы реализации средств и методов защиты информации;

· подтверждение свойства защищенности разрабатываемых систем путем формального доказательства соблюдения политики безопасности;

· составление формальной спецификации политики безопасности как важнейшей составной части организационного и документационного обеспечения разрабатываемых защищенных систем.

Производители защищенных информационных систем используют модели безопасности в следующих случаях:

· при составлении формальной спецификации политики безопасности разрабатываемой системы;

· при выборе и обосновании базовых принципов архитектуры защищенной системы, определяющих механизмы реализации средств защиты;

· в процессе анализа безопасности системы, при этом модель используется в качестве эталонной модели;

· при подтверждении свойств разрабатываемой системы путем формального доказательства соблюдения политики безопасности.

Потребители путем составления формальных моделей безопасности получают возможность довести до сведения производителей свои требования, а также оценить соответствие защищенных систем своим потребностям.

Эксперты в ходе анализа адекватности реализации политики безопасности в защищенных системах используют модели безопасности в качестве эталонов.

По сути, модели безопасности являются связующим элементом между производителями, потребителями и экспертами.

Субъектно-объектные модели разграничения доступа

Основы моделирования процессов защиты информации рассмотрены, например, в работах В. А. Герасименко, одного из наиболее известных отечественных исследователей теоретических и практических аспектов защиты информации в автоматизированных системах, автора системно концептуального подхода к информационной безопасности. В. А. Герасименко представил общую модель процессов защиты информации, структурировав ее на взаимосвязанные компоненты и выделив в отдельный блок модели систем разграничения доступа к ресурсам.

Разграничение доступа к информации — разделение информации, циркулирующей в информационной системе, на части, элементы, компоненты, объекты и т. д. и организация системы работы с информацией, предполагающей доступ пользователей к той части (к тем компонентам) информации, которая им необходима для выполнения функциональных обязанностей.

Разграничение доступа непосредственно обеспечивает конфиденциальность информации, а также снижает вероятность реализации угроз целостности и доступности. Разграничение доступа можно рассматривать среди других методов обеспечения информационной безопасности как комплексный программно-технический метод защиты информации. Разграничение доступа является также необходимым условием обеспечения информационной безопасности.

Большинство моделей разграничения доступа основывается на представлении системы как совокупности субъектов и объектов доступа.

Рассмотрим основные положения наиболее распространенных политик безопасности, основанных на контроле доступа субъектов к объектам и моделирующих поведение системы с помощью пространства состояний, одни из которых являются безопасными, а другие — нет. Все рассматриваемые модели безопасности основаны на следующих базовых представлениях:

1. В системе действует дискретное время.

2. В каждый фиксированный момент времени система представляет собой конечное множество элементов, разделяемых на два подмножества:

· подмножество субъектов доступа S;

· подмножество объектов доступа O.

Субъект доступа — активная сущность, которая может изменять состояние системы через порождение процессов над объектами, в том числе порождать новые объекты и инициализировать порождение новых субъектов.

Объект доступа — пассивная сущность, процессы над которой могут в определенных случаях быть источником порождения новых субъектов.

При таком представлении системы безопасность обработки информации обеспечивается путем решения задачи управления доступом субъектов к объектам в соответствии с заданным набором правил и ограничений, которые образуют политику безопасности. Общим подходом для всех моделей является именно разделение множества сущностей, составляющих систему, на множества субъектов и объектов, хотя сами определения понятий «объект» и «субъект» в разных моделях могут различаться.

В модели предполагается наличие механизма различения субъектов и объектов по свойству активности. Кроме того, предполагается также, что в любой момент времени t_k, в том числе и в начальный, множество субъектов доступа не пусто.

3. Пользователи представлены одним или некоторой совокупностью субъектов доступа, действующих от имени конкретного пользователя.

Пользователь — лицо, внешний фактор, аутентифицируемый некоторой информацией и управляющий одним или несколькими субъектами, воспринимающий объекты и получающий информацию о состоянии системы через субъекты, которыми он управляет.

Таким образом, в субъектно-объектной модели понятия субъектов доступа и пользователей не тождественны. Предполагается, что пользовательские управляющие воздействия не могут изменить свойств самих субъектов доступа, что не соответствует реальным системам, в которых пользователи могут изменять свойства субъектов через изменение программ. Однако подобная идеализация позволяет построить четкую схему процессов и механизмов доступа.

4. Субъекты могут быть порождены из объектов только активной сущностью (другим субъектом).

Объект o_i называется *источником* для субъекта s_m, если существует субъект sj, в результате воздействия которого на объект o_i возникает субъект s_m. Субъект sj является *активизирующим* для субъекта s_m.

Для описания процессов порождения субъектов доступа вводится следующая команда:

Create (s_j, o_i) → s_m — из объекта o_i порожден субъект s_m, при активизирующем воздействии субъекта s_j.

Create называют операцией порождения субъектов. Ввиду того, что в системе действует дискретное время, под воздействием активизирующего субъекта в момент времени *tk* новый субъект порождается в момент времени t_{k+1}.

Результат операции *Create* зависит как от свойств активизирующего субъекта, так и от свойств объекта-источника.

Активная сущность субъектов доступа заключается в их способности осуществлять определенные действия над объектами, что приводит к возникновению потоков информации.

5. Все взаимодействия в системе моделируются установлением отношений определенного типа между субъектами и объектами. Множество типов отношений определяется в виде набора операций, которые субъекты могут производить над объектами.

6. Все процессы в системе описываются доступом субъектов к объектам, вызывающим потоки информации.

Потоком информации между объектом o_i и объектом o_j называется произвольная операция над объектом o_j, реализуемая в субъекте s_m и зависящая от объекта o_i.

Поток может осуществляться в виде различных операций над объектами: чтение, изменение, удаление, создание и т. д.

Объекты, участвующие в потоке, могут быть как источниками, так и приемниками информации, как ассоциированными с субъектом, так и неассоциированными, а также

могут быть пустыми объектами (например, при создании или удалении файлов). Потоки информации могут быть только между объектами, а не между субъектом и объектом.

Доступом субъекта s_m *к объекту* o_j называется порождение субъектом s_m потока информации между объектом o_j и некоторым объектом o_i.

Формальное определение понятия доступа дает возможность средствами субъектно-объектной модели перейти непосредственно к описанию процессов безопасности информации в защищенных системах. С этой целью вводится множество потоков P для всей совокупности фиксированных декомпозиций системы на субъекты и объекты во все моменты времени (множество P является объединением потоков по всем моментам времени функционирования системы).

Правила разграничения доступа субъектов к объектам есть формально описанные потоки, принадлежащие множеству P.

7. Политика безопасности задается в виде правил, в соответствии с которыми должны осуществляться все взаимодействия между субъектами и объектами. Взаимодействия, приводящие к нарушению этих правил, пресекаются средствами контроля доступа и не могут быть осуществлены.

8. Все операции контролируются монитором безопасности и либо запрещаются, либо разрешаются в соответствии с правилами политики безопасности.

9. Совокупность множеств субъектов, объектов и отношений между ними (установившихся взаимодействий) определяет *состояние* системы. Каждое состояние системы является либо *безопасным,* либо *небезопасным* в соответствии с предложенным в модели критерием безопасности.

10. Основной элемент модели безопасности — это доказательство утверждения (теоремы) о том, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние при соблюдении всех установленных правил и ограничений.

Аксиомы политики безопасности

Анализ опыта защиты информации, а также основных положений субъектно-объектной модели позволяет сформулировать несколько аксиом, касающихся построения политик безопасности.

Аксиома 1. В защищенной информационной системе в любой момент времени любой субъект и объект должны быть идентифицированы и аутентифицированы.

Данная аксиома определяется самой природой и содержанием процессов коллективного доступа пользователей к ресурсам. Иначе субъекты имеют возможность выдать себя за других субъектов или подменить одни объекты доступа на другие.

Аксиома 2. В защищенной системе должна присутствовать активная компонента (субъект, процесс и т. д.) с соответствующим объектом-источником, которая осуществляет управление доступом и контроль доступа субъектов к объектам, — монитор или ядро безопасности.

Монитор безопасности — механизм реализации политики безопасности в информационной системе, совокупность аппаратных, программных и специальных компонентов системы, реализующих функции защиты и обеспечения безопасности (общепринятое сокращение — TCB — Trusted Computing Base).

В большинстве информационных систем можно выделить ядро (ядро ОС, машина данных СУБД), в свою очередь разделяемое на компоненту представления информации (файловая система ОС, модель данных СУБД), компоненту доступа к данным (система ввода–вывода ОС, процессор запросов СУБД) и надстройку (утилиты, сервис, интерфейсные компоненты) (рис. 3.1).

Субъекты Ядро системы Процессы Объекты

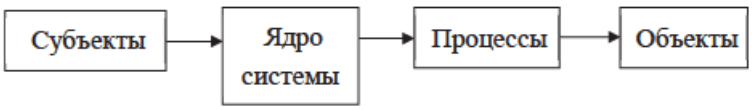

Рис. 3.1 - Незащищенная система

В защищенной системе появляется дополнительный компонент, обеспечивающий процессы защиты информации, прежде всего процедуры идентификации/аутентификации, а также управление доступом на основе той или иной политики безопасности (разграничения доступа) (рис. 7.2).

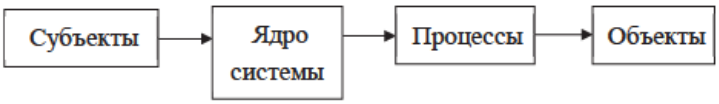

Рис. 3.2 - Защищенная система

С учетом нормативных требований по сертификации защищенных систем к реализации монитора безопасности предъявляются следующие обязательные требования:

1. Полнота. Монитор безопасности должен вызываться при каждом обращении за доступом любого субъекта к любому объекту, и не должно быть никаких способов его обхода.

2. Изолированность. Монитор безопасности должен быть защищен от отслеживания и перехвата работы.

3. Верифицируемость. Монитор безопасности должен быть проверяемым (само- или внешнетестируемым) на предмет выполнения своих функций.

4. Непрерывность. Монитор безопасности должен функционировать при любых, в том числе и аварийных ситуациях.

Монитор безопасности в защищенной системе является субъектом осуществления принятой политики безопасности, реализуя через алгоритмы своей работы соответствующие модели безопасности.

Аксиома 3. Для реализации принятой политики безопасности, управления и контроля доступа субъектов к объектам необходима информация и объект, ее содержащий.

Следствие 3.1. В защищенной системе существует особая категория активных сущностей, которые не инициализируют и которыми не управляют пользователи системы, — системные процессы (субъекты), присутствующие в системе изначально.

Следствие 3.2. Ассоциированный с монитором безопасности объект, содержащий информацию о системе разграничения доступа, является наиболее критическим с точки зрения безопасности информационным ресурсом в защищенной информационной системе.

Следствие 3.3. В защищенной системе может существовать доверенный пользователь (администратор системы), субъекты которого имеют доступ к ассоциированному с монитором безопасности объекту — данным для управления политикой разграничения доступа.

Принципы, способы представления и реализация ассоциированных с монитором безопасности объектов определяются типом политики безопасности и особенностями конкретной системы.

К настоящему времени разработано большое количество различных моделей безопасности, все они выражают несколько исходных политик безопасности. При этом имеет значение критерий безопасности доступов субъектов к объектам, т. е. правило разделения информационных потоков, порождаемых доступом субъектов к объектам, на безопасные и небезопасные.

Система безопасна тогда и только тогда, когда субъекты не имеют возможностей нарушать (обходить) установленную в системе политику безопасности.

Субъектом обеспечения политики безопасности выступает монитор безопасности. Его наличие в структуре системы соответственно является *необходимым* условием безопасности. Что касается условий *достаточности,* то они заключены в безопасности самого монитора безопасности.

4 Политика и модели дискреционного доступа. Парольные системы разграничения доступа. Политика и модели мандатного доступа

Политика и модели дискреционного доступа

Политика дискреционного (избирательного) доступа реализована в большинстве защищенных систем и исторически является первой проработанной в теоретическом и практическом плане.

Первые описания моделей дискреционного доступа к информации появились еще в 1960-х гг. и подробно представлены в литературе. Наиболее известны модель АДЕПТ-50 (конец 1960-х гг.), пятимерное пространство Хартсона (начало 1970-х гг.), модель Хариссона — Руззо-Ульмана (середина 1970-х гг.), модель Take-Grant (1976 г.). Авторами и исследователями этих моделей был внесен значительный вклад в теорию безопасности информационных систем, а их работы заложили основу для последующего создания и развития защищенных информационных систем.

Модели дискреционного доступа непосредственно основываются на субъектно-объектной модели и развивают ее как совокупность некоторых множеств взаимодействующих элементов (субъектов, объектов и т. д.). Множество (область) безопасных доступов в моделях дискреционного доступа определяется дискретным набором троек «пользователь (субъект) — поток (операция) — объект».

В модели, исходя из способа представления области безопасного доступа и механизма разрешений на доступ, анализируется и доказывается, что за конечное число переходов система останется в безопасном состоянии.

Модели на основе матрицы доступа

На практике наибольшее применение получили дискреционные модели, основанные на матрице доступа. В данных моделях область безопасного доступа строится как прямоугольная матрица (таблица), строки которой соответствуют субъектам доступа, столбцы — объектам доступа, а в ячейках записываются разрешенные операции (права) субъекта над объектом (рис. 3.3). В матрице используются следующие обозначения: *w* — «писать», *r* — «читать», *e* — «исполнять».

Рис. 3.3 - Матрица доступа

Права доступа в ячейках матрицы в виде разрешенных операций над объектами определяют виды безопасного доступа субъекта к объекту. Для выражения типов разрешенных операций используются специальные обозначения, составляющие основу (алфавит) некоторого языка описания политики разграничения доступа. Таким образом, в рамках дискреционной политики каждая ячейка содержит некоторое подмножество троек «субъект — операция — объект».

Матрица доступа представляет собой ассоциированный с монитором безопасности объект, содержащий информацию о политике разграничения доступа в конкретной системе. Структура матрицы, ее создание и изменение определяются конкретными моделями и конкретными программно-техническими решениями систем, в которых они реализуются.

Принцип организации матрицы доступа в реальных системах определяет использование двух подходов — централизованного и распределенного.

При *централизованном* подходе матрица доступа создается как отдельный самостоятельный объект с особым порядком размещения и доступа к нему. Количество объектов и субъектов доступа в реальных системах может быть велико. Для уменьшения количества столбцов матрицы объекты доступа могут делиться на две группы — группу объектов, доступ к которым не ограничен, и группу объектов дискреционного доступа. В матрице доступа представляются права пользователей только к объектам второй группы. Наиболее известным примером такого подхода являются «биты доступа» в UNIX-системах.

При *распределенном* подходе матрица доступа как отдельный объект не создается, а представляется или *«списками доступа»,* распределенными по объектам системы, или *«списками возможностей»,* распределенными по субъектам доступа. В первом случае каждый объект системы, помимо идентифицирующих характеристик, наделяется еще своеобразным списком, непосредственно связанным с самим объектом и представляющим, по сути, соответствующий столбец матрицы доступа. Во втором случае список с перечнем разрешенных для доступа объектов (строку матрицы доступа) получает каждый субъект при своей инициализации.

И централизованный, и распределенный принципы организации матрицы доступа имеют свои преимущества и недостатки, присущие в целом централизованному и децентрализованному принципам организации и управления.

Согласно *принципу управления доступом* выделяются два подхода:

· принудительное управление доступом;

· добровольное управление доступом.

В случае принудительного управления право создания и изменения матрицы доступа имеют только субъекты администратора системы, который при регистрации для работы в системе нового пользователя создает с соответствующим заполнением новую строку матрицы доступа, а при возникновении нового объекта, подлежащего избирательному доступу, образует новый столбец матрицы доступа. Подобный подход наиболее широко представлен в базах данных.

Принцип *добровольного управления доступом* основывается на принципе владения объектами. Владельцем объекта доступа называется пользователь, инициализировавший поток, в результате чего объект возник в системе, или определивший его иным образом. Права доступа к объекту определяют их владельцы.

Заполнение и изменение ячеек матрицы доступа осуществляют субъекты пользователей-владельцев соответствующих объектов. Подобный подход обеспечивает управление доступом в тех системах, в которых количество объектов доступа является значительным или неопределенным. Такая ситуация типична для операционных систем.

Все дискреционные модели уязвимы для атак с помощью «троянских» программ, поскольку в них контролируются только операции доступа субъектов к объектам, а не потоки информации между ними. Поэтому, когда «троянская» программа переносит информацию из доступного этому пользователю объекта в объект, доступный нарушителю, то формально никакое правило дискреционной политики безопасности не нарушается, но утечка информации происходит.

Парольные системы разграничения доступа

В документальных информационных системах, в системах автоматизации документооборота широкое распространение получили так называемые парольные системы разграничения доступа, представляющие отдельную разновидность механизмов реализации дискреционного принципа разграничения доступа.

Основные положения парольных систем можно сформулировать следующим образом.

1. Система представляется следующим набором сущностей:

· множеством информационных объектов (документов) $O(o_1, \ldots, o_m)$;

· множеством пользователей $S(s_1, \ldots, s_n)$;

· множеством паролей доступа к объектам $K(k_1, \ldots, k_p)$.

2. В системе устанавливается отображение множества O на множество K, задаваемое следующей функцией:

$$f_{ko} : O \rightarrow K.$$

Значением функции $f_{ko}(o) = k_o$ является пароль k_o доступа к документу o.

3. Область безопасного доступа задается множеством троек (s, k, o), каждый элемент которого соответствует владению пользователем паролем доступа к объекту. В результате устанавливается отображение множества S на множество K:

$$f_{ks} : S \rightarrow K.$$

Значением $f_{ks}(s) = K_s$ является набор паролей доступа к документам системы, известных пользователю s.

4. Процессы доступа пользователей к объектам системы организуются в две фазы:

· фаза открытия документа;

· фаза закрытия (сохранения) документа.

При открытии документа o пользователь s предъявляет (вводит, передает) монитору безопасности АС пароль $ks0$ доступа к данному документу.

Запрос в доступе удовлетворяется, если $k_{s0} = f_{k0}(o)$.

В случае успешного открытия пользователю предоставляются права работы по фиксированному набору операций с объектом.

Возможны два подхода, соответствующие добровольному и принудительному способам управления доступом.

При использовании принудительного способа назначение паролей доступа к документам, их изменение осуществляет только выделенный пользователь — администратор системы.

При необходимости шифрования измененного объекта или при появлении в системе нового объекта, подлежащего дискреционному доступу к нему, администратор системы на основе специальной процедуры генерирует пароль доступа к новому объекту, зашифровывает документ на ключе, созданном на основе пароля, и фиксирует новый документ в зашифрованном состоянии в системе. Администратор сообщает пароль доступа к данному документу тем пользователям, которым он необходим. Тем самым формируется подмножество троек доступа $\{(s_1, k, o), (s_2, k, o), \ldots\}$ к документу o.

При добровольном управлении доступом описанную выше процедуру формирования подмножества троек доступа к новому документу производят владельцы объекта.

Преимуществом парольных систем по сравнению с системами дискреционного разграничения доступа, основанными на матрице доступа, является то, что в них отсутствует ассоциированный с монитором безопасности объект, хранящий информацию о разграничении доступа к конкретным объектам.

Данный объект является наиболее критичным с точки зрения безопасности объектом системы.

Кроме того, в парольных системах обеспечивается безопасность и в том случае, когда не ограничен или технически возможен доступ посторонних лиц к носителям, на которых фиксируются и хранятся зашифрованные объекты.

Эти преимущества парольных систем разграничения доступа обусловливают их чрезвычайно широкое применение в документальных информационных системах.

Несмотря на то, что дискреционные модели разработаны почти 40 лет назад, и то, что многочисленные исследования показали их ограниченные защитные свойства, данные модели широко применяются на практике. Основные их достоинства — это простота и максимальная детальность в организации доступа.

Политика и модели мандатного доступа

Политика мандатного доступа является примером использования технологий, наработанных во внекомпьютерной сфере, в частности принципов организации секретного

делопроизводства и документооборота, применяемых в государственных структурах большинства стран.

Основным положением политики мандатного доступа является назначение всем участникам процесса обработки защищаемой информации и документам, в которых она содержится, специальной метки, например *секретно, сов. секретно* и т. д., получившей название уровня безопасности. Все уровни безопасности упорядочиваются с помощью установленного отношения доминирования, например, уровень *сов. секретно* считается более высоким, чем уровень *секретно.* Контроль доступа осуществляется в зависимости от уровней безопасности взаимодействующих сторон на основании двух правил:

1. *No read up (NRU)* — нет чтения вверх: субъект имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности.

2. *No write down (NWD)* — нет записи вниз: субъект имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности.

Первое правило обеспечивает защиту информации, обрабатываемой более доверенными (высокоуровневыми) лицами, от доступа со стороны менее доверенных (низкоуровневых).

Второе правило предотвращает утечку информации (сознательную или несознательную) от высокоуровневых участников процесса обработки информации к низкоуровневым.

Формализация механизмов разграничения доступа в секретном делопроизводстве применительно к субъектно-объектной модели показала необходимость решения следующих задач:

· разработки процедур формализации правила NRU, а в особенности правила NWD;

· построения формального математического объекта и процедур, адекватно отражающих систему уровней безопасности (систему допусков и грифов секретности).

При представлении служащих, работающих с секретными документами, в качестве субъектов доступа, а секретных документов в качестве объектов доступа буквальное следование правилу NWD приводит к включению в механизмы обеспечения безопасности субъективного фактора в лице субъекта-пользователя, который при внесении информации должен оценить соответствие вносимой информации уровню безопасности документа. Задача исключения данного субъективного фактора может решаться различными способами, самым простым из которых является полный запрет изменения субъектами объектов с уровнем безопасности более низким, чем уровень безопасности соответствующих субъектов. При этом существенно снижается функциональность системы.

Таким образом, если в дискреционных моделях управление доступом происходит путем наделения пользователей полномочиями осуществлять определенные операции над определенными объектами, то мандатные модели управляют доступом неявным образом — с помощью назначения всем сущностям системы уровней безопасности, которые определяют все допустимые взаимодействия между ними. Следовательно, мандатное управление доступом не различает сущностей, которым присвоен одинаковый уровень безопасности, и на их взаимодействия ограничения отсутствуют. Любой объект определенного уровня безопасности доступен любому субъекту соответствующего уровня безопасности (с учетом правил NRU и NWD). Мандатный подход к разграничению доступа, основанный лишь на понятии уровня безопасности, без учета специфики других характеристик субъектов и объектов приводит в большинстве случаев к избыточности прав доступа конкретных субъектов в пределах соответствующих классов безопасности. Для устранения данного недостатка мандатный принцип разграничения доступа дополняется дискреционным внутри соответствующих классов безопасности.

В теоретических моделях для этого вводят *матрицу доступа,* разграничивающую разрешенный по мандатному принципу доступ к объектам одного уровня безопасности.

5 Теоретико-информационные модели

Одной из самых труднорешаемых проблем безопасности в информационных системах, в том числе и основанных на моделях мандатного доступа, является проблема скрытых каналов утечки информации.

Скрытым каналом утечки информации называется механизм, посредством которого в системе может осуществляться информационный поток (передача информации) между сущностями в обход политики разграничения доступа.

Например, к скрытым каналам утечки информации относятся рассмотренные ранее потоки, возникающие за счет «троянских» программ, и неявные информационные потоки в системах на основе дискреционных моделей.

Скрытым каналом утечки информации в системах мандатного доступа является механизм, посредством которого может осуществляться передача информации от сущностей с высоким уровнем безопасности к сущностям с низким уровнем безопасности без нарушения правил NRU и NWD. В определенных случаях информацию можно получить или передать и без непосредственного осуществления операций *read*/*write* к объектам, в частности на основе анализа определенных процессов и параметров системы. Например, если по правилу NRU нельзя читать секретный файл, но можно «видеть» его объем, то высокоуровневый субъект, меняя по определенному правилу объем секретного файла, может таким кодированным образом передавать секретную информацию низкоуровневому объекту.

От высокоуровневых субъектов может передаваться информация о количестве создаваемых или удаляемых секретных файлов, получить доступ по чтению, к которым низкоуровневые субъекты не могут, но «видеть» их наличие и соответственно определять их количество могут.

Другие возможности «тайной» передачи информации могут основываться на анализе временных параметров протекания процессов.

Скрытые каналы утечки информации можно разделить на три вида:

· скрытые каналы по памяти (на основе анализа объема и других статических параметров объектов системы);

· скрытые каналы по времени (на основе анализа временных параметров протекания процессов системы);

· скрытые статистические каналы (на основе анализа статистических параметров процессов системы).

Требования по перекрытию и исключению скрытых каналов впервые были включены в спецификацию уровней защиты автоматизированных систем, предназначенных для обработки сведений, составляющих государственную тайну в США (Оранжевая книга).

Теоретические основы подходов к решению проблемы скрытых каналов разработаны Д. Денингом, исследовавшим принципы анализа потоков данных в программном обеспечении и принципы контроля совместно используемых ресурсов. Основываясь на идеях Денинга, Дж. Гоген и Дж. Мезигер предложили теоретико-информационный подход на основе понятий *информацинной невыводимости* и *информационного невмешательства*.

Сущность данного подхода заключается в отказе от рассмотрения процесса функционирования информационной системы как детерминированного процесса. При рассмотрении моделей конечных состояний (HRU, TAKE-GRANT, Белла — ЛаПадулы) предполагалось, что функция перехода в зависимости от запроса субъекта и текущего состояния системы однозначно определяет следующее состояние системы. В системах

коллективного доступа (много пользователей, много объектов) переходы, следовательно, и состояния системы обусловливаются большим количеством самых

разнообразных, в том числе и случайных, факторов, что предполагает использование аппарата теории вероятностей для описания системы.

При таком подходе политика безопасности требует определенной модификации и, в частности, теоретико-вероятностной трактовки процессов функционирования систем и опасных информационных потоков:

1. Информационная система рассматривается как совокупность двух непересекающихся множеств сущностей:

· множества высокоуровневых объектов *H*;

· множества низкоуровневых объектов *L*.

Информационная система представляется мандатной системой с решеткой, состоящей всего из двух уровней безопасности — высокого и низкого и соответственно определяющей невозможность обычных (*read*/*write*) информационных потоков «сверху вниз».

2. Состояние любого объекта является случайным. Понятие информационной невыводимости основывается на определении «опасных» потоков: в системе присутствует информационный поток от высокоуровневых объектов к низкоуровневым, если некое возможное значение переменной в некотором состоянии низкоуровневого объекта невозможно одновременно с определенными возможными значениями переменных состояний высокоуровневых объектов.

3. Формулируется следующий критерий информационной невыводимости: система безопасна в смысле информационной невыводимости, если в ней отсутствуют информационные потоки вида, задаваемого в п. 2.

Анализ критерия информационной невыводимости показывает, что его требования являются чрезвычайно жесткими и достижимы, в частности, при полной изоляции высокоуровневых объектов от низкоуровневых.

Требование отсутствия выводимости высокоуровневой информации на основе анализа состояний низкоуровневых объектов одновременно приводит и к обратному, т. е. отсутствию возможностей выводимости низкоуровневой информации из анализа состояний высокоуровневых объектов. Данное свойство является избыточным и противоречит основным положениям мандатной политики, а именно — неопасности и допустимости потоков «снизу вверх» от низкоуровневых сущностей к сущностям с более высокими уровнями безопасности.

Другой подход основывается на идее *информационного невмешательства.* Понятие опасных потоков имеет здесь следующий смысл: в системе присутствует информационный поток от высокоуровневых объектов к низкоуровневым, если информация (состояние) низкоуровневых объектов зависит от информации высокоуровневых объектов. Это значит, что на состояние высокоуровневых объектов в текущий момент времени не влияет состояние низкоуровневых объектов в предшествующий момент времени и наоборот. Разноуровневые объекты не имеют возможности влиять на последующие состояния объектов другого уровня. Анализ процессов функционирования информационной системы показывает, что такие требования являются чрезвычайно жесткими, фактически совпадающими с требованиями полной изоляции разноуровневых сущностей.

Несмотря на то, что понятия информационной невыводимости и информационного невмешательства непосредственно не применимы для разграничения доступа, они послужили основой широко применяемых в современных информационных системах *технологий представлений и разрешенных процедур*. Эти технологии исторически возникли как политика разграничения доступа в СУБД.

Представлением информации в информационной системе называется процедура формирования и представления пользователю (после его входа в систему и аутентификации) необходимого подмножества информационных объектов, в том числе с возможным их количественным и структурным видоизменением исходя из задач разграничения доступа к информации.

В технологиях представлений пользователи, входя и работая в системе, оперируют не с реальной, а с виртуальной системой, формируемой индивидуально для каждого. В результате задача разграничения доступа решается автоматически. Проблемы безопасности при этом сводятся к скрытым каналам утечки информации, рассмотрение и нейтрализация которых осуществляется на основе анализа условий и процедур, обеспечивающих выполнение критериев безопасности.

Технология представлений решает проблему скрытых каналов утечки первого вида. Часть каналов второго и третьего вида перекрывается техникой разрешенных процедур. Системой разрешенных процедур называется разновидность интерфейса системы, когда при входе в систему аутентифицированным пользователям предоставляется только возможность запуска и исполнения конечного набора логико-технологических процедур обработки информации без возможности применения элементарных методов доступа (read, write, create и т. п.) к информационным объектам системы. Следовательно, в системах с интерфейсом разрешенных процедур пользователи не видят информационные объекты, а выполняют операции на уровне логических процедур. Автоматизированная система при этом для пользователей превращается в дискретный автомат, получающий команды на входе и выдающий обработанную информацию на выходе.

Впервые подобный подход к представлению информационной системы был рассмотрен Гогеном (J. Goguen) и Мезигером (J. Meseguer), предложившими *автоматную модель информационного невлияния* (невмешательства) — GM-модель.

6 Политика и модели тематического разграничения доступа. Ролевая модель безопасности

Политика и модели тематического разграничения доступа

Политика тематического разграничения доступа близка к политике мандатного доступа.

Общей основой является введение специальной процедуры классификации сущностей системы (субъектов и объектов доступа) по какому-либо критерию. Выше рассматривалось, что основой классификации сущностей АС в моделях мандатного доступа является линейная решетка на упорядоченном множестве уровней безопасности. При этом использование аппарата решеток является принципиальным, так как посредством механизмов наименьшей верхней и наибольшей нижней границ обеспечивается возможность анализа опасности/неопасности потоков между любой парой сущностей системы.

В ряде случаев основанием для классификации информации и субъектов доступа к ней выступают не конфиденциальность данных и доверие к субъектам доступа, как в мандатных моделях, а тематическая структура предметной области информационной системы. Стремление расширить мандатную модель для отражения тематического принципа разграничения доступа, применяемого в государственных организациях многих стран, привело к использованию более сложных структур, чем линейная решетка уровней безопасности, именуемых MLS- решетками. MLS-решетка является произведением линейной решетки уровней безопасности и решетки подмножеств множества категорий (тематик).

Еще одним фактором, обусловливающим необходимость построения специальных моделей тематического разграничения доступа, является то, что в большинстве случаев на классификационном множестве в документальных информационных системах устанавливается не линейный порядок (как на множестве уровней безопасности в мандатных моделях), а частичный порядок, задаваемый определенного вида корневыми деревьями (иерархические и фасетные рубрикаторы).

Важным аспектом, присутствующим в практике разграничения доступа к «бумажным» ресурсам, является тематическая «окрашенность» информационных ресурсов предприятий, учреждений по организационно-технологическим процессам и профилям деятельности.

Организация доступа сотрудников к информационным ресурсам (в библиотеках, архивах, документальных хранилищах) осуществляется на основе *тематических классификаторов.* Все документы информационного хранилища тематически индексируются, т. е. соотносятся с теми или иными тематическими рубриками классификатора. Сотрудники предприятия согласно своим функциональным обязанностям или по другим основаниям получают права работы с документами определенной тематики. Данный подход в сочетании с дискреционным и мандатным доступом, обеспечивает более адекватную и гибкую настройку системы разграничения доступа на конкретные функционально-технологические процессы, предоставляет дополнительные средства контроля и управления доступом.

Ролевая модель безопасности

Ролевая модель безопасности представляет собой существенно усовершенствованную модель Харрисона–Руззо–Ульмана, однако ее нельзя отнести ни к дискреционным, ни к мандатным, потому что управление доступом в ней осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов. Поэтому ролевая модель представляет собой совершенно особый тип политики, которая основана на компромиссе между гибкостью управления доступом, характерной для дискреционных моделей, и жесткостью правил контроля доступа, присущей мандатным моделям.

В ролевой модели классическое понятие «субъект» замещается понятиями «пользователь» и «роль». Пользователь — это человек, работающий с системой и выполняющий определенные служебные обязанности. Роль — это активно действующая в системе абстрактная сущность, с которой связан набор полномочий, необходимых для осуществления определенной деятельности. Самым распространенным примером роли является присутствующий почти в каждой системе административный бюджет (например, root для UNIX и Administrator для Windows NT), который обладает специальными полномочиями и может использоваться несколькими пользователями.

Ролевая политика распространена очень широко, потому что она, в отличие от других более строгих и формальных политик, очень близка к реальной жизни. Ведь на самом деле работающие в системе пользователи действуют не от своего личного имени, они всегда осуществляют определенные служебные обязанности, т. е. выполняют некоторые роли, которые никак не связаны с их личностью.

Поэтому вполне логично осуществлять управление доступом и назначать полномочия не реальным пользователям, а абстрактным (неперсонифицированным) ролям, представляющим участников определенного процесса обработки информации. Такой подход к политике безопасности позволяет учесть разделение обязанностей и полномочий между участниками прикладного информационного процесса, т. к. с точки зрения ролевой политики имеет значение не личность пользователя, осуществляющего доступ к информации, а то, какие полномочия ему необходимы для выполнения его служебных обязанностей.

В такой ситуации ролевая политика позволяет распределить полномочия между этими ролями в соответствии с их служебными обязанностями: роли администратора назначаются специальные полномочия, позволяющие ему контролировать работу системы и управлять ее конфигурацией, роль менеджера баз данных позволяет осуществлять управление сервером баз данных, а права простых пользователей ограничиваются минимумом, необходимым для запуска прикладных программ. Кроме того, количество ролей в системе может не соответствовать количеству реальных пользователей: один пользователь, если на нем лежит множество обязанностей, требующих различных полномочий, может выполнять (одновременно или последовательно) несколько ролей, а несколько пользователей могут выполнять одну и ту же роль, если они производят одинаковую работу.

При использовании ролевой политики управление доступом осуществляется в две стадии: во-первых, для каждой роли указывается набор полномочий, представляющий

набор прав доступа к объектам, во-вторых — каждому пользователю назначается список доступных ему ролей. Полномочия назначаются ролям в соответствии с принципом наименьших привилегий, из которого следует, что каждый пользователь должен обладать только минимально необходимым для выполнения своей работы набором полномочий.

В отличие от других политик, ролевая политика практически не гарантирует безопасность с помощью формального доказательства, а только определяет характер ограничений, соблюдение которых и служит критерием безопасности системы.

Такой подход позволяет получать простые и понятные правила контроля доступа, которые легко могут быть применены на практике, но лишает систему теоретической доказательной базы. В некоторых ситуациях это обстоятельство затрудняет использование ролевой политики, однако в любом случае оперировать ролями гораздо удобнее, чем субъектами, поскольку это более соответствует распространенным технологиям обработки информации, предусматривающим разделение обязанностей и сфер ответственности между пользователями. Кроме того, ролевая политика может использоваться одновременно с другими политиками безопасности, когда полномочия ролей, назначаемых пользователям, контролируются дискреционной или мандатной политикой, что позволяет строить многоуровневые схемы контроля доступа.

ВЫВОДЫ

Определение политики безопасности и модели этой политики позволяют теоретически обосновать безопасность системы при корректном определении модели системы и ограничений в ее использовании. Обеспечение информационной безопасности предполагает повышение защищенности информации за счет разграничения доступа. В последнее десятилетие как в нашей стране, так и за рубежом активно проводятся исследования по развитию моделей разграничения доступа. Дальнейшими направлениями исследований в этой сфере могут быть поиски решений разграничения доступа в гипертекстовых информационно-поисковых системах, развитие концепции мультиролей в системах ролевого доступа, развитие моделей комплексной оценки защищенности системы.