

БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ

2. Разграничение доступа

Несанкционированный доступ к данным в ИС

- Анализ наносимого ущерба от различных видов угроз ИТ-безопасности показывает, что одной из наиболее опасных угроз является несанкционированный доступ (НСД) к конфиденциальной информации.
- По уровню наносимого ущерба этот вид угроз лишь незначительно уступает только вирусным инфекциям.
- В ИС НСД может быть реализован на двух этапах – при входе в ИС (путем фальсификации процедур идентификации / аутентификации) и на стадии *авторизации*.

Авторизация

- *Авторизация* особенно важна в развитых многопользовательских ИС, содержащих большие объемы данных различного назначения и разной степени конфиденциальности. Такие ИС, в первую очередь, представлены системами баз данных (БД). Далее, вопросы контроля доступа будут обсуждаться в ориентации именно на такие ИС.
- Конкретные механизмы управления доступом, применяемые в ИС основаны на определенных *моделях безопасности*.

Авторизация

- В ИС каждое групповое данное должно иметь связанный с ним собственный набор ограничений доступа. При осуществлении доступа в ИС проверяется, не нарушено ли какое-либо ограничение из набора. В случае нарушения, выполнение операции пользователя должно подавляться с выдачей сигнала ошибки и фиксацией в журнале попытки нарушения безопасности.
- Процедуры регулирования допустимых действий пользователей по отношению к различным данным в ИС называют *авторизацией* (от англ. authorization – разрешение, уполномочивание) или управлением доступом (контролем доступа).

Объекты и информация

- В общем случае, контроль доступа в ИС основан на использовании *субъектно-объектной модели доступа*.
- *Аксиома*. Любая информация в КС представляется *словом* в некотором языке *Я*.
- *Определение*. *Объект* – это произвольное конечное множество слов языка *Я*.
- *Определение*. *Преобразование информации* – это отображение, заданное на множестве слов языка *Я*.
- Преобразование информации осуществляется во времени, поэтому оно может или выполняться, или храниться.

Субъекты. Доступы субъектов

- ▣ **Определение. Субъект** – это сущность, описывающая преобразование информации в КС.
- ▣ Субъект для выполнения преобразования использует информацию, содержащуюся в объектах КС, т. е. осуществляет **доступ** к ним. Основными видами доступа являются:
 - ▣ доступ субъекта к объекту на *чтение (read)*;
 - ▣ доступ субъекта к объекту на *запись (write)*;
 - ▣ доступ субъекта к объекту на *активизацию (execute)*.

Доступы субъектов к объектам.

Угрозы безопасности

- ▣ **Аксиома.** Все вопросы безопасности информации описываются *доступами субъектов к объектам*.
- ▣ **Определение . Угроза** (threat) безопасности информации (КС) – это потенциально осуществимое воздействие на КС, которое прямо или косвенно может нанести ущерб безопасности информации.

Угрозы безопасности

- Угрозы направлены на *три основных свойства* (компонента, аспекта) безопасности информации:
 - ▢ **конфиденциальность** (confidentiality – защита от несанкционированного доступа);
 - ▢ **целостность** (integrity – защита от несанкционированного изменения информации);
 - ▢ **доступность** (availability – защита от несанкционированного удержания информации и ресурсов, защита от разрушения, защита работоспособности).
- Угрозы реализуют или пытаются реализовать **нарушители** (violations, perpetrators) информационной безопасности.

Действия нарушителей

- По отношению к КС нарушители ИБ могут совершать *атаки и злоупотребления*.
- Атака (attack) (вторжение) – это действие, которым нарушитель пытается скомпрометировать (поставить под угрозу) конфиденциальность, целостность или доступность информации.
- Злоупотребление (misuse) – это слово имеет широкое толкование и может отражать различные события, начиная от кражи конфиденциальных данных и заканчивая засорением почтовой системы спамом. *Злоупотребление определяет действие, которое нарушает стратегию использования сети*, в то время как атака определяет действие, которое *ставит под угрозу защиту сети*.

Уязвимости. Модель нарушителя

- Злоумышленник реализует угрозы, путем использования *уязвимостей* КС.
- Уязвимость (vulnerability) – любая характеристика или свойство КС, использование которой нарушителем может привести к реализации угрозы.
- Иными словами, это слабые места в системе. Уязвимости могут использоваться для компрометации (взлома) систем.
- Формализованное описание или представление комплекса возможностей нарушителя по реализации тех или иных угроз безопасности информации называется *моделью нарушителя* (violator model).

Политика и модель безопасности

- Фундаментальным понятием в сфере защиты информации компьютерных систем является *политика безопасности*. Под ней понимают интегральную совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает состояние защищенности информации в заданном пространстве угроз.
- Формальное выражение и формулирование политики безопасности (математическое, схемотехническое, алгоритмическое и т. д.) называют *моделью безопасности*.

Модели безопасности

- ▣ *Модели безопасности* играют важную роль в процессах разработки и исследования защищенных КС, так как обеспечивают системотехнический подход, включающий решение следующих важнейших задач:
 - ▣ выбор и обоснование базовых принципов архитектуры защищенных КС;
 - ▣ подтверждение свойств (защищенности) разрабатываемых систем путем формального доказательства соблюдения ПБ;
 - ▣ составление формальной спецификации ПБ как важнейшей составной части обеспечения разрабатываемых защищенных КС.

Субъектно-объектная формализация КС

- В механизмах и процессах коллективного доступа к информационным ресурсам большинство моделей разграничения доступа основывается на представлении КС как совокупности *субъектов и объектов* доступа. Основные положения *субъектно-объектной* формализации КС в аспекте безопасности информации состоят в следующем.

Субъектно-объектная формализация КС

1. В КС действует дискретное время.
2. В каждый фиксированный момент времени t_k КС представляет собой конечное множество элементов, разделяемых на два подмножества:
 - подмножество субъектов доступа S ;
 - подмножество объектов доступа O .
3. Пользователи КС представлены одним или некоторой совокупностью субъектов доступа, действующих от имени конкретного пользователя.
4. Субъекты КС могут быть порождены из объектов только активной сущностью (другим субъектом).

Субъекты и объекты доступа

- ▣ **Определение.** Под *субъектом доступа* понимается активная сущность КС, которая может изменять состояние системы через порождение процессов над объектами, в том числе, порождать новые объекты и инициализировать порождение новых субъектов.
- ▣ **Определение.** Под *объектом доступа* понимается пассивная сущность КС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов.
- ▣ Предполагается наличие априорно безошибочного механизма различения активных и пассивных сущностей (т. е. субъектов и объектов) по свойству активности.

Субъектно-объектная формализация КС

- ▣ **Определение.** Под *пользователем* КС понимается лицо, внешний фактор, аутентифицируемый некоторой информацией, и управляющий одним или несколькими субъектами, воспринимающий объекты и получающий информацию о состоянии КС через субъекты, которыми он управляет.
- ▣ Таким образом, в субъектно-объектной модели понятия субъектов доступа и пользователей не тождественны.

Порождение субъектов доступа

- ▣ **Определение.** Объект o_i называется источником для субъекта s_m если существует субъект s_j , в результате воздействия которого на объект o_i возникает субъект s_m .
- ▣ Соответственно, субъект s_j называется *активизирующим* для субъекта s_m .
- ▣ Для описания процессов порождения субъектов доступа вводится следующее обозначение:
- ▣ **Create** (s_j, o_i) $\rightarrow s_m$ – "из объекта o_i порожден субъект s_m при активизирующем воздействии субъекта s_j ".
- ▣ **Create** называют операцией порождения субъектов.

Потоки информации

- Активная сущность субъектов доступа заключается в их возможности осуществлять определенные действия над объектами, что приводит к возникновению потоков информации. Исходя из этого, *центральным положением субъектно-объектной модели* является следующее.
- *Все процессы безопасности в КС описываются доступами субъектов к объектам, вызывающими потоки информации.*

Потоки информации

- ▣ **Определение.** *Потоком информации* между объектом o_i и объектом o_j называется произвольная операция над объектом o_j , реализуемая субъектом s_m и зависящая от объекта o_i .
- ▣ Для описания потоков вводят следующее обозначение:
- ▣ ***Stream*** $(s_m, o_i) \rightarrow o_j$ – "поток информации от объекта o_i (o_j) к объекту o_j (o_i) через субъект s_m ".
- ▣ Виды различных операций над объектами – чтение, изменение, создание, удаление и т. д.
- ▣ Объекты o_i и o_j , в потоке, могут быть: как источниками, так и приемниками информации, как ассоциированными с субъектом, так и нет, а также могут быть пустыми ($\emptyset$) объектами (например, при создании или удалении файлов).

Доступы субъектов к объектам

- Поток всегда порождается субъектом доступа. На этом основании вводится следующее центральное в политике и моделях разграничения доступа понятие.
- **Определение.** Доступом субъекта s_m к объекту o_j называется порождение субъектом s_m потока информации между объектом o_j и некоторым(и) объектом o_i .
- Это определение позволяет средствами субъектно-объектной модели описывать процессы безопасности информации в защищенных КС. С этой целью вводится множество потоков P для всей совокупности фиксированных декомпозиций КС на субъекты и объекты во все моменты времени работы КС.

Легальные и нелегальные потоки информации в КС

- С точки зрения безопасности множество потоков P разбивается на два непересекающихся подмножества P_N и P_L : $P = P_L \cup P_N$, $P_L \cap P_N = \emptyset$,
- P_L – множество легальных (безопасных) потоков;
- P_N – множество нелегальных (опасных) потоков, нарушающих состояние защищенности информации в КС.
- На основе множества потоков возникает понятие, составляющее основу формализации политики разграничения доступа в моделях безопасности.
- *Правила разграничения доступа субъектов к объектам есть формально описанные легальные потоки P_L .*

Персонификация субъектов и объектов

- Анализ практического опыта по защите компьютерной информации, а также основных положений субъектно-объектной модели КС позволяет сформулировать несколько аксиоматических условий, касающихся структуры и функционирования защищенных КС.
- *Аксиома* . В защищенной КС в любой момент времени любой субъект и объект должны быть персонифицированы (идентифицированы и аутентифицированы) .
- Данная аксиома определяется самой природой и содержанием процессов коллективного доступа пользователей к ресурсам КС.

Монитор безопасности

- *Аксиома.* В защищенной КС должна присутствовать активная компонента (субъект, процесс и т. д.) с соответствующим объектом-источником, которая осуществляет управление доступом и контроль доступа субъектов к объектам.
- В литературе для данной активной компоненты утвердился термин *монитор безопасности* (сервер, менеджер, ядро безопасности, Trusted Computing Base – ТСВ). Монитор безопасности (МБ), по существу, реализует определенную политику безопасности во всех процессах обработки данных.

Ядро КС

- В структуре большинства типов программных средств, на основе которых строятся информационные системы (ОС, СУБД), можно выделить **ядро** (ядро ОС, машина данных СУБД), в свою очередь, разделяемое на **компоненту представления информации** (файловая система ОС, модель данных СУБД) и на **компоненту доступа к данным** (система ввода-вывода ОС, процессор запросов СУБД), а также **надстройку** (утилиты, сервис, интерфейсные компоненты).
- Инициализированные субъекты при осуществлении процессов доступа обращаются за сервисом, функциями к ядру системы.

Роль и место монитора безопасности в КС



Требования к монитору безопасности

- ▣ **Полнота.** Монитор безопасности должен вызываться (активизироваться) при каждом обращении за доступом любого субъекта к любому объекту, и не должно быть никаких способов его обхода;
- ▣ **Изолированность.** Монитор безопасности должен быть защищен от отслеживания и перехвата своей работы.
- ▣ **Верифицируемость.** Монитор безопасности должен быть проверяемым (само- или внешне тестируемым) на предмет выполнения своих функций.
- ▣ **4. Непрерывность.** Монитор безопасности должен функционировать при любых штатных и нештатных, в том числе и аварийных ситуациях.

Системны процессы

- Монитор безопасности, как и любая активная сущность в КС, является субъектом с соответствующим объектом-источником и ассоциированными объектами. Отсюда вытекают следующие важные следствия.
- **Следствие 1.** В защищенной КС существуют особая категория субъектов (активных сущностей), которые не инициализируют и которыми не управляют пользователи системы — это т. н. **системные процессы** (субъекты), присутствующие (функционирующие) в системе изначально.

Системные субъекты

- К числу *системных субъектов* относится исходный системный процесс, который инициализирует первичные субъекты пользователей, а также МБ, который управляет доступами субъектов пользователей к объектам системы. Соответственно, для обеспечения защищенности в КС свойства системных субъектов должны быть неизменными, от чего напрямую зависит безопасность.
- **Следствие 2.** Ассоциированный с МБ объект, содержащий информацию по системе разграничения доступа, является наиболее критическим с точки зрения безопасности информационным ресурсом в защищенной КС.

Доступ к объекту, ассоциированному с МБ

- Для планирования и управления системой разграничения доступа конкретного коллектива пользователей КС должна быть предусмотрена процедура доступа к ассоциированному с МБ объекту со стороны, т. е. через субъект(ы) пользователя. Отсюда вытекает еще одно важное следствие.
- **Следствие 3.** В защищенной системе должен существовать доверенный пользователь (*администратор системы*), субъекты которого имеют доступ к ассоциированному с монитором безопасности объекту для управления политикой разграничения доступа.

Политики безопасности

- Принципы, способы представления и реализация ассоциированных с МБ объектов определяются типом политики безопасности и особенностями конкретной КС.
- Несмотря на то, что к настоящему времени разработано и апробировано в практической реализации большое количество различных моделей безопасности КС, все они выражают лишь несколько исходных политик безопасности.
- В упрощенной трактовке *политику безопасности* понимают как общий принцип (методологию, правило, схему) безопасной работы (доступа) коллектива пользователей с общими информационными ресурсами.

Политики безопасности

- Важнейшее значение имеет критерий безопасности доступов субъектов к объектам, т. е. правило разделения информационных потоков, порождаемых доступами субъектов к объектам, на опасные и неопасные.
- Методологической основой для формирования политик безопасности в защищенных КС послужили реальные организационно-технологические схемы обеспечения безопасности информации во вне компьютерных сферах.
- Многие подходы к защите компьютерной информации были "подсмотрены", в частности, в сфере работы с "бумажными" конфиденциальными документами, т. е. в сфере делопроизводства.

Политики безопасности

- Выделяются следующие виды политик безопасности:
 - ▢ *дискреционная политика безопасности;*
 - ▢ *мандатная политика безопасности;*
 - ▢ *политика ролевого разграничения доступа;*
 - ▢ *политика безопасности информационных потоков;*
 - ▢ *политика изолированной программной среды;*
 - ▢ *тематическая политика безопасности* и др.
- Первые две политики безопасности дискреционная и мандатная являются основными (базовыми).

Дискреционная политика безопасности

- Определяется двумя свойствами:
 - все субъекты и объекты идентифицированы;
 - права доступа субъектов на объекты определяется на основании некоторого внешнего по отношению к системе правила.
- Множество безопасных (разрешенных) доступов P_L задается для именованных субъектов и объектов явным образом в виде дискретного набора троек "субъект-поток (операция)-объект".

Дискреционная политика безопасности

- Принцип дискреционной политики разграничения доступа можно охарактеризовать схемой "каждый с каждым", т. е. для любой из всевозможных комбинаций «субъект-объект» должно быть явно задано разрешение / запрещение доступа и вид соответствующей разрешенной / запрещенной операции (Read, Write и т. д.).
- Таким образом, при дискреционной политике разграничение доступа осуществляется самым детальным образом – до уровня отдельно взятого субъекта, отдельно взятого объекта доступа и отдельно взятой операции.

Дискреционная политика безопасности

- Достоинство ДПБ – относительно простая реализация системы разграничения доступа.
- Недостаток ДПБ относится к статичности определенных в ней правил разграничения доступа. Она не учитывает динамику изменения состояний КС.
- Кроме того, при использовании ДПБ возникает вопрос – определения правил распространения прав доступа и анализа их влияния на безопасность КС.
- В общем случае при использовании данной политики перед системой защиты (МБ) стоит алгоритмически неразрешимая задача – проверить, приведут ли действия субъекта к нарушению безопасности или нет.

Мандатная политика безопасности

- Множество безопасных (разрешенных) доступов P_L задается неявным образом через введение для пользователей-субъектов некоторой дискретной характеристики доверия (уровня допуска), а для объектов некоторой дискретной характеристики конфиденциальности (грифа секретности), и наделение на этой основе пользователей-субъектов некими полномочиями порождать определенные потоки в зависимости от соотношения "уровень допуска-поток (операция)-уровень конфиденциальности".

Мандатная политика безопасности

- В отличие от ДПБ, в МПБ разграничение доступа производится менее детально – до уровня группы пользователей с одним уровнем допуска и группы объектов с одним уровнем конфиденциальности. Это упрощает и улучшает схему управления доступом.
- Основная цель МПБ – предотвратить утечку информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа.
- Для систем с МПБ, задача проверки безопасности является алгоритмически разрешимой. Такие системы характеризуются более высокой надежностью. Недостаток МБП – более высокая сложность реализации.

Политика ролевого разграничения доступа

- Эта политика является развитием дискреционной политики; при этом права доступа субъектов на объекты группируются с учетом специфики их применения.
- Множество безопасных (разрешенных) доступов P_L задается через введение в системе дополнительных абстрактных сущностей – *ролей*, выступающих некими "типовыми" (ролевыми) субъектами доступа, с которыми ассоциируются конкретные пользователи (в роли которых осуществляют доступ).
- Ролевые субъекты доступа наделяются затем правами доступа к объектам системы на основе дискреционного или мандатного принципа.

Политика безопасности информационных потоков

- Основана на разделении всех возможных информационных потоков на два непересекающихся множества: *благоприятных* и *неблагоприятных*.
- Цель данной политики состоит в том, чтобы обеспечить невозможность возникновения в КС неблагоприятных информационных потоков.
- ПБИП в большинстве случаев используется в сочетании с политикой другого вида.
- Реализация ПБИП на практике, как правило, является трудной задачей, особенно, если необходимо обеспечить защиту КС от возникновения неблагоприятных информационных потоков во времени.

Политика изолированной программной среды

- Целью этой политики является определение порядка безопасного взаимодействия субъектов системы, обеспечивающего невозможность воздействия на систему защиты и модификации ее параметров или конфигурации, результатом которых могло бы стать изменение реализуемой системой защиты политики разграничения доступа.
- Политика изолированной программной среды реализуется путем изоляции субъектов системы друг от друга и путем контроля порождения новых субъектов таким образом, чтобы в системе могли активизироваться только субъекты из predetermined списка.

Политика тематического доступа

- Множество безопасных доступов задается неявным образом через введение:
 - для пользователей-субъектов некоторой тематической характеристики – разрешенных тематических информационных рубрик,
 - для объектов аналогичной характеристики в виде набора тематических рубрик, информация по которым содержится в объекте.
- На этой основе осуществляется наделение субъектов-пользователей полномочиями порождать определенные потоки в зависимости от соотношения наборов тематических рубрик субъекта и объекта.