Информационная безопасность

Лекция 3

Политика безопасности

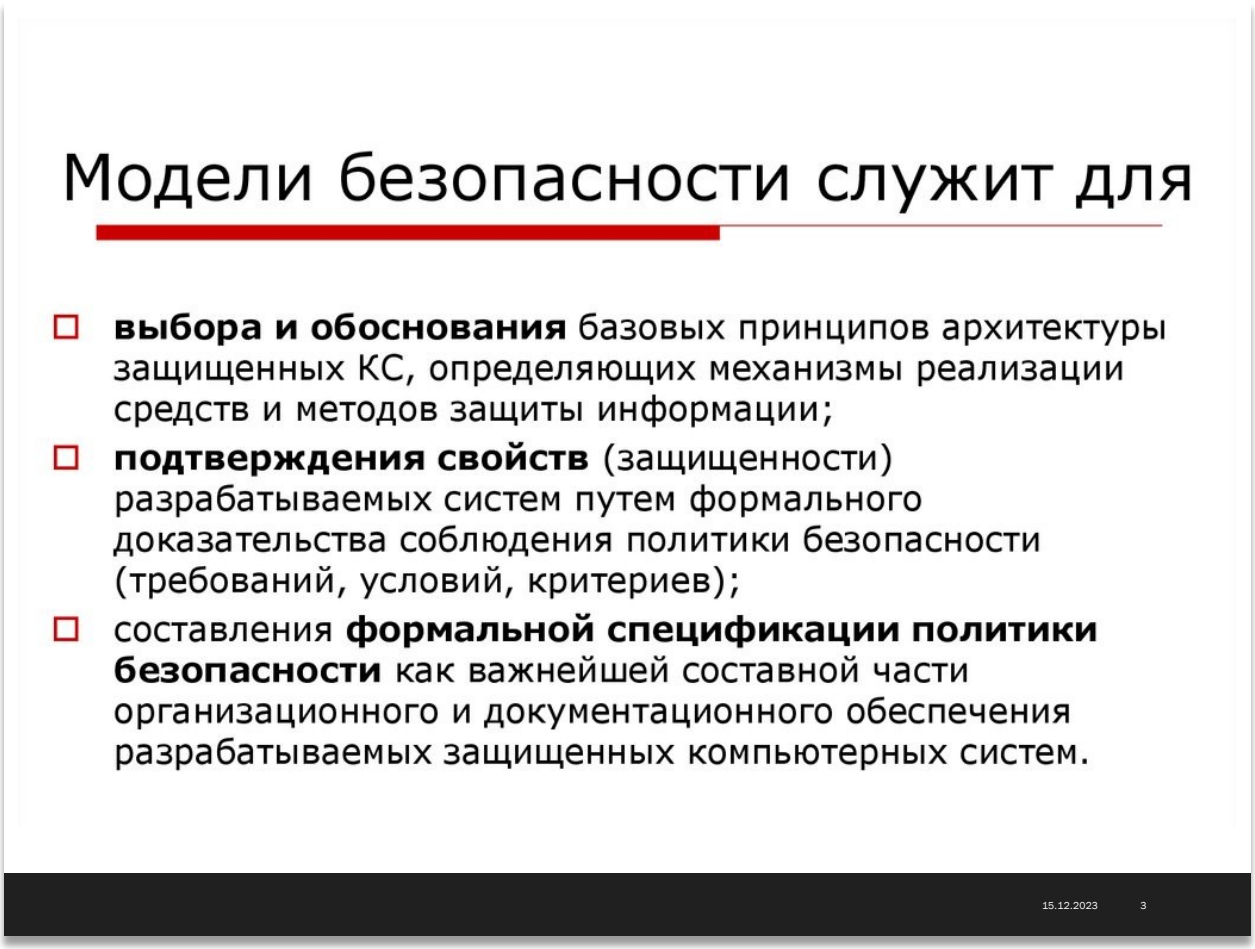
Технология защиты информационных систем начала развиваться относительно недавно, но уже сегодня существует значительное число теоретических моделей, позволяющих описывать различные аспекты безопасности и обеспечивать средства защиты с формальной стороны.

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.

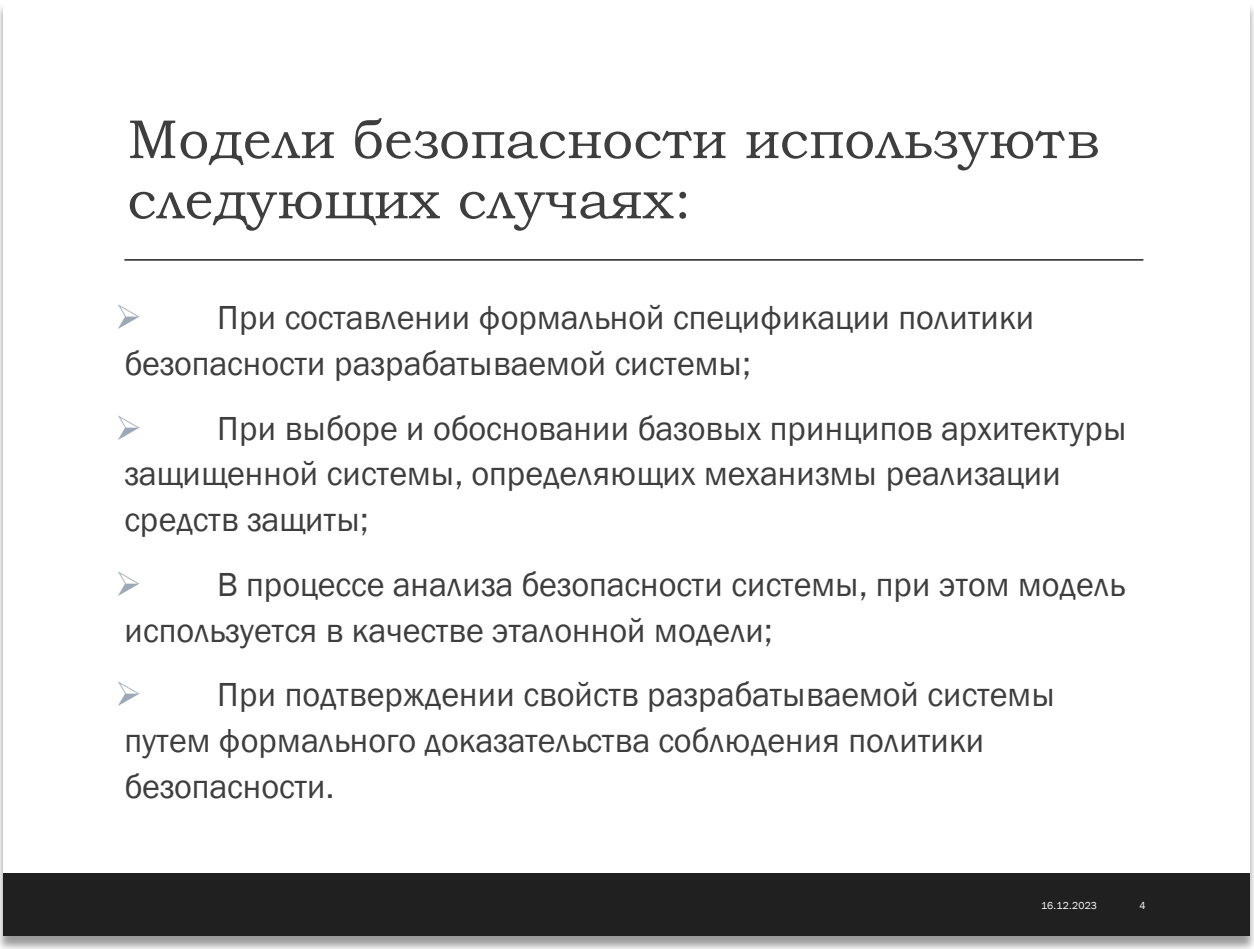
Кроме того, модели безопасности позволяют решить еще целый ряд задач, возникающих в ходе проектирования, разработки и сертификации защищенных систем, поэтому их используют не только теоретики информационной безопасности, но и другие категории специалистов, участвующих в процессе создания и эксплуатации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

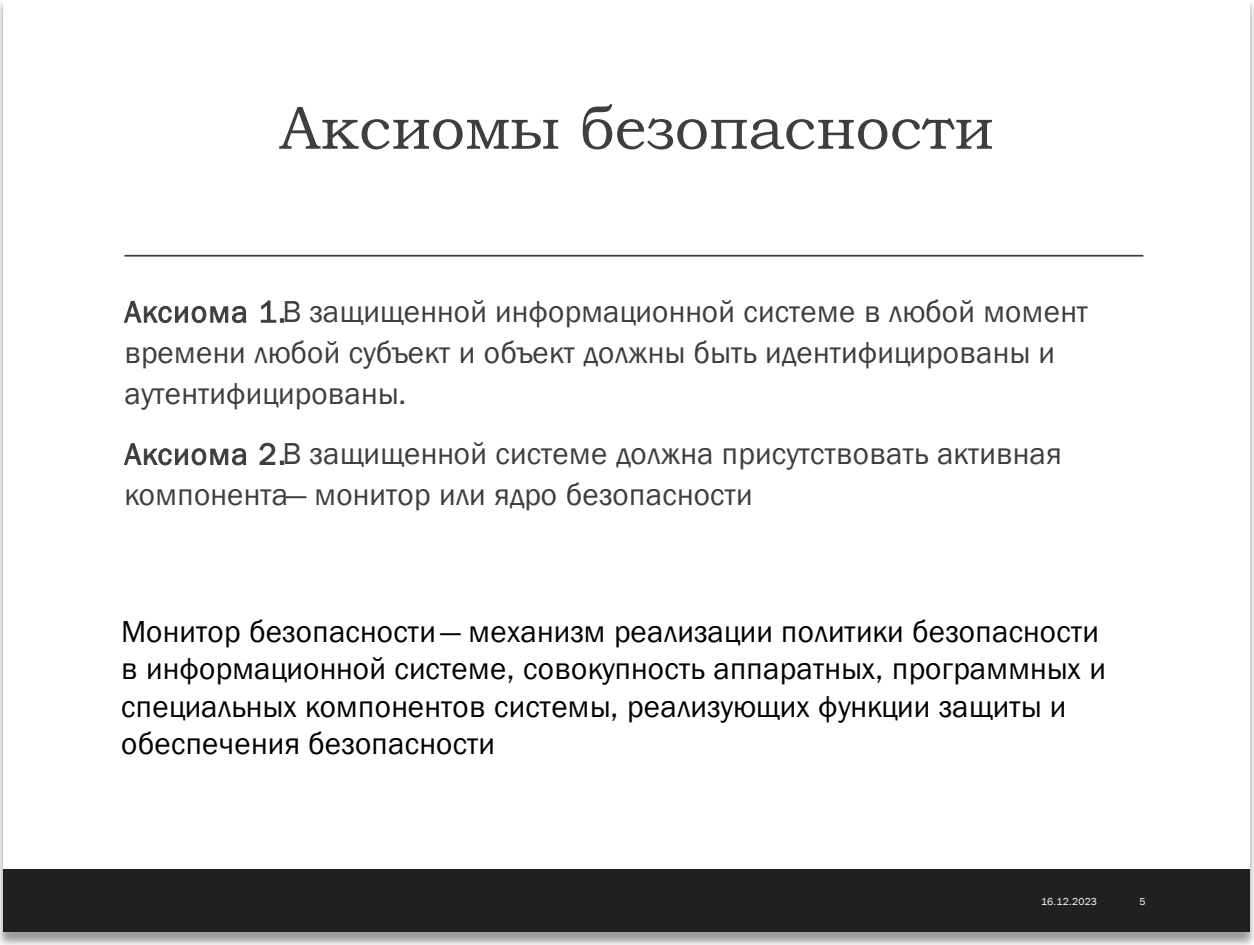
Потребители путем составления формальных моделей безопасности получают возможность довести до сведения производителей свои требования, а также оценить соответствие защищенных систем своим потребностям.

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.

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. 7.1).

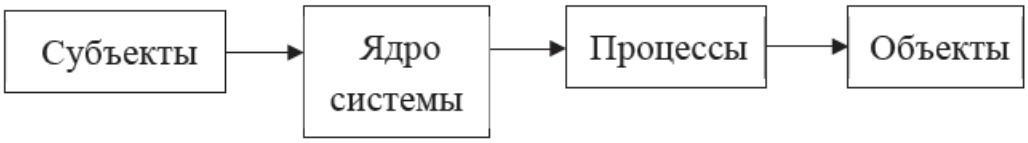


Рис. 7.1. Незащищенная система

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).

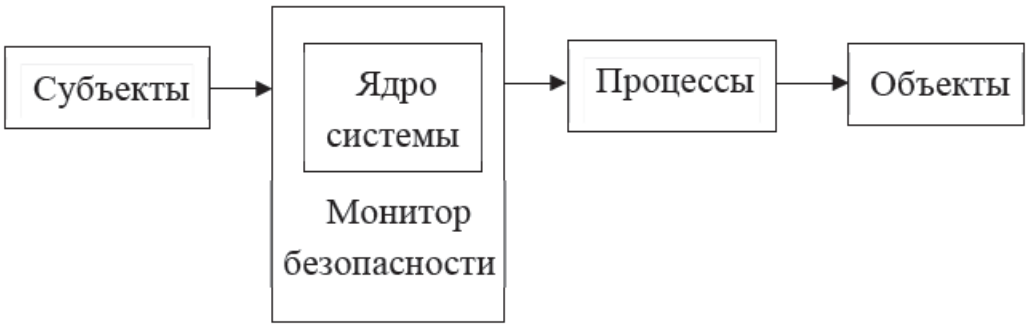
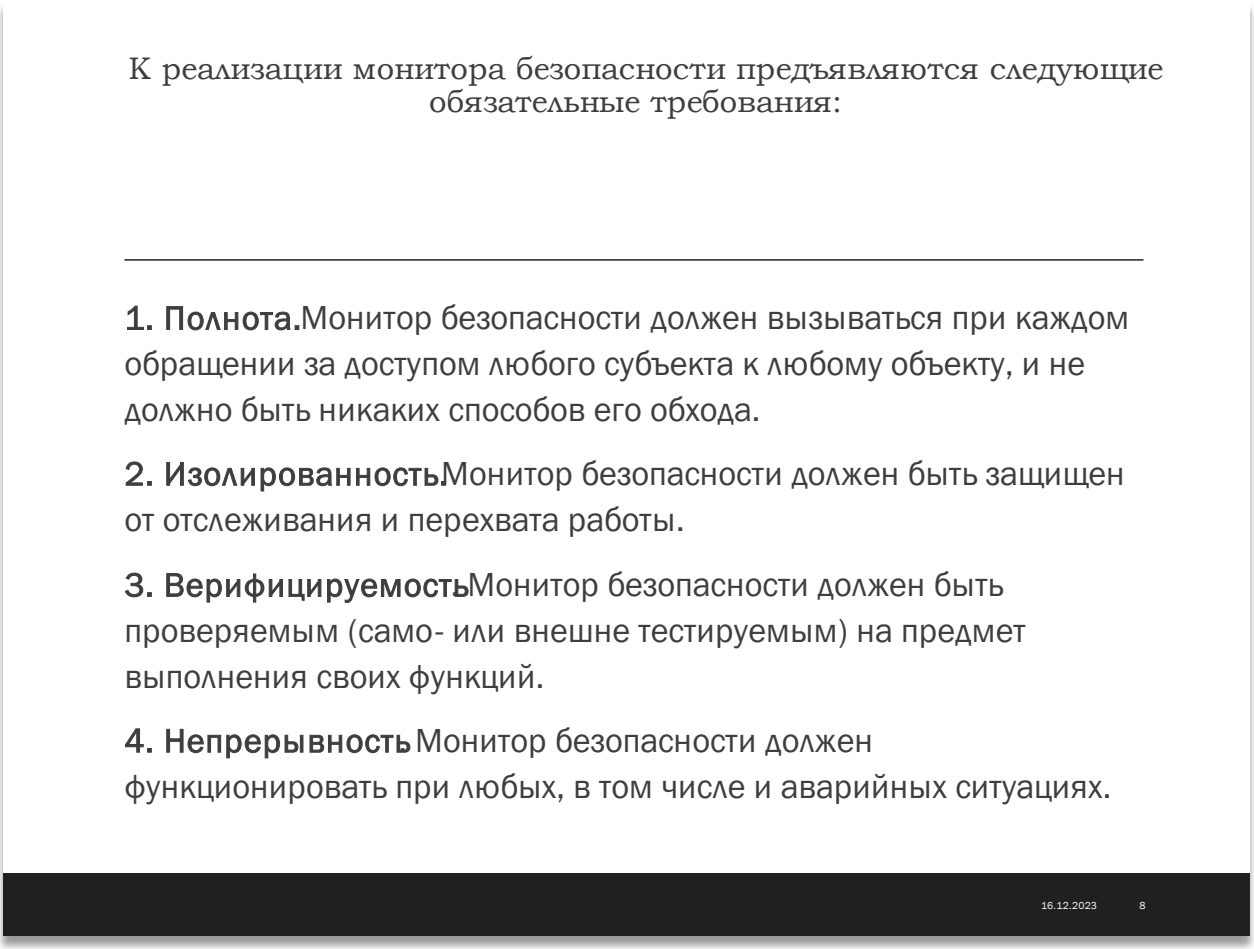


Рис. 7.2. Защищенная система

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



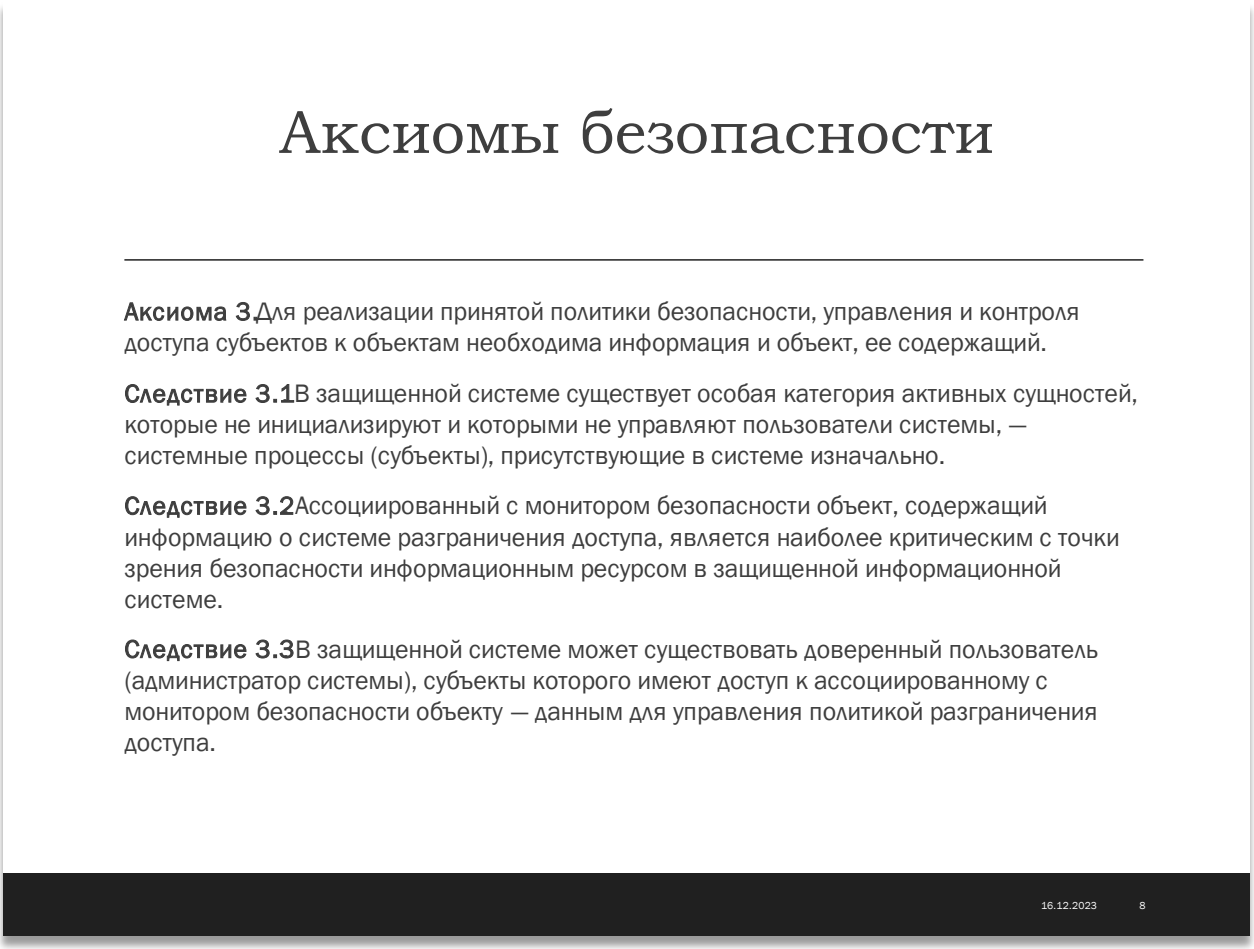
1. Полнота. Монитор безопасности должен вызываться при каждом обращении за доступом любого субъекта к любому объекту, и не должно быть никаких способов его обхода.

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

3. Верифицируемость. Монитор безопасности должен быть проверяемым (само- или внешне тестируемым) 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.

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

В матрице используются следующие обозначения:

w — «писать», r — «читать», e — «исполнять».

Матрица доступа

	Файл 1	Файл 2	Файл 3
User 1	R	RW	
User 2	R	RW	
User 3	RW	RW	RW

16.12.2023 11

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

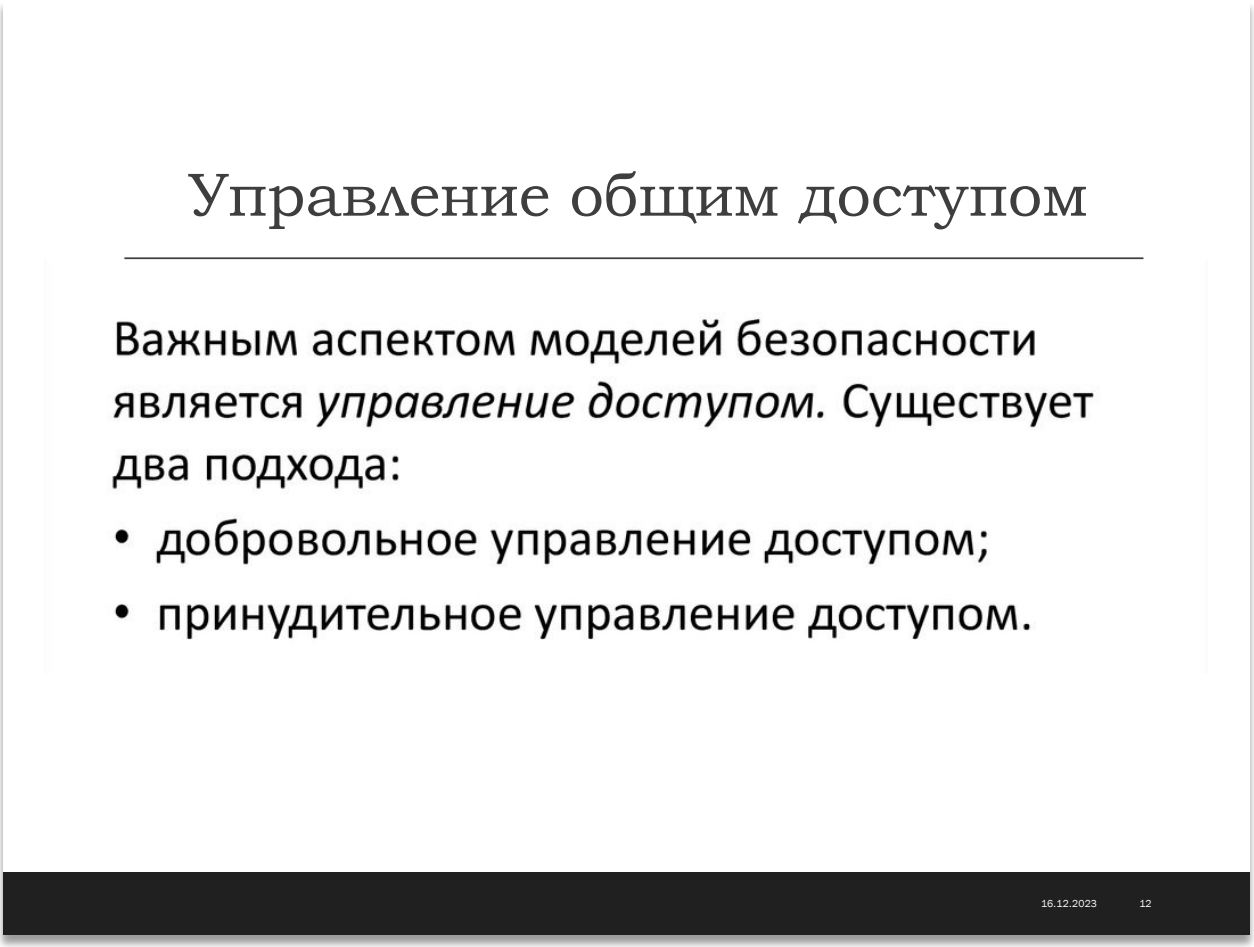
представляются права пользователей только к объектам второй группы. Наиболее известным примером такого подхода являются «биты доступа» в UNIX-системах.

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.

Парольные системы разграничения доступа

1. Система представляется следующим набором сущностей:
- множеством информационных объектов (документов) O(o1, ..., om);
- множеством пользователей S(s1, ...,sn);
- множеством паролей доступа к объектам K(k1, ...,kp).

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

fko: O → K.

Значением функции fko(o) = ko является пароль ko 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:

fks: S → K.

Значением fks(s) = Ks 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.

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 о пользователь s предъявляет (вводит, передает) монитору безопасности АС пароль k_{s0} 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 о.

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. 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.

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

— СКРЫТЫЙ КАНАЛ УТЕЧКИ

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.

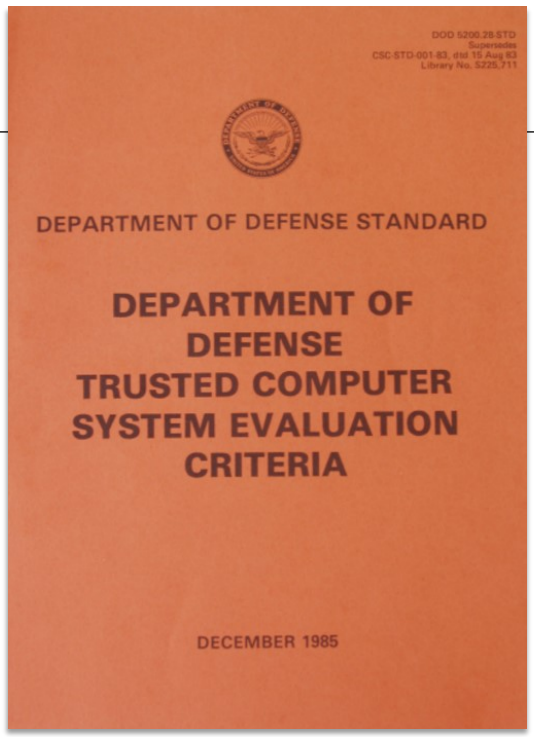
От высокоуровневых субъектов может передаваться информация о количестве создаваемых или удаляемых секретных файлов, получить доступ по чтению к которым низкоуровневые субъекты не могут, но «видеть» их наличие и соответственно определять их количество могут.

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).

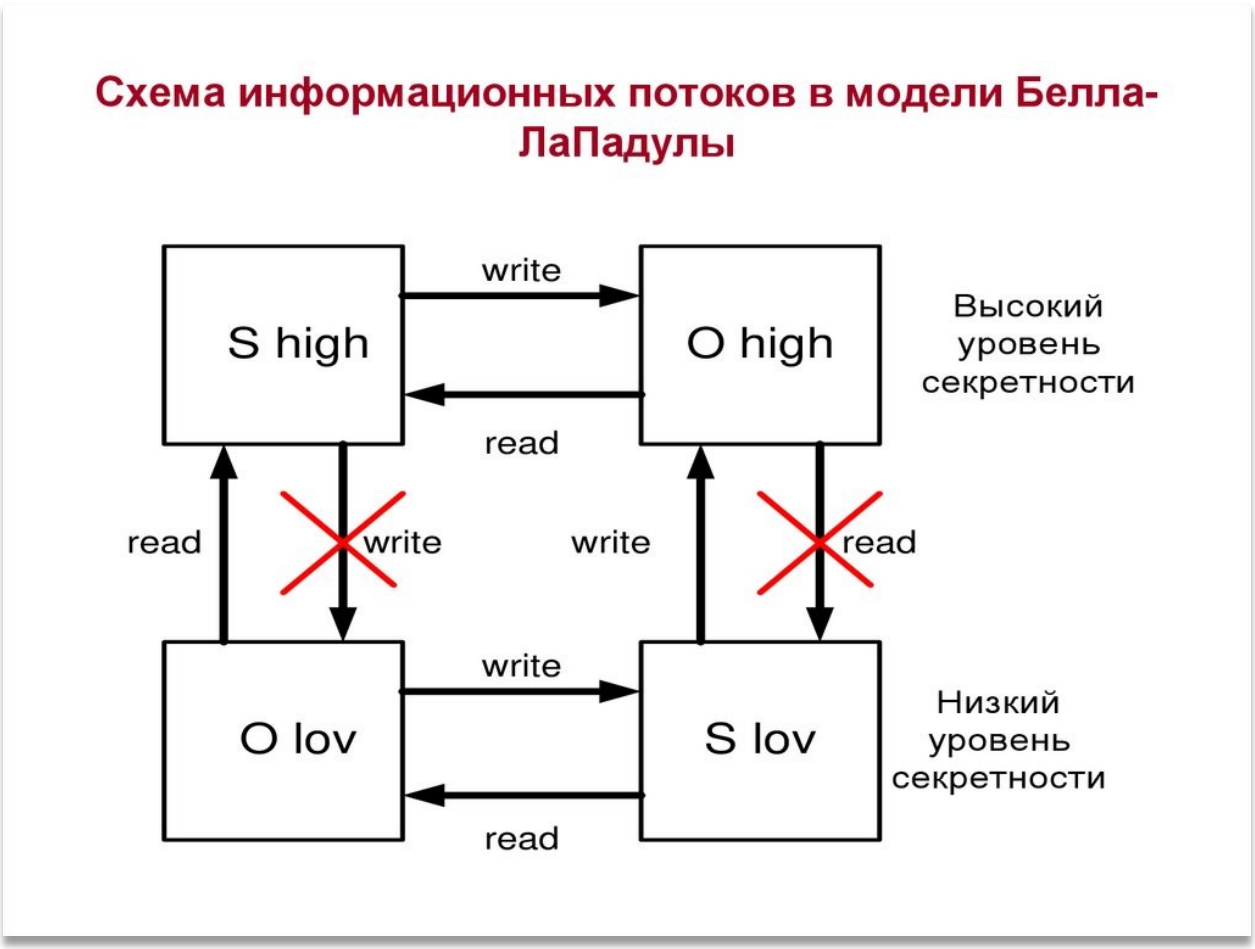
Оранжевая книга



16.12.2023 16

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 информационной 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.

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.