

Модели управления доступом в распределенных информационных системах

01, январь 2011

авторы: Медведев Н. В., Гришин Г. А.

УДК 598.87

Введение

Широкое внедрение распределенных информационных систем в жизнь современного общества привело к необходимости решения ряда проблем защиты информации от несанкционированного доступа (НСД). Основным механизмом защиты от НСД является реализация одной из существующих моделей доступа. Однако, данные модели были разработаны в конце 70-х годов и не учитывают всех особенностей крупных территориально-распределенных информационных систем.

В настоящей статье будет проведен анализ существующих моделей доступа (мандатная, дискреционная, ролевая), рассмотрены особенности применения каждой из них, выбрана наиболее подходящая для распределенных информационных систем, а также предложены основные подходы к ее совершенствованию для устранения недостатков и трудностей практической реализации.

1. Политика безопасности

Под понятием политики безопасности понимается совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое, а иногда и достаточное, условие безопасности системы.

В соответствии с существующими подходами принято считать, что информационная безопасность ИС обеспечена в случае, если для любых информационных ресурсов в системе поддерживается определенный уровень:

1. конфиденциальности (невозможности несанкционированного получения информации);
2. целостности (невозможности несанкционированной ее модификации);
3. доступности (возможности за разумное время получить требуемую информацию).

В руководящих документах Гостехкомиссии при Президенте Российской Федерации, опубликованных в 1992 Г. и посвященных вопросам защиты информации в автоматизированных системах ее обработки, указывается на то, что основная задача политики безопасности - это обеспечение защиты от несанкционированного доступа (НСД) к информации. Именно в результате несанкционированного доступа к ресурсам КС реализуются угрозы безопасности, преднамеренно планируемые злоумышленником.

Для строгого и однозначного толкования норм и правил политики безопасности обычно дается ее формализованное описание в виде соответствующей модели.

Основная цель такого описания - 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.

На практике это означает, что только соответствующим образом уполномоченные пользователи получают доступ к информации и смогут осуществить с ней только санкционированные действия.

Все существующие в настоящее время модели безопасности основаны на следующих базовых представлениях:

1. Компьютерная система является совокупностью взаимодействующих сущностей - субъектов и объектов.

Объекты можно представлять в виде контейнеров, содержащих информацию, а субъектами считать выполняющиеся программы, которые воздействуют на объекты различными способами. При таком представлении безопасность обработки информации обеспечивается путем решения задачи управления доступом субъектов к объектам в соответствии с тем набором правил и ограничений, которые образуют политику безопасности. Считается, что система безопасна, если субъекты не имеют возможности нарушить правила политики безопасности. Таким образом, общим подходом для всех моделей является именно разделение множества сущностей, образующих систему, на множества субъектов и объектов.

2. Все взаимодействия в системе моделируются установлением отношений определенного типа между субъектами и объектами. Множество типов таких отношений определяется в виде набора операций, которые субъекты могут производить над объектами.
3. Все операции между субъектами и объектами, контролируемые монитором взаимодействий, либо запрещаются, либо разрешаются в соответствии с правилами политики безопасности.
4. Политика безопасности задается в виде правил, определяющих взаимодействия между субъектами и объектами. Взаимодействия, приводящие к нарушению этих правил, пресекаются средствами контроля доступа и не могут быть осуществлены.
5. Совокупность множеств субъектов, объектов и отношений между ними (установившихся взаимодействий) определяет состояние системы. В этом пространстве состояний каждое состояние системы является либо безопасным, либо небезопасным в соответствии с принятым в модели критерием безопасности.

6. Основной элемент модели безопасности - это доказательство того, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние при соблюдении всех установленных правил и ограничений.

Среди моделей политики безопасности можно выделить два основных типа:

1. дискреционные (произвольные);
2. мандатные (нормативные).

В основе этих моделей лежат, соответственно, дискреционное управление доступом (Discretionary Access Control - DAC) и мандатное управление доступом (Mandatory Access Control - MAC).

В качестве классических примеров моделей этих типов можно назвать дискреционную модель Хааррисона-Руззо-Ульмана (модель HRU) и мандатную модель Белла-Лападула (модель БЛ).

Однако существует также и ролевая модель, которая очень близка к дискреционной, но при этом содержит признаки мандатной модели доступа.

В информационных системах, особенно правительственных, в которых хранится и обрабатывается критичная информация, политика безопасности основывается на мандатной (или многоуровневой) политике безопасности (МПБ). Многоуровневая политика безопасности принята всеми развитыми государствами мира. В повседневном, секретном делопроизводстве у нас в стране принята эта же политика. В конце 70-х годов, когда были разработаны первые модели многоуровневого управления доступом в информационных системах, разработчики систем защиты информации пришли к выводу, что для больших, сложных систем именно подобного рода модели больше подходят для применения на практике.

Дискреционная модель обеспечивает произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа. В рамках этой модели система обработки информации

представляется в виде совокупности активных сущностей – субъектов, которые осуществляют доступ к информации, пассивных сущностей – объектов, содержащих защищаемую информацию и конечного множества прав доступа, означающих полномочия на выполнение соответствующих действий. Принято считать, что все субъекты одновременно являются и объектами. Поведение системы характеризуется текущим состоянием, текущее состояние характеризуется тройкой множеств: субъектов, объектов и матрицы прав доступа, описывающей текущие права доступа субъектов к объектам.

Ролевая модель представляет собой существенно усовершенствованную дискреционную модель, однако её нельзя отнести ни к дискреционным, ни к мандатным моделям, 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. В ролевой модели классическое понятие субъект замещается понятиями пользователь и роль.

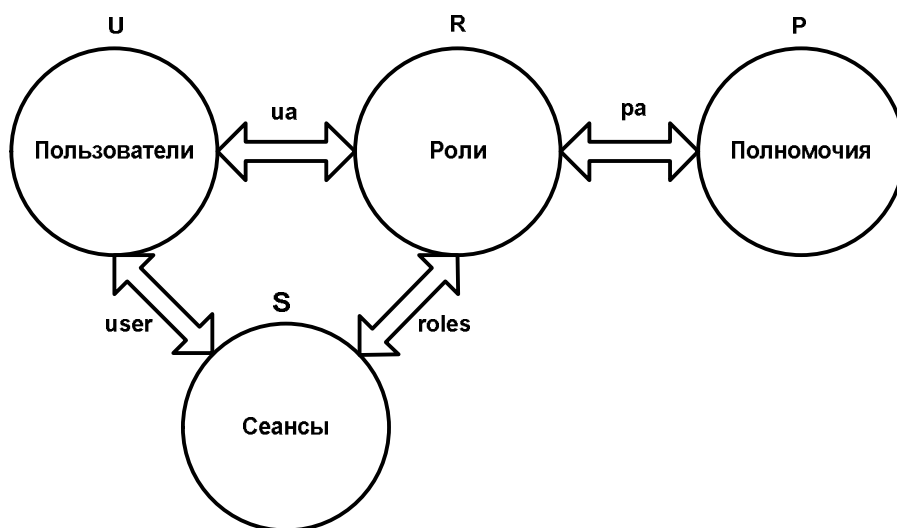


Рис.1 Схематическое представление объектов и субъектов доступа в ролевой модели управления

Суть мандатного принципа контроля доступа состоит в сопоставлении каждому субъекту (пользователю) и объекту системы

классификационных меток, которые можно условно считать уровнями секретности, кроме того, внутри каждого уровня секретности содержатся категории (их можно понимать как отделы или подразделения) [1].

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила — читать можно только то, что положено.

Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может писать в секретные файлы, но не может — в несекретные (разумеется, должны также выполняться ограничения на набор категорий). На первый взгляд подобное ограничение может показаться странным, однако оно вполне разумно. Ни при каких операциях уровень секретности информации не должен понижаться, хотя обратный процесс вполне возможен. Посторонний человек может случайно узнать секретные сведения и сообщить их куда следует, однако лицо, допущенное к работе с секретными документами, не имеет права раскрывать их содержание простому смертному.

В основном данный механизм направлен на защиту от ошибок пользователей, которые могут непреднамеренно разгласить конфиденциальные данные. Кроме того, при использовании описанной схемы разграничения прав доступа, после того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа, что позволяет проведение более жесткой и четкой сформулированной политики безопасности [2].

Мандатная политика безопасности устойчива к атакам «Троянским конем». На чем строится защита от таких атак поясним на примере.

Пример : Пусть пользователи U_1 и U_2 находятся на разных уровнях, то есть $c(U_1) > c(U_2)$. Тогда, если U_1 может поместить в объект O_1 ценную информацию, то он может писать туда и $c(U_2) < c(U_1) \leq c(O_1)$, то есть $c(U_2) < c(U_1)$. Тогда любой «Троянский конь» T , содержащийся в объекте O_2 , который может считать информацию в O_1 , должен отражать соотношение

$$c(O_2) \geq c(O_1)$$

Тогда $c(O_2) > c(U_2)$ и пользователь U_2 не имеет право прочитать в O_2 , что делает съем в O_1 и запись в O_2 бессмысленным.

2. Модель Белла-Лападула

В современных системах защиты модель политики безопасности реализуется через мандатный контроль доступа. Мандатный контроль доступа еще называют обязательным, так как его проходит каждое обращение субъекта к объекту, если субъект и объект находятся под защитой системы безопасности.

Цель модели политики безопасности в сохранении секретности информации. Вопросы целостности при помощи этой политики не решаются или решаются как побочный результат защиты секретности. Вместе с тем, они могут быть противоречивы.

Модель Белла-Лападула - это одна из первых моделей политики безопасности и впоследствии наиболее часто используемая. Она была разработана для обоснования безопасности систем, использующих многоуровневую политику безопасности.

Классическая модель Белла-Лападула построена для анализа систем защиты, реализующих мандатное разграничение доступа. Возможность ее использования в качестве формальной модели таких систем непосредственно отмечена в критерии TCSEC («Оранжевая книга»). Модель Белла-Лападула была предложена в 1975 году.

Материалы, в которых опубликована модель в 1976г., до сих пор недоступны, и поэтому в качестве самого близкого к оригиналу источника

была принята работа Джона МакЛина (J. McLean), опубликованная в 1987 году.

Идеи, лежащие в основе модели Белла-Лападула берут происхождение из «бумажного мира». Белл и Лападула перенесли модель безопасности, принятую при работе с документами, в мир компьютерных систем. Основным наблюдением, сделанным Беллом и Лападулом, является то, что в правительстве США все субъекты и объекты ассоциируются с уровнями секретности, варьирующимися от низких уровней (неклассифицированных), до высоких (совершенно секретных).

Кроме того, они обнаружили, что для предотвращения утечки информации к неуполномоченным субъектам этим субъектам с низкими уровнями секретности не позволяется читать информацию из объектов с высокими уровнями секретности. Это ведет к первому правилу модели Белла-Лападула.

Первое правило модели Белла-Лападула:

Простое свойство безопасности, также известное как правило «нет чтения вверх» (No Read Up, NRU) или как свойство простой безопасности (ss-свойство), гласит, что субъект с уровнем секретности X_s , может читать информацию из объекта с уровнем секретности X_o , только если X_s преобладает над X_o .

Это означает, что если в системе, удовлетворяющей правилам модели Белла-Лападула, субъект с уровнем доступа «Секретный» попытается прочесть информацию из объекта, классифицированного как «Совершенно секретный», то такой доступ будет запрещен.

Белл и Лападул сделали дополнительное наблюдение при построении своей модели: в правительстве США субъектам не позволяется размещать информацию или записывать ее в объекты, имеющие более низкий уровень секретности.

Например: когда «Совершенно секретный» документ помещается в «Неклассифицированное» мусорное ведро.

В таком случае может произойти утечка информации. Это ведет ко второму правилу модели Белла-Лападула.

Второе правило модели Белла-Лападула:

Свойство, известное как правило «нет записи вниз» (No Write Down, NWD) или как свойство ограничения, гласит, что субъект с уровнем секретности X_s может писать информацию в объект с уровнем секретности X_o , только если X_o преобладает над X_s .

Это означает, что если в системе, удовлетворяющей правилам модели Белла-Лападула, субъект с уровнем доступа «Совершенно секретно» попытается записать информацию в «Неклассифицированный» объект, то такой доступ не будет разрешен. Введение свойства «нет записи вниз» разрешает проблему троянских коней, так как запись информации на более низкий уровень секретности, типичная для троянских коней, запрещена.

Правила запрета по записи и чтению отвечают интуитивным представлениям о том, как предотвратить утечку информации к неуполномоченным источникам. На рис.2 показаны потоки информации в модели Белла-Лападула.

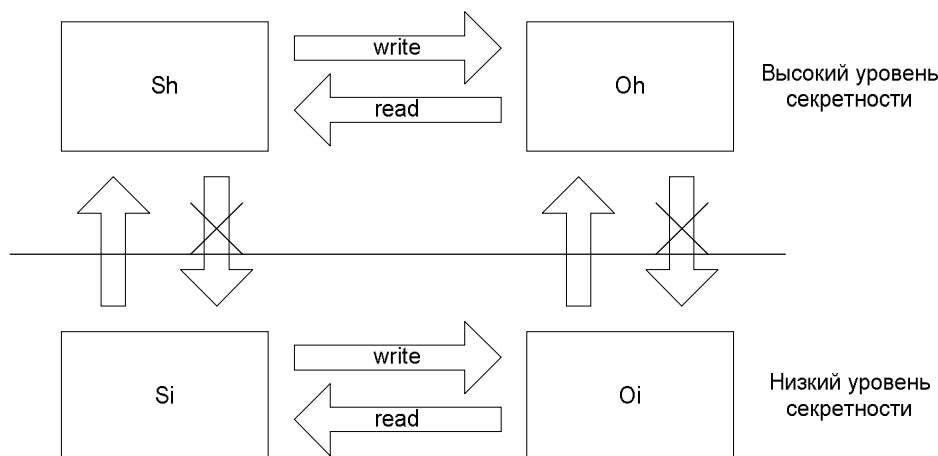


Рис. 2. Диаграмма потоков данных для модели Белла-Лападула

Т.о. основой многоуровневой политики является решетка ценностей.

Пусть между двумя произвольными объектами X и Y имеется информационный поток от X к Y , где X -источник, Y - получатель информа-

ции. Если $(Y) > (X)$, то это означает, что Y - более ценный объект, чем X . Политика мандатная политика безопасности (далее по тексту МПБ) считает информационный поток от X к Y разрешенным тогда и только тогда, когда $(Y) > (X)$, т.е. Y секретнее, чем X .

Тогда правила модели Белла-Лападула можно представить в виде:
свойство простой безопасности (ss-свойство):

$$X \xrightarrow{r} Y \Leftrightarrow c(X) \geq c(Y),$$

свойство ограничения:

$$X \xrightarrow{w} Y \Leftrightarrow c(X) \leq c(Y).$$

Таким образом, МПБ имеет дело с множеством информационных потоков в системе и делит их на разрешенные и неразрешенные очень простым условием. Однако эта простота касается информационных потоков, которых в системе огромное количество.

Управление доступом в модели Белла-Лападула происходит с использованием матрицы управления доступом или меток безопасности во взаимосвязи с правилами простой безопасности и свойства ограничения.

В дополнение к имеющимся режимам доступа чтения и записи модель включает режимы добавления, исполнения и управления - причем последний определяет, может ли субъект передавать другим субъектам права доступа, которыми он обладает по отношению к объекту. Управление при помощи меток безопасности усиливает ограничение предоставляемого доступа на основе сравнения атрибутов класса доступа субъектов и объектов.

Пример:

Пусть определены конечные множества S , O , R , L .

S - множество субъектов системы;

O - множество объектов, не являющихся субъектами;

R - множество прав доступа, $R = \{read(r), write(w), execute(e), append(a)\}$;

L - уровни секретности.

Множество V состояний системы определяется произведением множеств:

$$V = B \times M \times F \times H,$$

где сомножители определяются следующим образом. B - множество текущих доступов и есть подмножество множества подмножеств произведения $S \times O \times R$. Множество подмножеств будем обозначать $P(S \times O \times R)$ элементы множества B будем обозначать b и они представляют в текущий момент t графы текущего доступа (в каждый момент субъект может иметь только один вид доступа к данному объекту).

M - матрица разрешенных доступов, $M = \| M_{ij} \|$, $M_{ij} \subseteq R$.

F - подмножество множества $L^S \times L^S \times L^O$, где каждый $\dot{f} = (f_s, f_o, f_c)$, $\dot{f} \in F$, - вектор, который состоит из трех компонент, каждая из которых тоже вектор (или отображение).

f_s - уровень допуска субъектов (это некоторое отображение $f_s: S \rightarrow L$);

f_o - уровень секретности объектов (это некоторое отображение $f_o: O \rightarrow L$);

f_c - текущий уровень секретности субъектов (это тоже некоторое отображение $f_c: S \rightarrow L$).

Элементы подмножества F , которые допущены для определения состояния должны удовлетворять соотношению:

$$\forall S \in S \quad f_s(S) \geq f_c(S).$$

H - текущий уровень иерархии объектов, в работе McLean этот уровень не изменяется, совпадает с f_o и далее не рассматривается.

Элементы множества V состояний будут обозначаться через v . Пусть определены множество Q - запросов в систему и множество D - решений по поводу этих запросов ($D = \{yes, no, error\}$). Определим множество W действий системы как

$$W \subseteq Q \times D \times V \times V = \{ (q, d, v_1, v_2) \}.$$

Каждое действие системы (q, d, v_1, v_2) имеет следующий смысл: если система находилась в данный момент в состоянии v_1 , поступил запрос q , то принято решение d и система перешла в состояние v_2 .

Пусть T - множество значений времени (для удобства будем считать, что $T = N$ - множество натуральных чисел). Определим набор из трех функций (x, y, z) :

$$x: T \rightarrow Q,$$

$$y: T \rightarrow D,$$

$$z: T \rightarrow V,$$

и обозначим множества таких функций X, Y, Z соответственно.

Рассмотрим $X \times Y \times Z$ и определим понятие системы в модели Б-Л.

Определение. Системой $\Sigma(Q, D, W, z_0)$ называется подмножество $X \times Y \times Z$ такое, что

$$(x, y, z) \in \Sigma(Q, D, W, z_0) \Leftrightarrow (x_t, y_t, z_t, z_{t-1}) \in W,$$

для каждого значения $t \in T$, где z_0 - начальное состояние системы.

Определение. Каждый набор $(x, y, z) \in \Sigma(Q, D, W, z_0)$ называется реализацией системы.

Определение. Если (x, y, z) - реализация системы, то каждая четверка (x_t, y_t, z_t, z_{t-1}) называется действием системы.

Нетрудно видеть, что при отсутствии ограничений на запросы таким образом определен некоторый автомат, у которого входной алфавит Q , а выходной D , а множество внутренних состояний V . Автомат задается множеством своих реализаций. Перейдем к определению понятий, связанных с безопасностью системы.

Определение. Тройка $(S, O, X) \in S \times O \times R$ удовлетворяет свойству простой секретности (ss - свойство) относительно $\dot{f}$, если $X = execute$, или $X = append$, или, если $X = read \text{ и } f_S(S) \geq f_O(O)$, или $X = write \text{ и } f_S(S) \geq f_O(O)$.

Определение. Состояние $v = (b, M, \dot{f}, h)$ обладает ss - свойством, если для каждого элемента $(S, O, X) \in b$ этот элемент обладает ss - свойством относительно $\dot{f}$.

Определение. Состояние $v = (b, M, \dot{f}, h)$ обладает *- свойством, если для каждого $(S, O, X) \in b$ при $X = write$ текущий уровень субъекта $f_c(S)$ равен уровню объекта $f_o(O)$, или при $X = read$ $f_c(S) \geq f_o(O)$, или при $X = append$ $f_o(O) \geq f_c(S)$.

Определение. Состояние обладает *- свойством относительно множества субъектов S' , $S' \subset S$, если оно выполняется для всех троек (S, O, X) таких, что $S \in S'$.

Определение. Субъекты из множества $S \setminus S'$ называются доверенными.

Лемма. Из *- свойства для (S, O, X) следует ss - свойство относительно $\dot{f}$.

Доказательство. Утверждение следует из условия $f_c(S) \leq f_s(S)$.

Определение. Состояние $v = (b, M, \dot{f}, h)$ обладает ds - свойством, если $\forall (S, O, X) \in b \Rightarrow X \in m_{so}$, где $M = //m_{so} //$ - матрица доступа состояния v .

Определение. Состояние $v = (b, M, \dot{f}, h)$ называется безопасным, если оно обладает одновременно ss - свойством, *- свойством относительно S' и ds - свойством.

Напомним формулировку политики МПБ, связанной с решеткой ценностей $SC \times L$ в информации: информационный поток между двумя объектами называется разрешенным, если класс объекта источника доминируется классом объекта получателя. Из определения ss - свойства следует, что в безопасном состоянии возможно чтение вниз, что согласуется с эквивалентным определением MLS политики. Кроме того, ss - свойство определяет ограничение на возможность модификации, которое связано с W :

$$f_s(S) \geq f_o(O)$$

Объясним *- свойство. Если субъект может понизить свой текущий допуск до $f_C(S) = f_O(O)$, то, согласно *- свойству, он может писать в объект. При этом он не может читать объекты на более высоких уровнях, хотя допуск $f_S(S)$ ему это может позволить. Тем самым исключается возможный канал утечки.

Таким образом, при записи информационный поток опять не может быть направлен вниз. Исключение возможно только для доверенных субъектов, которым разрешено строить информационный поток вниз. При этом доверенность субъекта означает безопасность такого потока вниз (поэтому эти потоки считаются разрешенными). Сказанное выше означает, что безопасное состояние модели Б-Л поддерживает политику МПБ. Значит, для того, чтобы доказать, что любой поток на траектории вычислительной системы разрешен, достаточно показать, что выходя из безопасного состояния и следуя допустимым действиям мы опять приходим в безопасное состояние, тем самым любая реализация процесса будет безопасной.

3. Реализация модели Белла-Лападула в распределенных информационных системах

Несмотря на все достоинства, оказалось, что при использовании модели Белла-Лападула в контексте практического проектирования и разработки реальных компьютерных систем возникает ряд технических вопросов, что является логическим следствием достоинства модели Белла-Лападула - ее простоты. Проблемы появляются при рассмотрении вопросов построения политик безопасности для конкретных типов систем, т. е. на менее абстрактном уровне. Здесь системный компонент модели усложняется, что может привести к неадекватности модели Белла-Лападула в ее классической форме. Как следствие в мире компьютерной безопасности ведется широкая полемика по поводу применимости модели Белла-Лападула для построения безопасных систем.

В свете недавних тенденций использования распределенных конфигураций требуется рассматривать модели безопасности не только для автономных, но и для распределенных компьютерных систем. Очевидным способом распространения модели Белла-Лападула на распределенные системы будет назначение уровней секретности различным компонентам этих систем и соблюдение гарантии выполнения правил-ограничений по чтению и записи.

Например, некоторым компонентам можно назначить уровни секретности, меняющиеся от неклассифицированного до совершенно секретного уровня, и на основании принципов модели Белла-Лападула синтезировать соединения между различными компонентами системы.

Может показаться, что если конфиденциальному субъекту A будет разрешено чтение информации из неклассифицированного объекта B , никакая конфиденциальная информация не будет раскрыта.

Но при более подробном рассмотрении реализации операции удаленного чтения снизу может быть сделано неприятное наблюдение. Операция чтения между удаленными компонентами приводит к протеканию потока информации от читаемого объекта к запросившему доступ на чтение субъекту. Данный поток является безопасным, поскольку информация не разглашается неавторизованному субъекту. Однако в распределенной конфигурации чтение инициируется запросом от одного компонента к другому. Такой запрос образует прохождение потока информации в неверном направлении (запись в объект с меньшим уровнем секретности).

Таким образом, удаленное чтение в распределенных системах может произойти, только если ему предшествует операция записи вниз, что является нарушением правил модели Белла-Лападула.

Многие исследователи рассматривают эту проблему как наиболее убедительное свидетельство неадекватности модели Белла-Лападула. Однако на практике эта проблема часто является несущественной. Достаточно внедрения в систему дополнительных средств обработки удаленных за-
<http://technomag.edu.ru/doc/164245.html>

просов для обеспечения того, чтобы поток информации от высокоуровневого субъекта к низкоуровневому объекту был ограничен запросом на доступ. Фактически некоторые архитектуры предлагают отдельные компоненты, выполняющие обработку таких запросов и потока информации в распределенных системах.

В описании правил модели Белла-Лападула не было указано, какие субъекты должны подчиняться этим правилам.

Например, компьютерные системы обычно имеют администратора, который управляет системой, добавляя и удаляя пользователей, восстанавливает функционирование после сбоев, устанавливает специальное программное обеспечение, устраняет ошибки в операционной системе или приложениях и т. п.

Очевидно, что процессы, действующие в интересах таких администраторов, не могут управляться правилами модели Белла и Лападула или каких-либо других моделей, не позволяющих им выполнять функции администрирования.

Это наблюдение показывает еще одну техническую проблему, связанную с правилами модели Белла-Лападула. Можно сказать, что эти правила обеспечивают средства для предотвращения угрозы нарушения секретности для нормальных пользователей, но не говорят ничего по поводу той же проблемы для так называемых доверенных субъектов. Доверенные субъекты могут функционировать в интересах администратора. Также они могут быть процессами, обеспечивающими критические службы, такие как драйвер устройства или подсистема управления памятью. Такие процессы часто не могут выполнить свою задачу, не нарушая правил модели Белла-Лападула. Неприменимость модели Белла-Лападула для доверенных субъектов может быть выражена путем внесения поправки в данное ранее определение операций чтения и записи модели Белла-Лападула. Но хотя это и делает определение более точным, оно несколько не облегчает задачу

для разработчика, желающего построить безопасный драйвер или утилиту поддержки работы администратора.

Одним из решений, рассматриваемых в литературе по безопасности, было предложение представлять и использовать для потока информации модель, требующую того, чтобы никакая высокоуровневая информация никогда не протекала на более низкий уровень.

Джон МакЛин разработал концептуальное описание системы, названной Система Z.

Данное описание показывает, что система, удовлетворяющая правилам модели Белла-Лападула, может иметь ряд проблем с секретностью. Система Z выражается в терминах набора субъектов и объектов, с каждым из которых связан уровень секретности. Совокупность уровней секретности для каждого субъекта и объекта в некоторый момент времени описывает состояние системы. Система Z удовлетворяет модели Белла-Лападула, если во всех состояниях системы комбинации уровней субъектов и объектов таковы, что в этом состоянии никакой субъект не может осуществить запись вниз или чтение сверху.

Предположив, что система Z удовлетворяет условиям модели Белла-Лападула, можно быть уверенным, что любая угроза секретности будет обнаружена. Однако МакЛин указал на техническую деталь, которая не очевидна в таких системах. Если в некотором состоянии секретный субъект захотел прочитать совершенно секретный объект, то до тех пор, пока система удовлетворяет модели Белла-Лападула, осуществить это будет невозможно, но ничто в модели Белла-Лападула не предотвращает систему от «деклассификации» объекта от совершенно секретного до секретного (по желанию совершенно секретного пользователя).

В качестве иллюстрации можно привести следующий пример. Допустим, субъект с высокой степенью доверия A читает информацию из объекта, уровень классификации которого также равен A . Далее данный

субъект понижает свою степень доверия до уровня B ($A > B$). После этого он может записать информацию в файл с классификацией B .

Нарушения правил модели Белла и Лападула формально не произошло, но безопасность системы нарушена.

Фактически МакЛин описал конфигурацию, в которой все субъекты могут читать и записывать любой объект путем назначения соответствующих уровней секретности объекта перед выполнением запросов на доступ. В такой системе, которая, очевидно, не обеспечивает секретность информации, все состояния могут быть рассмотрены как удовлетворяющие требованиям модели Белла-Лападула.

Все описанное выше является справедливым для модели Белла-Лападула в ее классической формулировке, кочующей из книги в книгу и из статьи в статью. Но в оригинальной модели, представленной авторами, было введено требование сильного и слабого спокойствия. Данные требования снимают проблему Z -системы.

Правило сильного спокойствия гласит, что уровни секретности субъектов и объектов никогда не меняются в ходе системной операции. Реализовав это правило в конкретной системе, можно сделать заключение, что описанные выше проблемы никогда не возникнут. Очевидным недостатком такой реализации в системе является потеря гибкости при выполнении операций.

Правило слабого спокойствия гласит, что уровни секретности субъектов и объектов никогда не меняются в ходе системной операции таким образом, чтобы нарушить заданную политику безопасности. Это правило может потребовать, чтобы субъекты и объекты воздерживались от действий в период времени, когда меняются их уровни секретности.

Например, может потребоваться, чтобы уровень секретности объекта никогда не менялся в то время, когда к нему обращается некоторый субъект.

Однако если операция чередуется с изменением уровня безопасности, не вызывающего нарушения безопасности, то правило слабого спокойствия будет по-прежнему соблюдено.

Например, субъект повышает свой уровень с секретного до совершенно секретного в ходе выполнения операции чтения неклассифицированного объекта.

Фактически система Z описывает алгебру моделей, самой строгой из которых (основание) является модель Белла-Лападула с сильным спокойствием (ни один субъект модели не может изменить свою классификацию), а самой слабой (вершина) модель Белла-Лападула в классической формулировке без ограничений для субъектов и объектов на изменение классификации.

Заключение

В данной статье была рассмотрена классическая модель мандатного доступа, выявлены ее недостатки при реализации в распределенных информационных системах и предложены подходы к ее совершенствованию с использованием правил спокойствия.

Список использованных источников

1. Мельников В. П., Клейменов С.А. Информационная безопасность и защита информации. – М.: Издательский центр «Академия», 2008.– 336 с.
2. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000. - 452 с.