ФГБОУ ВПО «Воронежский государственный
технический университет»

Кафедра систем информационной безопасности

335-2014

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к практическим занятиям № 5–6 по дисциплине
«Управление информационной безопасностью»
для студентов специальности
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Воронеж 2014

Составитель д-р техн. наук К. А. Разинкин

УДК 004.056.5

Методические указания к практическим занятиям № 5–6 по дисциплине «Управление информационной безопасностью» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения» / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. К. А. Разинкин. – Воронеж, 2014. 50 с.

Методические указания нацелены на привитие практических навыков управления информационной безопасностью на основе моделей дискреционного, мандатного и ролевого управления доступом, безопасности информационных потоков. В указаниях приведены основные теоретические положения и примеры решения типовых задач.

Методические указания подготовлены в электронном виде в текстовом редакторе и содержатся в файле Разинкин_ПЗ_УИБ_№5-6.pdf.

Табл. 1. Ил. 5. Библиогр.: 13 назв.

Рецензент д-р техн. наук, проф. А. Г. Остапенко

Ответственный за выпуск зав. кафедрой д-р техн. наук, проф. А. Г. Остапенко

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

ВВЕДЕНИЕ

Управление информационной безопасностью (ИБ) – неотъемлемая часть управления любой современной организацией в целом, независимо от ее размера и сферы деятельности.

Управление ИБ - сложный непрерывный процесс, перед которым стоит множество целей и задач, являющихся обеспечивающими, вспомогательными по отношению к основным бизнес-целям и задачам организации. Они формулируются в различных документах организации: концепциях, стратегиях, политиках, стандартах, инструкциях и т. д.

Процесс управления ИБ распадается на тесно взаимосвязанные подпроцессы, каждый из которых вносит существенный вклад в достижение общих целей управления ИБ. Объектами управления в рамках этих подпроцессов являются активы, риски ИБ, инциденты ИБ, непрерывность бизнеса, изменения, усовершенствования и многое другое. От эффективности и результативности каждого из этих подпроцессов зависят общая эффективность и результативность всей деятельности по управлению ИБ в организации [5].

В методических указаниях рассмотрены формальные модели управления доступом и информационными потоками и их практические реализации в компьютерных системах (КС), создающие предпосылки для развития теории компьютерной безопасности и разработки новых эффективных методов анализа защищенности современных или перспективных КС, таких как операционных систем, СУБД, систем электронного документооборота и т.д. [2].

Практическое занятие № 5
Модель Белла-ЛаПадулы. Мандатное управление доступом

Теоретические положения

Классическая модель Белла-ЛаПадулы *{Bell-LaPadula)* описана в 1975 году [8] и в настоящее время является основной моделью, предназначенной для анализа систем защиты, реализующих мандатное управление доступом.

В классической модели Белла-ЛаПадулы рассматриваются условия, при выполнении которых в КС невозможно возникновение информационных потоков от объектов с большим уровнем конфиденциальности к объектам с меньшим уровнем конфиденциальности. Основными элементами классической модели Белла-ЛаПадулы являются: S - множество субъектов; O — множество объектов; R = *{read, write, append* (доступ на запись в конец объекта), *execute}* — множество видов доступа и видов прав доступа; $B = \{b \subset S \times O \times R\}$ — множество возможных множеств текущих доступов в системе; $(L, \leq)$ — решетка уровней конфиденциальности, например L = *{U (unclussifted), C {confidential), S {secret), TS {top secret)},* где $U < C < S < TS$; $M \{m_{|S|\times|O|}\}$ множество возможных матриц доступов, где $m_{|S|\times|O|}$ — матрица доступов, $m[s,o] \subseteq R$ — права доступа субъекта s к объекту o; $(f_s, f_o, f_c) \in F = L^S \times L^O \times L^S$ — тройка функций (f_s, f_o, f_c), задающих соответственно: $f_s : S \to L$ — уровень доступа субъектов; $f_o : S \to L$ — уровень конфиденциальности объектов; $f_c : S \to L$ — текущий уровень доступа субъектов, при этом для любого $s \in S$ выполняется неравенство $f_c(s) \leq f_s(s)$; $V = B \times M \times F$ — множество состояний системы; Q — множество запросов системе; D — множество ответов по запросам, например D =

{yes, no, error}; $W \subseteq Q \times D \times V \times V$ — множество действий системы, где четверка $(q, d, \upsilon^*, \upsilon) \in W$ означает, что система по запросу q с ответом d перешла из состояния υ в состояние υ^*; $N_0 = \{1,2,...\}$ — множество значений времени; X - множество функций x: $N_0 \to Q$, задающих все возможные последовательности запросов к системе; Y - множество функций y: $N_0 \to D$ задающих все возможные последовательности ответов системы по запросам; Z — множество функций $z : N_0 \to V$, задающих все возможные последовательности состояний системы.

Определение 1. $\sum(Q, D, W, z_0) \subseteq X, Y, Z$ называется системой, когда для каждого $(x, y, z) \in \sum(Q, D, W, z_0)$ выполняется условие: для $t \in N_0$, $(x_t, y_t, z_{t+1}, z_t) \in W$, где z_0 — начальное состояние системы. При этом каждый набор $(x, y, z) \in \sum(Q, D, W, z_0)$ называется реализацией системы, а $(x_t, y_t, z_{t+1}, z_t) \in W$ - действием системы в момент времени $t \in N_0$.

В классической модели Белла-ЛаПадулы рассматриваются следующие запросы, входящие во множество *Q:*

- запросы изменения множества текущих доступов b;
- запросы изменения функций f;
- запросы изменения прав доступа в матрице т.

Следующий список описывает изменения каждого элемента состояния системы. Конкретное решение по запросу включает возможность производить следующие изменения в состоянии системы.

1. Изменение текущих доступов:

- *получить доступ* (добавить тройку (субъект, объект, вид доступа) в текущее множество доступов b);

- *отменить доступ* (удалить тройку (субъект, объект, вид доступа) из текущего множества доступов *b*).

2. Изменение значений функций уровней конфиденциальности и доступа:

- *изменить уровень конфиденциальности объекта;*
- *изменить уровень доступа субъекта.*

3. Изменение прав доступа:

- *дать разрешение на доступ* (добавить право доступа в соответствующий элемент матрицы доступов *m);*
- *отменить разрешение на доступ* (удалить право доступа из соответствующего элемента матрицы доступов *m).* Безопасность системы определяется с помощью трех свойств:

ss – свойства простой безопасности (*simple security);*

* — свойства «звезда»;

ds — свойства дискреционной безопасности *(discretionary security).*

Определение 2. Доступ $(s, o, r) \in S \times O \times R$ обладает *ss*-свойством относительно $f = (f_s, f_o, f_c) \in F$, когда выполняется одно из условий: $r \in$ *{execute, append};* $r \in$ *{read, write}* и $f_s \geq f_0(o)$

Определение 3. Состояние системы $(b, m, f) \in V$ обладает *ss*-свойством, когда каждый элемент $(s, o, r) \in b$ обладает *ss*-свойством относительно.

Определение 4. Доступ $(s, o, r) \in S \times O \times R$ обладает *-свойством относительно $f = (f_s, f_o, f_c) \in F$, когда выполняется одно из условий: *r= execute; r= append* и $f_0(o) \geq f_c(s)$; *r= read* и $f_c(s) \geq f_o(o)$; *r= write* и $f_c(s) = f_o(o)$.

Определение 5. Состояние системы $(b, m, f) \in V$ обладает *-свойством, когда каждый элемент $(s, o, r) \in b$ обладает *-свойством относительно.

Определение 6. Состояние системы $(b, m, f) \in V$ обладает *-свойством относительно подмножества $S' \subseteq S$, когда каждый элемент $(s, o, r) \in b$, где $s \in S'$, обладает *-свойством относительно *f*. При этом S / S' называется множеством доверенных субъектов, т. е. субъектов, имеющих право нарушать требования *-свойства.

Определение 7. Состояние системы $(b, m, f) \in V$ обладает *ds*-свойством, когда для каждого доступа $(s, o, r) \in b$ выполняется условие $r \in m[s, o]$.

Определение 8. Состояние системы (b, m, f) называется безопасным, когда оно обладает *-свойством относительно *S', ss*-свойством и *ds*-свойством.

Определение 9. Реализация системы $(x, y, z) \in \sum(Q, D, W, z_0)$ обладает *ss*-свойством (*-свойством, *ds*-свойством), когда в последовательности $(z_0, z_1, \ldots)$ каждое состояние обладает *ss*-свойством (*-свойством, *ds*-свойством).

Определение 10. Система $\sum(Q, D, W, z_0)$ обладает *ss*-свойством (*- свойством, *ds*-свойством), когда каждая ее реализация обладает *ss*-свойством (*-свойством, *ds*-свойством).

Определение 11. Система $\sum(Q, D, W, z_0)$ называется безопасной, когда она обладает *ss*-свойством, *-свойством, *ds*-свойством одновременно.

Проверка безопасности системы по определению в большинстве случаев не может быть реализована на практике в связи с тем, что при этом требуется проверка безопасности всех реализаций системы, а их бесконечно много. Следовательно, необходимо определить и обосновать иные условия безопасности системы, которые можно проверять на практике. В классической модели Белла-ЛаПадулы эти условия задаются для множества действий системы *W*.

Теорема 1. (A1). Система $\sum(Q, D, W, z_0)$ обладает *ss*-свойством для любого начального состояния z_0, обладающего *ss*-свойством, тогда и только тогда, когда для каждого действия $(q, d, q^*, m^*, f^*, q, m, f) \in W$ выполняются *условия 1, 2.*

Условие 1. Каждый доступ $(s, o, r) \in b^* \setminus b$ обладает *ss*-свойством относительно f^*.

Условие 2. Если $(s, o, r) \in b$ и не обладает *ss*-свойством относительно f^*, то $(s, o, r) \notin b^*$.

Теорема 2. (A2). Система $\sum(Q, D, W, z_0)$ обладает *-свойством относительно $S' \subseteq S$ для любого начального состояния z_0, обладающего *-свойством относительно *S'*, тогда и только тогда, когда для каждого действия $(q, d, q^*, m^*, f^*, q, m, f) \in W$ выполняются *условия 1* и *2*.

Условие 1. Для $s \in S'$ доступ $(s, o, r) \in b^* \setminus b$ *-свойством относительно *f**.

Условие 2. Для $s \in S'$, если доступ $(s, o, r) \in b$ и не обладает *-свойством относительно *f**, то $(s, o, r) \notin b^*$.

Теорема 3. (A3). Система $\sum(Q, D, W, z_0)$ обладает *ds*-свойством для любого начального состояния z_0, обладающего *ds*-свойством, тогда и только тогда, когда для каждого дейст-

вия $(v, d, v^*, m^*, f^*, v, m, f) \in W$ выполняются *условия 1* и *2*.

Условие 1. Для каждого $(s, o, r) \in b^* \setminus b$, выполняется условие $r \in m^*[s, o]$.

Условие 2. Если доступ $(s, o, r) \in b$ и $r \notin m^*[s, o]$, то $(s, o, r) \notin b$.

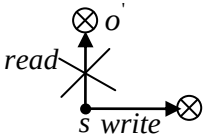
Теорема 4. (базовая теорема безопасности — БТБ). Система $\sum(Q, D, W, z_0)$ безопасна для безопасного z_0 тогда и только тогда, когда множество действий системы W удовлетворяет условиям *теорем 1-3*.

Доказательство. Данная теорема следует из *теорем 1-4*. Описанная классическая модель Белла-ЛаПадулы предоставляет общий подход к построению систем, реализующих мандатную политику безопасности. В модели определяется, какими свойствам должны обладать состояния и действия системы, что бы система была безопасной согласно данным определениям. В то же время в модели не задается точный порядок действий системы управления доступом по запросам на доступ субъектов к объектам.

Пример 1. Пусть субъект *s* запрашивает доступ *read к* объекту *o'* (см. рис. 1). В данной ситуации система может выбрать один из двух возможных ответов по запросу:

1) запретить субъекту *s* запрашиваемый им доступ *read* к объекту *o'*;

2) закрыть доступ *write* субъекта *s* к объекту *o*. Повысить текущий уровень конфиденциальности $f_c(s)$ надо *High*. Разрешить субъекту *s* запрашиваемый им доступ *read* к объекту *o'*.



$$f_s(s) = f_o(o') = High$$

$$f_c(s) = f_o(o') = Low$$

Рис. 1. Иллюстрация *-свойства

Каждый из описанных путей соответствует требованиям безопасности модели Белла-ЛаПадулы.

В реальных системах возможны более сложные ситуации, чем ситуация, описанная в *примере 1*. Кроме того, возможно использование в системе каких-то других видов доступа субъектов к объектам, которые потребуют дополнительного определения свойств безопасности, что не всегда легко сделать. В связи с этим большое значение имеет корректное определение свойств безопасности.

Мандатная ДП-модель. Правила преобразования состояний мандатной модели

С использованием модели Белла-ЛаПадулы и способов реализации информационных потоков определим запрещенные информационные потоки из множества N_f, условия возникновения которых, как правило, анализируются в КС с мандатным управлением доступом.

Определение 12. Определим как запрещенные в КС с мандатным управлением доступом следующие четыре вида информационных потоков (запрещенные информационные потоки из множества N_f).

1. Информационные потоки по памяти и по времени между сущностями одного уровня конфиденциальности (определяются в соответствии с априорно заданной политикой управления доступом и информационными потоками).
2. Информационные потоки по памяти от сущностей с большим уровнем конфиденциальности к сущностям с меньшим уровнем конфиденциальности информации.
3. Информационные потоки по времени от сущностей с большим уровнем конфиденциальности к сущностям с меньшим уровнем конфиденциальности информации.
4. Информационные потоки по памяти от субъектов с низким уровнем доступа к субъектам с высоким уровнем

доступа или к сущностям, функционально ассоциированным с субъектами с высоким уровнем доступа.

Информационные потоки по памяти первого вида не нарушают требований мандатного управления доступом, так как возникают между сущностями одного уровня конфиденциальности.

Модель Белла-ЛаПадулы в основном ориентированы на обеспечение в КС условий защиты от возникновения запрещенных информационных потоков по памяти второго вида.

Для анализа информационных потоков по памяти, позволяющих субъекту повысить свой уровень доступа (запрещенных информационных потоков четвертого вида), рассмотрим ДП-модель КС с мандатным управлением доступом (далее будем называть мандатной ДП-моделью), в основе которой использованы базовая ДП-модель, БК ДП-модель и ФАС ДП-модель. При этом дополнительно используем обозначения: $(L, \leq)$ - решетка линейно упорядоченных уровней доступа и конфиденциальности ; $ES \subset E \setminus S$ — множество сущностей, которые могут быть применены для создания новых субъектов (в отличие от дискреционных ДП-моделей, в мандатной ДП-модели субъект может создать субъекта из сущности, когда сущность принадлежит множеству *ES);* $f_s : S \to L$ — функция, задающая уровень доступа каждого субъекта системы $\sum(G^*, OP)$; $f_e : E \setminus S \to L$ — функция, задающая уровень конфиденциальности каждой сущности системы, не являющейся субъектом, при этом, если для двух сущностей $e_1, e_2 \in E$ выполняется неравенство $e_1 \leq e_2$ (сущность e_1 содержится в контейнере e_2), то по определению выполняется условие $f_e(e_1) \leq f_e(e_2)$; $OCR: E \setminus S \to \{true,\ false\}$ — функция, задающая способ доступа к сущностям, не являющимся субъектами, внутри контейнеров. Если сущность $e \in E$ является контейнером и доступ к сущностям, содержащимся

внутри контейнера e, разрешен без учета уровня конфиденциальности контейнера e, то по определению выполняется равенство *CCR(e)=false,* в противном случае выполняется равенство *CCR(e)=true.* При этом по определению для каждой сущности $e \in E$, являющейся объектом, выполняется условие *CCR(e) — false.*

Определение 13. Пусть $G = (S, E, R \cup A \cup F, H, f_s, f_e, CCR)$ — конечный помеченный ориентированный граф, без петель, где назначение элементов графа *S, E, R, A, F, H* соответствует *определению 7* занятия № 4. При этом для каждой сущности $e \in E \setminus S$ определены значения функций $f_e(e), CCR(e)$, для каждого субъекта $s \in S$ определено значение функции $f_s(s)$.

Предположение 1. Значение решетки уровней доступа и конфиденциальности $(C, \leq)$ множества сущностей *ES* не изменяются на траекториях функционирования системы $\sum(G^*, OP)$. При создании сущности для нее определяются значения функций f_e, CCR, которые не изменяются в дальнейшем на траекториях функционирования системы. При создании субъекта для него определяется значение функции f_s, которое может быть изменено на траекториях функционирования системы только в случае, когда данный субъект либо является функционально ассоциированной сущностью другого субъекта, либо он реализовал информационный поток по памяти к сущности, функционально ассоциированной с другим субъектом.

Правила дискреционного управления доступом могут быть использованы в КС с мандатным управлением доступом. В то же время условия передачи прав доступа на основе правил дискреционного управления доступом с использованием преобразований множества прав доступов не используются в мандатной ДП-модели. Таким образом, в дальнейшем используется следующее предположение.

Предположение 2. На траекториях функционирования системы $\sum(G^*, OP)$ не используются правила преобразования состояний, позволяющие субъектам брать, передавать и удалять права доступа к сущностям, удалять субъектов или сущности. При проверке возможности предоставления субъекту права доступа к сущности не учитывается содержимое множества прав доступа *R*.

В ДП-моделях КС с дискреционным управлением доступом рассматривалась возможность реализации субъектами доступов друг к другу на основе имеющихся у них прав доступа. В мандатной ДП-модели рассматриваются условия реализации запрещенных информационных потоков, при этом доступы субъектов к сущностям реализуются в зависимости от уровней доступа субъектов и уровней конфиденциальности сущностей. Таким образом, в дальнейшем используется следующее предположение.

Предположение 3. На любых траекториях функционирования системы $\sum(G^*, OP)$ не реализуются доступы субъектов к субъектам системы.

Таким образом, в рамках *предположений 2* и *3* в мандатной ДП-модели не рассматривается дискреционное управление доступом.

В соответствии с *предположением 2* при проверке возможности предоставления субъекту доступа к сущности не учитывается содержимое множества прав доступа *R,* а используется проверка соотношения уровня доступа субъекта и уровня конфиденциальности сущности. Кроме того, доверенными могут являться субъекты системы, имеющие низкий уровень доступа, например субъекты, являющиеся системными процессами, функциональность которых не требует предоставления им возможности доступа к сущностям с высоким уровнем конфиденциальности. Недоверенные субъекты системы могут иметь различные уровни доступа. Например, процессы, запущенные от имени недоверенного

пользователя с высоким уровнем доступа, в общем случае могут иметь различные уровни доступа, не превышающие уровень доступа пользователя. Таким образом, в дальнейшем используется следующее предположение.

Предположение 4. Каждый субъект системы $\sum(G^*, OP)$ вне зависимости от его уровня доступа может являться либо доверенным, либо недоверенным. Доверенные субъекты не участвуют в реализации информационных потоков по времени.

Используем обозначения:

$N_s(l) = \{s \in N_s : f_s(s) \le l\}$ — множество недоверенных субъектов системы $\sum(G^*, OP)$ с уровнем доступа не большим l, где $l \in L$; $L_s(l) = \{s \in L_S : f_s(s) \le l\}$ — множество доверенных субъектов системы $\sum(G^*, OP)$ с уровнем доступа не большим l, где $l \in L$.

Определим *ss*-свойство и *-свойство безопасности системы $\sum(G^*, OP)$. При этом в отличие от классической модели Белла-ЛаПадулы используем следующее предположение.

Предположение 5. В мандатной ДП-модели не рассматриваются субъекты, которые могут нарушать *-свойство безопасности (доверенные субъекты модели Белла-ЛаПадулы).

Определение 14. В состоянии $G = (S, E, R \cup A \cup F, H, (f_s, f_e, CCR))$ системы $\sum(G^*, OP)$ доступ $(s, e, \alpha) \in A$, где субъект $s \in S$, сущность $e \in E \setminus S$, вид доступа $\alpha \in R_a$, обладает *ss*-свойством, когда выполняются условия: $f_s(s) \ge f_e(e)$; для каждой сущности-контейнера $e' \in E \setminus S$ такой, что e < *e'* и *CCR(e')= true*, выполняется неравенство $f_s(s) \ge f_e(e')$.

Определение 15. В состоянии $G = (S, E, R \cup A \cup F, H, (f_s, f_e, CCR))$ системы $\sum(G^*, OP)$ доступы $(s, e_1, read_a), (s, e_2 \alpha) \in A$, где субъект $s \in S$, сущности вид доступа $\alpha \in \{write_a, append_a\}$, обладают *-свойством, когда выполняется условие $f_e(e_1) \leq f_e(e_2)$.

Определение 16. Состояние системы $\sum(G^*, OP)$ обладает *ss*-свойством или *-свойством, когда в состоянии все доступы обладают *ss*-свойством или *-свойством соответственно.

Определение 17. Состояние системы $\sum(G^*, OP)$ называется безопасным в смысле Белла-ЛаПадулы, когда оно обладает *ss*-свойством и *-свойством. Система $\sum(G^*, OP)$ называется безопасной в смысле Белла-ЛаПадулы, когда все состояния системы на всех конечных траекториях ее функционирования безопасны в смысле Белла-ЛаПадулы.

В мандатной ДП-модели определены следующие правила преобразования состояний (см. таблицу), в которых использованы определения ss-свойства и *-свойства безопасности. Таким образом, устранен недостаток классической модели Белла-ЛаПадула, заключающийся в отсутствии в ней описания правил перехода системы из состояния в состояние.

Таблица

Правила преобразования мандатной ДП-модели

Правило	Исходное состояние $G = (S, E, R \cup A \cup F, H, f_s, f_e, CCR)$	Результирующее состояние $G' = (S', E', R' \cup A' \cup F', H', f_s', f_e', CCR')$
create_entity (x,y,z,I,ccr)	$x \in S; y \notin E; z \in E \setminus S; l \le f_e(z);$ $ccr \in \{true, false\}$; $(x, z, \alpha_a) \in A$, где $\alpha_a \in \{write_a, append_a\}$; не существует сущности $e \in E \setminus S$ такой, что $f_e(y) < f_e(e)$ и $(x, e, read_a) \in A$	$S' = S; E' = E \cup \{y\}; R' = R; f_s' = f_s;$ $H'(x) = H(x) \cup \{y\}; H'(y) = \varnothing$ для $e \in E \setminus \{z\}$ выполняется равенство $H'(e) = H(e)$; $A' = A \cup \{x, y, write_a\}; f_e'(y) = l;$ для $e \in E \setminus S$ выполняются равенства $f_e'(e) = f_e(e); CCR'(e) = CCR(e);$ если $y \in O'$, то $CCR'(y) = false;$ если $y \in C'$, то $CCR'(y) = ccr;$ если $x \in N_S \cap S$, то $F' = F \cup \{x, e, write_t\}; e \in E$ **и** $y \le e$; если $x \in L_S \cap S$, **то** $F' = F$
create_subject (x, y,z,l)	$x \in S; y \in ES; z \notin E; f_s(x) \le f_e(y);$ $f_s(x) \ge l$; для каждой сущности-контейнера $y' \in E \setminus S$ такой, что $y < y'$ *и* $CCR(y') = true,$ выполняется неравенство $f_s(x) \ge f_e(y')$	$S' = S \cup \{z\}; E' = E \cup \{z\}; R' = R; A' = A;$ $H'(x) = H(x) \cup \{z\}; H'(y) = \varnothing$ для $e \in E \setminus \{z\}$ выполняется равенство $H'(e) = H(e);$ $f_s'(z) = l;$ $CCR'(z) = false;$ для $s \in S$ выполняется равенство $f_s' = f_s(s)$; для $e \in E \setminus S$ выполняются равенства $f_e'(e) = f_e(e); CCR'(e) = CCR(e)$ если $x \in N_s \cap S$, то $F' = F \cup \{x, x, write_t\} \cup \{x, e, write_t\}; e \in E$ и $y \le e$; если $x \in L_s \cap S,$ то $F' = F$

Продолжение таблицы

Правило	Исходное состояние $G = (S, E, R \cup A \cup F, H, (f_s, f_e), CCR)$	Результирующее состояние $G' = (S', E', R' \cup A' \cup F', H', (f_s', f_e'), CCR')$
rename_entity (x, y, z)	$x \in S; y, z \in E \setminus S; y \in H(x)$ $(x, z, write_a) \in A;$ не существует сущности $e \in E \setminus S$ такой, что $f_e(y) \le f_e(e)$ и $(x, e, read_a) \in A$	$S' = S; E' = E; R' R; H' = H;$ $f_s' = f_s; f_e' = f_e; CCR' = CCR;$ $A' = A \cup (x, y, write_a);$ если $x \in N_S \cap S,$, то $F' = F \cup \{(e, e, write_t) : e \in E; x \ne e\}$ и $e \le z$ $\cup \{(s, s, write_t) : s \in S; x \ne s\}$ и $(s, e, \alpha_r) \in R,$ где $e \in E; e \le y;$ и $\alpha_r \in R_t$ если $x \in L_s \cap S$, то $F' = F$
access_read(x,y)	$x \in S; y \in E \setminus S; f_s(x) \ge f_e(y);$ для каждой сущности-контейнера $y' \in E \setminus S$ такой, что $y < y'$ и $CCR(y') = true,$ выполняется неравенство $f_s(x) \ge f_e(y')$; не существует сущности $z \in E \setminus S$ такой, что $f_e(x) \le f_e(y)$ и $(x, z, \alpha_a) \in A$, где $\alpha_a \in \{write_a, append_a\}$	$S' = S; E' = E; R' = R; H' = H;$ $f_s' = f_s; f_e' = f_e; CCR' = CCR;$ $A' = A \cup (x, y, read_a);$ если $x \in N_S \cap S,$, то $F' = F \cup (y, x, write_m) \cup \{(e, e, write_t) : e \in E, x \ne e$ и $y \le e\}$ если $x \in L_S \cap S$, то $F' = F \cup (y, x, write_m)$
access_write (x,y)	$x \in S; y \in E \setminus S; f_s(x) \ge f_e(y);$ для каждой сущности-контейнера $y' \in E \setminus S$ такой, что $y < y'$ и $CCR(y') = true,$ выполняется неравенство $f_S(x) \ge f_e(y')$; не существует сущности $z \in E \setminus S$ такой, что $f_e(x) \le f_e(z)$ и $(x, z, read_a) \in A$	$S' = S; E' = E; R' = R; H' = H;$ $f_s' = f_s; f_e' = f_e; CCR' = CCR;$ $A' = A \cup (x, y, write_a);$ если $x \in N_s \cap S$, то $F' = F \cup (x, y, write_m) \cup \{(e, e, write_t) : e \in E;$ $x \ne e$ и $y \le e;$ если $x \in L_S \cap S$, то $F' = F \cup (x, y, write_m)$

Продолжение таблицы

Правило	Исходное состояние $G = (S, E, R \cup A \cup F, H, (f_s, f_e), CCR)$	Результирующее состояние $G' = (S', E', R' \cup A' \cup F', H', (f_s', f_e'), CCR')$
access_append (x,y)	$x \in S; y \in E \setminus S; f_s(x) \geq f_e(y)$; для каждой сущности-контейнера $y' \in E \setminus S$ такой, что $y < y'$ и $CCR(y') = true$, выполняется неравенство $f_S(x) \geq f_e(y')$ не существует сущности $z \in E \setminus S$ такой, что $f_e(y) \leq f_e(z)$ и $(z, read_a) \in A$	$S' = S; E' = E; R' = R; H' = H; f_s' = f_s; f_e' = f_e$ $CCR' = CCR; A' = A \cup (x, y, append_a)$ если $x \in N_S \cap S$, то $F' = F \cup (x, y, write_m) \cup (e, write_t); e \in E;$ $x \neq e$ и $y \leq e$; если $x \in L_S \cap S$, то $F' = F \cup (x, y, write_m)$
flow{x,y,y',z)	$x, z \in S; y, y' \in E; x \neq z; y \leq y'$ $(x, y, \alpha_a), (z, y', \beta_\alpha) \in A,$ где $\alpha_a, \beta_a \in R_a$	$S' = S; E' = E; R' = R; H' = H;$ $f_s' = f_s; f_e' = f_e;$ $ССД' = ССД;$ если $x, y \in N_S \cap S,$ то $F' = F \cup (x, z, write_t) (x, x, write_t);$ если $x, z \cap L_s \cap S \neq \varnothing,$ то $F' = F$
find(x, y, z)	$x, z \in S; z \in E; x \neq z;$ $(x, y, \alpha), (y, z, \beta) \in A \cup F$,где $\alpha, \beta \in$ $write_a, append_a, write_m, write_t$	$S' = S; E' = E; R' = R; H' = H;$ если $f_s' = f_s; f_e' = f_e; CCR' = CCR;$ $write_t \neq \alpha, \beta$, то $F' = F \cup (x, z, write_m);$ если $write_t \in \alpha, \beta$ и $x, y \in N_s \cap S,$ то $F' = F \cup (x, z, write_t);$ если $write_t \in \alpha, \beta$ и $x, y \cap L_s \cap S = \varnothing,$ то F' = F

Продолжение таблицы

Правило	Исходное состояние $G = (S, E, R \cup A \cup F, H, (f_s, f_e), CCR)$	Результирующее состояние $G' = (S', E', R' \cup A' \cup F', H', (f'_s, f'_e), CCR')$
post(x,y,z)	$x, z \in S; z \in E; x \neq z;$ $(x, y, \alpha) \in R$ $(z, y, read_a) \notin A \cup F$,где $\alpha \in \{write_a, append_a, write_m, write_t\}$	$S' = S; E' = E; R' = R; H' = H;$ $f'_s = f_s; f'_e = f_e; CCR' = CCR;$ если $\alpha \neq write_t$, то $F' = F \cup (z, write_m)$; если $\alpha = write_t$ и $x, y \in N_s \cap S,$ то $F' = F \cup (z, write_t)$; если $\alpha = write_t$ и $\{z\} \cap L_s \cap S = \varnothing,$ то F' = F
pass(x,y, z)	$x, z \in S; z \in E; x \neq z;$ $(x, y, \alpha) \in R$ $(z, y, read_a) \notin A \cup F$,где $\alpha \in \{write_a, append_a, write_m, write_t\}$	$S' = S; E' = E; R' = R; H' = H;$ $f'_s = f_s; f'_e = f_e; CCR' = CCR;$ если $\alpha \neq write_t$, то $F' = F \cup (z, write_m)$; если $\alpha = write_t$ и $y \in N_s \cap S,$ то $F' = F \cup (z, write_t)$; если $\alpha = write_t$ и $y \in L_S \cap S,$ то $\{z\} \cap \varnothing$, то F' =F
control(x,y,z)	$x, z \in S; z \in E; z \in$ [illegible]$; f_s(z) < f_s(y)$ и или $x = z$, или $(x, z, write_m) \in F$	$S' = S; E' = E; R' = R; H' = H;$ $f'_s(z) = f_s(y);$ $f'_s = f_s; f'_e = f_e; CCR' = CCR;$ для $s \in S \setminus \{z\}$ выполняется равенство $f'_s(s) = f_s(s)$

Безопасность в смысле Белла-Ла Падулы

В рамках мандатной ДП-модели доказано утверждение, аналогичное утверждению, обоснованному в *теореме 4* данной работы (базовой теореме безопасности модели Белла-ЛаПадулы).

Теорема 5. **(БТБ-ДП).** Пусть $G_0 = (b_0, E_0, R_0 \cup A_0 \cup F_o, H_0, f_{s0}, f_{e0}, CCR_0)$ — начальное состояние системы $\sum(G^*, OP)$, являющееся безопасным в смысле Белла-ЛаПадулы, и $A_0 = F_0 = \varnothing$. Тогда система $\sum(G^*, OP, G_0)$ является безопасной в смысле Белла-ЛаПадулы.

Таким образом, в системе $\sum(G^*, OP)$ по *теореме 2* не могут быть реализованы запрещенные информационные потоки второго вида (информационные потоки по памяти от сущностей с большим уровнем конфиденциальности к сущностям с меньшим уровнем конфиденциальности).

Типовые задачи

Задание 1. Опишите состояния системы Белла-ЛаПадулы со следующими параметрами: $S = (s_1, s_2)$, $O = (o_1, o_2)$, $R = \{read, write\}$, $(C, \leq) = (Low, High)$, M — не используется, $f_s(s_1) = f_0(o_1) = Low$, $f_s(s_2) = f_o(o_2) = High$.. Подсчитайте количество различных состояний системы для следующих случаев:

- в системе не требуется выполнение свойств безопасности;
- в системе требуется выполнение только *ss*-свойства;
- в системе требуется выполнение *ss* -свойства и *-свойства.

Решение. В определениях *ss*-свойства, *-свойства безопасности классической модели Белла-ЛаПадулы отсутствуют ограничения на совместный доступ субъектов системы к объектам системы. Кроме того, по условию значения функций f_s и f_0 не меняются при переходе системы из состояния в состояние. Следовательно, будем считать, что выполняются условия:

$V = (b, f_c)$, где $b \subseteq S \times O \times R$ – множество состояний системы;

$V_1 = (b_1, f_c(s_1))$, где $b_1 \subseteq \{s_1\} \times O \times R$ – множество состояний субъекта s_1;

$V_2 = (b_2, f_c(s_2))$, где $b_2 \subseteq \{s_1\} \times O \times R$ – множество состояний субъекта s_2.

При этом справедливо равенство $V = V_1 \times V_2$.

Существуют состояния, в которых для выполнения *-свойства безопасности функция текущего уровня доступа субъекта s_2 может принимать значения *Low* или *High.* В таких состояниях будем считать, что справедливо равенство $f_c(s_2) = Low$.

Если в системе не требуется выполнение свойств безопасности, то каждый субъект может получать любые доступы к объектам. Следовательно, справедливы равенства $|V_1| = |V_2| = 16, |V| = 256$.

Если в системе требуется выполнение только *ss*-свойства, то субъект s_1 может получать любые доступы к объекту o_1 субъект s_2 может получать любые доступы к объектам o_1 и o_2. Следовательно, справедливы равенства $|V_1| = 4, |V_2| = 16, |V| = 64$..

Пусть в системе требуется выполнение *ss*-свойства и *-свойства. Тогда справедливы равенства:

$$V_1 = \{(\varnothing, low), (s_1, o_1, read, Low), (s_1, o_1, write, Low), (s_1, o_1, read, s_1, o_1, write, Low)\};$$

$$|V_1| = 4;$$

$$V_2 = \{(\varnothing, Low), (s_2, o_1, read, Low)(s_2, o_1, write), low (s_2, o_2, read, High), (s_2, o_2, read, High), (s_2, o_2, write, High), (s_2, o_2, read), (s_2, o_2, write), High), (s_2, o_2, read), (s_2, o_1, read), High), (s_2, o_2, write), (s_2, o_1, read), High), (s_2, o_2, read), (s_2, o_2, write), (s_2, o_2, read), High)\};$$

$$|V_2| = 10;$$

$$|V| = 40.$$

Задание 2. Переформулируйте определения *ss*-свойства и *-свойства функции переходов $T(s, q, (b, f)) = (b^*, f^*)$, включив в них определение безопасности функции переходов в смысле администрирования.

Решение. Дадим определения *ss*-свойства и *-свойства безопасности функции переходов с учетом определения безопасности в смысле администрирования.

Определение. Функция переходов *T(u,q,(b,f))=(b*,f*)* обладает *ss*-свойством, когда выполнены следующие условия:

- если $(s_0, o, read) \in b^* \setminus b$, то $f_s(s) \geq f_0(s)$ и $f^* = f$;
- •если $f_s(s) \neq f_s^*(s)$,то $f_0^* = f_0, b^* = b, u \in c_s(s)$,для $s' \neq s$ справедливо равенство $f_s^*(s') = f_s^*(s')$, и если $(s, o, read) \in b$, то $f_s^*(s) \geq f_o(o)$;
- •если $f_s(s) \neq f_s^*(s)$,то $f_s^* = f_s, b^* = b, u \in c_0(s)$,для $o' \neq o$ справедливо равенство $f_s^*(s') = f_0(s')$ и если $(s, o, read) \in b$, то $f_s(s) \geq f_o^*(o)$.

Определение. Функция переходов $T(u,q,(b,f))=(b^*,f^*)$ обладает *-свойством, когда выполнены следующие условия:

- если $(s,x,read)\in b^*$ и $(s,x,read)\in b$, то $f^*=f$ и $f_0(y)\geq f_0(x)$;
- если $f_0(y)\neq f_o^*(o)$, то $b^*=b, f_s^*=f_s, u\in c_0(y)$, для $z\neq y$ справедливо равенство $f_0^*(z)=f_0(z)$, и если $(s,x,read)\in b$, то $f_0^*(y)\geq f_0(z)$, или если $(s,y,read)\in b$, то $f_0(z)\geq f_o^*(y)$.

Задание 3. Рассмотрите возможность учета в определении безопасности функции переходов в смысле администрирования требований мандатной политики безопасности.

Решение. Дадим определения ss-свойства и *-свойства безопасности функции переходов с учетом определения безопасности в смысле администрирования и требований мандатной политики безопасности.

Определение. Функция переходов $T(u,q,(b,f)) = (b^*,f^*)$ обладает ss-свойством, когда выполнены следующие условия:

- если $(s,o,read)\in b^*\setminus b$, то $f_s(s)\geq f_o(o)$ и $f^*=f$;;
- если $f_s(s)\neq f_s^*(s)$, то $f_o^*=f_o, b^*=b, u\in c_s(s), f_s(y)\geq f_s(s), f_s(y)\geq f_s^*$ для $s'\neq s$ и справедливо равенство $f_s^*(s')=f_s(s')$, и если $(s,o,read)\in b$, то $f_s^*(s)\geq f_o(o)$;
- если $f_o(o)\neq f_0^*(o)$, то $f_s^*=f_s, b^*=b, u\in c_o(o), f_s(y)\geq f_o(o), f_s(y)\geq f_o^*(o)$, для $o'\neq o$ справедливо равенство $f_o^*(o')=f_o(o')$ и если $(s,o,read)\in b$, то $f_s^*(s)\geq f_o^*(o)$.

Определение. Функция переходов $T(u,q,(b,f)) = (b^*,f^*)$ обладает *-свойством, когда выполнены следующие условия:

- если $(s, x, read) \in b^*$ и $(s, x, read) \in b$, то $f^* = f$ и $f_o(y) \geq f_o(x)$;
- если $f_o(y) \neq f_o^*(y)$, то $b^* = b$, $f_s^* = f_s, u \in c_0(y), f_s(x) \geq f_0(y), f_s(x) \geq f_o^*(y)$, для $z \neq y$ справедливо равенство $f_o^*(z) = f_o(z)$, и если $(s, x, read) \in b$, то $f_0(x) \geq f_o^*(y)$.

Задачи для самостоятельного решения

1. Каковы основные недостатки классической модели Белла-ЛаПадулы?

2. Известно, что при реализации мандатного управления доступом может допускаться использование правил дискреционного управления доступом (например, с использованием *ds*-свойства безопасности модели Белла-ЛаПадулы). Учитывая это обстоятельство, предложите подход по созданию запрещенного информационного потока от объекта с высоким уровнем конфиденциальности к объекту с низким уровнем конфиденциальности, использующий кооперацию субъектов КС.

3. Рассмотрите возможность учета в определении безопасности функции переходов в смысле администрирования требований мандатной политики безопасности (например, потребовав, чтобы инициировать изменение уровня конфиденциальности объекта мог только субъект, имеющий не меньший чем у объекта уровень доступа).

4. Опишите состояния, соответствующие *условиям 3* или *4 теоремы 6*, и последовательности преобразований этих состояний, соответствующие определению предиката *can_increase_level(x,Go).*

Практическое занятие № 6
Ролевое и мандатное ролевое управление доступом

Теоретические положения

Ролевое управление доступом представляет собой развитие политики дискреционного управления доступом, при этом права доступа субъектов системы к объектам группируются с учетом специфики их применения, образуя роли. Ролевое управление доступом является составляющей многих современных КС. Как правило, оно применяется в системах защиты СУБД, отдельные элементы ролевого управления доступом реализуются в сетевых ОС.

Задание ролей позволяет определить более четкие и понятные для пользователей КС правила управления доступом. При этом ролевое управление доступом наиболее эффективно используется в КС, для пользователей которых четко определен круг их должностных полномочий и обязанностей.

Роль является совокупностью прав доступа к объектам КС. Однако ролевое управление доступом не является частным случаем дискреционного управления доступом, так как его правила задают порядок предоставления прав доступа субъектам (пользователям) КС в зависимости от сессии его работы и от имеющихся или отсутствующих у него ролей в каждый момент времени, что является характерным для систем мандатного управления доступом. В то же время правила ролевого управления доступом являются более гибкими, чем правила мандатного управления доступом, построенные на основе жестко определенной решетки (шкалы) ценности информации.

Для анализа и изучения свойств КС с ролевым управлением доступом используются формальные модели, в основе которых лежит базовая модель ролевого управления доступом.

Базовая модель ролевого управления доступом

Основными элементами базовой модели ролевого управления доступом *(RBAC — Role-Based Access Control)* [4, 11, 12] являются: U — множество пользователей; R — множество ролей; P — множество прав доступа к объектам КС; S — множество сессий пользователей; $PA: R \to 2^P$ — функция, задающая для каждой роли множество прав доступа; при этом для каждого права доступа $p \in P$ существует роль $r \in R$ такая что $p \in PA(r)$; $UA: U \to 2^R$ — функция, задающая для каждого пользователя множество ролей, на которые он может быть авторизован; $user: S \to U$ — функция, задающая для каждой сессии пользователя, от имени которого она активизирована; $roles: S \to 2^R$ — функция, задающая для пользователя множество ролей, на которые он авторизован в данной сессии, при этом в каждый момент времени для каждой сессии $s \in S$ выполняется условие $roles(s) \subseteq UA(user(s))$.

Заметим, что могут существовать роли, на которые не авторизован ни один пользователь.

В базовой модели ролевого управления доступом предполагается, что множества *U, R, P* и функции *PA, UA* не изменяются с течением времени.

Множество ролей, на которые авторизуется пользователь в течение одной сессии, модифицируется самим пользователем. При этом отсутствуют механизмы, позволяющие одной сессии активизировать другую сессию. Все сессии активизируются только пользователем.

Для обеспечения возможности большего соответствия реальным КС, каждый пользователь которых занимает определенное положение в служебной иерархии, на множестве ролей реализуется иерархическая структура.

Определение 1. Иерархией ролей в базовой модели ролевого управления доступом называется заданное на множестве ролей *R* отношение частичного порядка «<». При

этом по определению выполняется условие: для пользователя $u \in U$, если роли $r, r' \in R, r \in UA(u)$ и $r' \le r$, то $r' \in UA(u)$.

Таким образом, наряду с данной ролью пользователь должен оыть авторизован на все роли, в иерархии ее меньшие.

Отношение частичного порядка на множестве ролей не обязательно задает на нем решетку.

Другим важным механизмом базовой модели ролевого управления доступом являются ограничения, накладываемые на множества Ролей, на которые может быть авторизован пользователь или на которые он авторизуется в течение одной сессии. Данный механизм также необходим для широкого использования ролевого управления доступом, так как обеспечивает большее соответствие используемым в существующих КС технологиям обработки информации.

Дадим определения для ряда распространенных видов ограничений.

Определение 2. В базовой модели ролевого управления доступом заданы ограничения статического взаимного исключения ролей или прав доступа, когда выполняются условия:

- $R = R_1 \cup ... \cup R_n$, где $R_i \cap R_j = \varnothing$ для $1 \le i < j \le n$, $|UA(u) \cap R_i| \le 1$ для $u \in U, i \in 1,2,...,n$;
- $P = P_1 \cup ... \cup P_m$, где $P_i \cap P_j = \varnothing$ для $1 \le i < j \le n$, $|PA(p) \cap P_i| \le 1$ для $p \in U, i \in 1,2,...,m$.

Множество ролей и множество прав доступа разделяются на непересекающиеся подмножества. При этом каждый пользователь может обладать не более чем одной ролью из каждого подмножества ролей, а каждая роль не более чем одним правом доступа из каждого подмножества прав доступа.

Определение 3. В базовой модели ролевого управления доступом задано ограничение динамического взаимного исключения ролей, когда выполняются условия:

- $R = R_1 \cup ... \cup R_n$, где $R_i \cap R_j = \varnothing$ для $1 \le i < j \le n$;;
- $|roles(s) \cap R_i| \le 1$ для $s \in S, i \in 1,2,...,n$.

Множество ролей разделяется на непересекающиеся подмножества. При этом в каждой сессии пользователь может обладать не более чем одной ролью из каждого подмножества ролей.

Определение 4. В базовой модели ролевого управления доступом заданы статические количественные ограничения на обладание ролью или правом доступа, когда определены две функции:

$$\alpha : R \to N_0; \beta : P \to N_0,$$

где *No* — множество натуральных чисел с нулем, и выполняются условия:

$$|UA^{-1}(r)| \le \alpha(r) \text{ для } r \in R;$$

$$|PA^{-1}(p)| \le \beta(p) \text{ для } p \in P.$$

Для каждой роли устанавливается максимальное число пользователей, которые могут быть на нее авторизованы, а для каждого права доступа устанавливается максимальное число ролей, которые могут им обладать.

Определение 5. В базовой модели ролевого управления доступом задано динамическое количественное ограничение на обладание ролью ние ролью, когда определена функция: $\gamma : R \to N_0$, и выполняется условие:

$$|roles^{-1}(r)| \le \gamma(r) \text{ для } r \in R..$$

Для каждой роли устанавливается максимальное число сессий пользователей, которые могут одновременно быть на нее авторизованы.

Определение 6. В базовой модели ролевого управления доступом заданы статические ограничения необходимого обладания ролью или правом доступа, когда определены две функции:

$$\alpha : R \to 2^R \text{ и } \beta : P \to 2^P,$$

и выполняются условия:

- для $u \in U$, если $r, r' \in R, r \in UA(u)$ и $r' \in \alpha(r)$, то $r' \in UA(u)$;
- для $r \in R$, если $p, p' \in P, p \in PA(r)$ и $p' \in \beta(p)$, то $p' \in PA(r)$.

Для каждой роли для того, чтобы на нее мог быть авторизован пользователь, могут быть определены роли, на которые пользователь также должен быть авторизован. Для каждого права доступа для того, чтобы им обладала роль, могут быть определены права доступа, которыми данная роль также должна обладать.

Определение 7. В базовой модели ролевого управления доступом задано динамическое ограничение необходимого обладания ролью, когда определена функция

$$\gamma : R \to 2^R$$

и выполняется условие: для $s \in S$, если $r, r' \in R, r \in R$ и $roles(s)$ и $r' \in \gamma(r)$, то $r' \in roles(s)$.

Для каждой роли для того, чтобы на нее мог быть авторизован пользователь в некоторой сессии, могут быть определены роли, на которые пользователь также должен быть авторизован в данной сессии.

Общая структура элементов базовой модели ролевого управления доступом имеет вид, показанный на рис. 1.

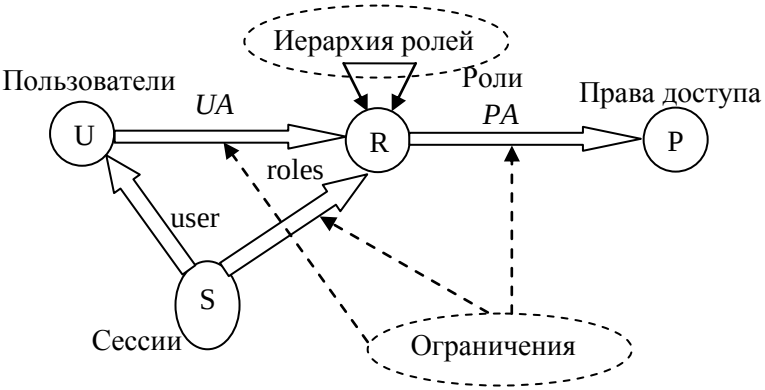


Рис. 1. Структура элементов базовой модели ролевого управления доступом

Модель администрирования ролевого управления доступом

В дополнение к используемым элементам базовой модели в модели администрирования ролевого управления доступом рассматриваются следующие элементы:

AR — множество административных ролей $(AR \cap R = \varnothing)$;

AP — множество административных прав доступа $(AP \cap P = \varnothing)$;

APA: $AR \to 2^{AP}$ — функция, задающая для каждой административной роли множество административных прав доступа, при этом для каждого права доступа $p \in AR$ существует роль $r \in AR$ такая, что $p \in APA($;;

AUA: $U \to 2^{AR}$ — функция, задающая для каждого пользователя множество административных ролей, на которые он может быть авторизован.

Кроме того, переопределяется функция:

$roles : S \to 2^R \cup 2^{AR}$ — функция, задающая для пользователя, множество ролей, на которые он авторизован в данной сессии, при этом в каждый момент времени для каждой сессии $s \in S$ выполняется условие $roles(s) \subseteq UA(user(s)) \cup AUA(user(s))$.

Как и в базовой модели, в модели администрирования ролевого управления доступом реализуются иерархия административных ролей и механизмы ограничений.

Определение 8. Иерархией административных ролей в модели администрирования ролевого управления доступом называется заданное на множестве ролей *AR* отношение частичного порядка «^». При этом выполняется условие: для $u \in U$, если $r, r' \in AR, r \in AUA(u)$ и $r' \le r$, то $r' \in AUA(u)$.

Задачи администрирования могут быть разделены на три группы:

1) администрирование множеств авторизованных ролей пользователей;

2) администрирование множеств прав доступа, которыми обладает роли;

3) администрирование иерархии ролей.

Как правило, каждой административной роли назначают подмножество иерархии ролей, параметры которых данная административная роль позволяет изменять. Рассмотрим каждую из задач администрирования подробнее.

Администрирование множеств авторизованных ролей пользователей

При администрировании множеств авторизованных ролей пользователей изменяются значения функции *UA*, для чего определяются специальные административные роли из множества *AR*. При этом следует задать:

• для каждой административной роли множество ролей, множества авторизованных пользователей которых она позволяет изменять;

• для каждой роли предварительное условие, которому должны соответствовать пользователи, прежде чем они будут включены во множество ее авторизованных пользователей. Рассмотрим пример.

Пример 1. Пусть заданы иерархия ролей (рис. 2, а) и иерархия административных ролей (рис. 2, б).

Минимальная роль в иерархии — служащий *(E)*. Иерархия ролей разработчиков проектов имеет максимальную роль — директор *(DIR)* и минимальную роль — инженер *(ED)*. В организации выполняются работы по двум проектам. В каждом проекте заданы максимальная роль — руководитель проекта *(PL1, PL2* соответственно), минимальная роль — инженер проекта *(E1, E2* соответственно) и несравнимые между собой роли — инженер по производству *(PE1, PE2* соответственно) и инженер по контролю *(QE1, QE2* соответственно).

Иерархия административных ролей состоит из четырех ролей с максимальной ролью — старший офицер безопасности *(SSO)*.

В рассматриваемом примере административная роль *PSO1* позволяет включать во множества авторизованных ролей пользователя роли *PE1, QE1, E1*. При этом для того чтобы любая из перечисленных ролей могла быть включена во множество авторизованных ролей пользователя, он уже должен обладать ролью *ED*.

Для роли $x \in R$ обозначим:

x: U —> {false,true} — функция такая, что по определению для пользователя *u* e *U* справедливо равенство *x(u) = true* тогда и только тогда, когда *x* G *UA(u)*.

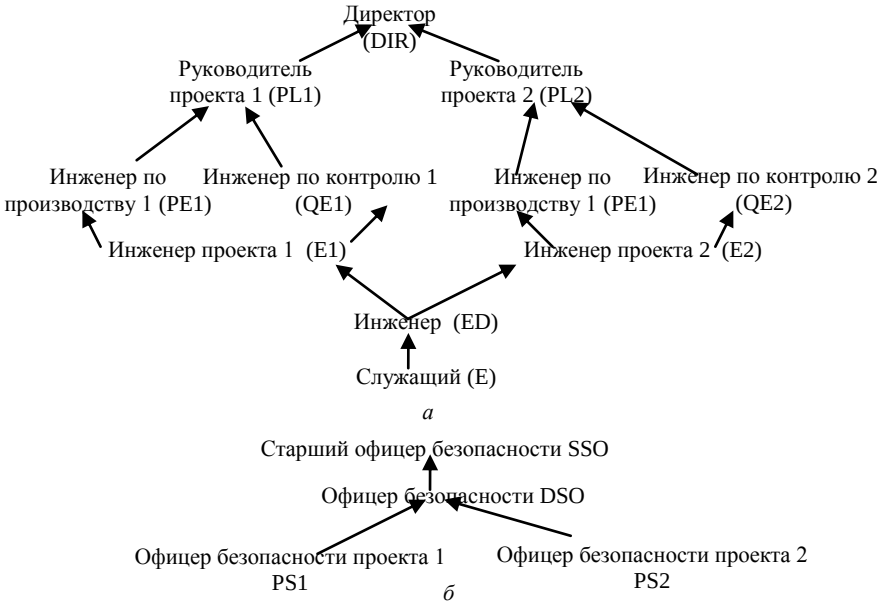


Рис. 2. Пример иерархии ролей (а) и административных ролей (б) пользователей

Определение 9. Предварительным условием для роли $r \in R$ называется функция $c_r : \to \{false, true\}$ такая, что по определению для пользователя $x \in U$ справедливо равенство $c_r(u) = c_r(x_1(u),..,x_k(u))$, где $x_1,...,x_k \in R$ и $c_r(y_1,...,y_k)$ — булева функция от k булевых переменных. При этом роль r может быть включена во множество авторизованных ролей пользователя *u,* когда справедливо равенство $c_r(u)=true$.

Обозначим через *CR* все предварительные условия для ролей из *R.*

Определение 10. Для администрирования множеств авторизованных ролей пользователей на множестве административных ролей задаются функции:

$can-assign_r : AR \to CR \times 2^R$ - функция, задающая для каждой административной роли множество ролей, которые могут быть включены во множество авторизованных ролей пользователя с использованием данной административной роли при выполнении заданных предварительных условий;

$can-revoke_r : AR \to 2^R$ — функция, задающая для каждой административной роли множество ролей, которые могут быть исключены из множества авторизованных ролей пользователя с использованием Данной административной роли.

Как правило, множество ролей, являющееся значением функций $can-assign_r$, или $can-revoke_r$, задается интервалом ролей одного из четырех видов:

$$[x, y] = \{x_i \in R, \text{ где } x \le x_i \text{ и } x_i \le y\};$$
$$(x, y] = \{x_i \in R, \text{ где } x < x_i \text{ и } x_i \le y\};$$
$$[x, y) = \{x_i \in R, \text{ где } x \le x_i \text{ и } x_i < y\};$$
$$(x, y) = \{x_i \in R, \text{ где } x < x_i \text{ и } x_i < y\},$$

где $x, y \notin R$.

Модель мандатного ролевого управления доступом. Защита от угрозы конфиденциальности информации

Ролевое управление доступом является развитием дискреционного управления доступом, в то же время оно является достаточно гибким и, используя механизм ролей, позволяет реализовать требования мандатной политики безопасности, ориентированной на защиту от угрозы конфиденциальности информации.

Рассмотрим подход [13], реализующий мандатное управление доступом на основе базовой модели ролевого управления доступом.

Используем следующие обозначения:

O — множество объектов;

$(L, \leq)$ — решетка уровней конфиденциальности;

$c : U \to L$ — функция уровней доступа пользователей;

$c : O \to L$ — функция уровней конфиденциальности объектов;

$A = \{read, write\}$ — виды доступа.

Будем различать два вида мандатного управления доступом: либеральный и строгий (в смысле Белла-ЛаПадулы).

Определение 11. Доступ $(s, o, r) \in S \times P$ является безопасным для либерального мандатного управления доступом, когда выполняется одной из условий:

- $r = read$ и $c(user(s)) \geq c(o)$ (*ss*-свойство);
- $r = write$ и, если существует доступ $(s, o', read) \in S \times P$, то $c(o) \geq c(o')$ (либеральное *-свойство).

Определение 12. Доступ $(s, o, r) \in S \times P$ является безопасным для строгого мандатного управления доступом, когда выполняется одной из условий:

- $r = read$ и $c(user(s)) \geq c(o)$ (*ss*-свойство);
- $r = write$ и, если существует доступ $(s, o', read) \in S \times P$, то $c(o) = c(o')$ (строгое *-свойство).

Построим систему ролевого управления доступом. Пусть

$R = \{x\_read \mid x \in L\} \cup \{x\_write \mid x \in L\}$ — множество ролей;

$P = \{(o, read) \mid o \in O\} \cup \{(o, write) \mid o \in O\}$ — множество прав доступа.

Зададим на множестве ролей R иерархию, при этом иерархии ролей на множествах $\{x\_read \mid x \in L\}$ и $\{x\_write \mid x \in L\}$ будут независимы.

Определение 13. Иерархией на множестве ролей R в соответствии с требованиями либерального мандатного управления доступом называется отношение частичного порядка «<», где для ролей $r, r' \in R$ справедливо неравенство $r \le r'$, когда выполняется одно из условий:

- $r = x\_read, r' = x'\_read$ и $x \le x'$
- $r = x\_write, r' = x'\_write$ и $x' \le x$.

Определение 14. Иерархией на множестве ролей R в соответствии с требованиями строгого мандатного управления доступом называется отношение частичного порядка «$\le$», где для ролей $r, r' \in R$ справедливо неравенство $r \le r'$, когда выполняется одно из условий:

- $r = x\_read, r' = x'\_read$ и $x \le x'$;
- $r = x\_write, r' = x'\_write$ и $x = x'$ (каждая роль вида *x_write* сравнима только сама с собой).

Определение 15. Модель ролевого управления доступом соответствует требованиям либерального мандатного управления доступом, когда иерархия на множестве ролей R соответствует требованиям *определения 20*, и выполняются ограничения:

- ограничение функции UA — для каждого пользователя $u \in U$ роль $x\_read = \oplus(UA(u) \cap \{y\_read \mid y \in L\}) \in UA(u)$ (здесь $x = c(u)$) и $\{y\_write \mid y \in L\} \subseteq UA(u)$;
- ограничение функции *roles* — для каждой сессии $s \in S$ справедливо равенство

$roles(s) = \{x\_read \mid y \in L, y \le x\} \cup \{x\_write\}$;

- ограничение функции *PA* — должно выполняться:
  - для каждого $x \in L$ доступ (*o, read*) $\in PA(x\_read)$ тогда и только тогда, когда доступ $(o, write) \in PA(x, write)$;
  - для каждого доступа $(o, read) \in P$ существует единственная роль $x\_read : (o, read) \in PA(x\_read)$ (здесь $x = c(o)$).

Определение 16. Модель ролевого управления доступом соответствует требованиям строгого мандатного управления доступом, когда иерархия на множестве ролей *R* соответствует требованиям *определения 21*, и выполняются ограничения:

- ограничение функции *UA* — для каждого пользователя $u \in U$ роль $x\_read = \oplus(UA(u) \cap \{y\_read \mid y \in L\}) \in UA(u)$ (здесь $x = c(u)$) и $\{y\_write \mid y \in L\} \subseteq UA(u)$;
- ограничение функции *roles* — для каждой сессии $s \in S$ справедливо равенство *roles(s) ={x_read, x_write};*
- ограничение функции PA — должно выполняться:
  - для каждого $x \in L$ доступ *(o, read)* $\in PA(x\_read)$ тогда и только тогда, когда доступ $(o, write) \in PA(x, write)$;
  - для каждого доступа $(o, read) \in P$ существует единственная роль $x\_read : (o, read) \in PA(x\_read)$ (здесь *x = c(o)).*

Таким образом, требования соответствия либеральному и строгому мандатному управлению доступом для моделей ролевого управления доступом совпадают во всем, кроме

требований к соответствующей иерархии ролей и ограничениям на функцию *roles*.

В рамках модели мандатного ролевого управления доступом дадим определение информационного потока.

Определение 17. Будем считать, что существует информационный поток от объекта $o \in O$ к объекту $o' \in O$ тогда и только тогда, когда существуют роли $r, r' \in R$, сессия $s \in S$ такие, что $(r, read) \in PA(s), (r', write) \in PA(s)$ и $r, r' \in roles(s)$.

Обоснуем, что в модели ролевого управления доступом, соответствующей требованиям либерального или строгого мандатного управления доступом, невозможна реализация запрещенных информационных потоков от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности.

Теорема 1. Если модель ролевого управления доступом соответствует требованиям либерального или строгого мандатного управления доступом, то в ней для любых объектов $o, o' \in O$ таких, что $c(o) > c(o')$, невозможно возникновение информационного потока от o к o'.

Защита от угроз конфиденциальности и целостности информации

Модель мандатного ролевого управления доступом в первую очередь ориентирована на обеспечение защиты от угрозы конфиденциальности информации. В то же время возможно доопределение свойств модели с целью анализа систем защиты от двух угроз: целостности информации и конфиденциальности информации.

Используем обозначения модели ролевого управления доступом защиты от угрозы конфиденциальности информации. Также используем обозначения:

$(LI, \leq)$ — решетка уровней целостности информации;

$ci: U \to LI$ — функция уровней целостности пользователей;

$ci: O \to LI$ — функция уровней целостности объектов.

По аналогии с моделью ролевого управления доступом защиты от угрозы конфиденциальности информации, будем различать два вида мандатного контроля целостности информации: либеральный и строгий.

Определение 18. Доступ $(s, o, p) \in S \times P$ является безопасным для либерального мандатного контроля целостности, когда выполняется одно из условий:

- $r = read$ и $ci(user(s)) \leq ci(o)$;
- $r = write$ и, если существует доступ $(s', o', read) \in S \times P$, то $ci(o) \leq ci(o')$.

Определение 19. Доступ $(s, o, p) \in S \times P$ является безопасным для строгого мандатного контроля целостности, когда выполняется одно из условий:

- $r = read$ и $ci(user(s)) \leq ci(o)$;
- $r = write$ и, если существует доступ $(s', o', read) \in S \times P$, то $ci(o) \leq ci(o')$.
-

Рассмотрим иерархию ролей на множестве $RI = \{x_i \_ read \mid x_i \in LI\} \cup \{x_i \_ write \mid x_i \in LI\}$.

Иерархии ролей на множествах $\{x_i \_ read \mid x_i \in LI\}$ и $\{x_i \_ write \mid x_i \in LI\}$ независимы.

Определение 20. Иерархией на множестве ролей *RI* в соответствии с требованиями либерального мандатного контроля целостности называется отношение частичного порядка «≤», где для ролей $r, r' \in R$ справедливо неравенство $r \le r'$, когда выполняется одно из условий:

- $r = x_i\_read, r' = x_i'\_read$ и $x_i' \le x_i$;
- $r = x_i\_write, r' = x_i'\_write$ и $x_i \le x_i'$.

Определение 21. Иерархией на множестве ролей *RI* в соответствии с требованиями строгого мандатного контроля целостности называется отношение частичного порядка «≤», где для ролей $r, r' \in R$ справедливо неравенство $r \le r'$, когда выполняется одно из условий:

- $r = x_i\_read, r' = x_i'\_read$ и $x_i' \le x_i$;
- $r = x_i\_write, r' = x_i'\_write$ и $x_i \le x_i'$ (каждая роль вида x_i*_write* сравнима только сама с собой).

Определение 22. Модель ролевого управления доступом соответствует требованиям либерального мандатного контроля целостности, когда иерархия на множестве ролей *RI* соответствует требованиям определения 27 и выполняются ограничения:

- ограничение функции *UA* — для каждого пользователя $u \in U$ роль $x_i\_read = \oplus(UA(u) \cap \{y_i\_read \mid y_i \in LI\}) \in UA(u)$ (здесь $x_i = c_i(u)$ и $\{y_i\_write \mid y_i \in LI\} \subset UA(u)$;
- ограничение функции *roles* — для каждой сессии $s \in S$ справедливо равенство $roles(s) = \{y_i\_read \mid y_i \in LI, y_i \ge x_i\} \cup \{x_i\_write\}$;
- ограничение функции *PA* — должно выполняться:

- для каждого $x_i \in LI$ доступ $(o, read) \in PA(x_i\_read)$ тогда и только тогда, когда доступ $(o, write) \in PA(x_i\_write)$;
- для каждого доступа $(o, read) \in P$ существует единственная роль $x_i\_read : (o, read) \in PA(x_i\_read)$ (здесь $x_i = c_i(o)$).

Определение 23. Модель ролевого управления доступом соответствует требованиям строгого мандатного контроля целостности, когда иерархия на множестве ролей *RI* соответствует требованиям *определения 28* и выполняются ограничения:

- ограничение функции *UA* — для каждого пользователя $u \in U$ роль $x_i\_read = \oplus(UA(u) \cap \{y_i\_read \mid y_i \in LI\}) \in UA(u)$ (здесь $x_i = c_i(u)$) и $\{y_i\_write \mid y_i \in LI\} \subseteq UA(u)$;
- ограничение функции *roles* — для каждой сессии $s \in S$ справедливо равенство $roles(s) = \{x_i\_read, x_i\_write\}$;
- ограничение функции *PA* — должно выполняться:
  - тогда, для каждого $x_i \in LI$ доступ $(o, read) \in PA(x_i\_read)$ тогда и только когда доступ $(o, write) \in PA(x_i\_write)$;
  - для каждого доступа $(o, read) \in P$ существует единственная роль $x_i\_read : (o, read) \in PA(x_i read)$ (здесь $x_i = c_i(o)$).

Построим систему мандатного ролевого управления доступом, ориентированную на защиту от угроз конфиденциальности и целостности информации. Пусть

$R = \{x_i\_read \mid x \in L\} \times \{x_i\_read \mid x_i \in LI\} \cup \{x_i\_write \mid x \in L\} \times \{x_i\_write \mid x_i \in LI\}$ — множество ролей.

Зададим на множестве ролей R иерархию, при этом возможно произвольное сочетание иерархий ролей либерального или строгого мандатного управления доступом с либеральным или строгим контролем целостности. Иерархии ролей на множествах $\{x\_read | x \in L\} \times \{x\_read | x_i \in LI\}$ и $\{x\_write | x \in L\} \times \{x\_write | x_i \in LI\}$ независимы.

В качестве примера рассмотрим требования либерального мандатного управления доступом и контроля целостности.

Определение 24. Иерархией на множестве ролей R в соответствии с требованиями либерального мандатного управления доступом и контроля целостности называется отношение частичного порядка «$\leq$», где для

$$r = (c, ri), r' = (c', ri') \in R, rc, rc' \in \{x\_read | x \in L\} \cup \{x\_write | x \in L\}, ri, ri' \in \{x\_read | x_i \in LI\} \cup \{x\_write | x_i \in LI\},$$

справедливо неравенство $r \leq r'$, когда $rc \leq rc'$ в иерархии ролей либерального мандатного управления доступом (в соответствии с *определением 20*) и $ri \leq ri'$ в иерархии ролей либерального контроля целостности (в соответствии с *определением 27*).

Определение 25. Модель ролевого управления доступом соответствует требованиям либерального мандатного управления доступом и контроля целостности, когда иерархия на множестве ролей R соответствует требованиям *определения 31* и выполняются ограничения:

- ограничение функции UA — для каждого пользователя $u \in U$ роль

$$(x\_read, x_i\_read) \in \oplus(UA(u) \cap (\{x\_read | y \in L\} \times \{y\_read | y_i \in LI\}) \in UA(u))$$

(здесь $x = c(u), x_i = c_i(u)$) и

$$\{(y\_write \mid y \in L\} \cup \{(y_i write \mid y_i \in LI\} \subseteq UA;$$

- ограничение функции *roles* — для каждой сессии $s \in S$ справедливо равенство

roles(s)=

$$\{(y\_read, y_i\_read) \mid y \in L, y_i \in LI, y \le x, y_i \ge x_i\} \cup \{(x\_write, x_i write)\};$$

- ограничение функции PA — должно выполняться:
  - для каждых $x \in L, x_i \in LI$, доступ $(o, read) \in PA(x\_read, x_i\_read)$ тогда и только тогда, когда доступ $(o, write) \in PA(x\_write, x_i\_write)$;
  - для каждого доступа $(o, read) \in P$ существует единственная роль $(x\_read, x_i\_read): (o, read) \in PA(x\_read, x_i\_read)$ (здесь $x = c(o), x_i = c_i(0)$).

Для решеток уровней конфиденциальности $(L, \le) = (LS, HS)$ и уровней целостности $(LI, \le) = (LI, HI)$ на рис. 3 представлены иерархии ролей для четырех возможных сочетаний иерархий ролей либерального мандатного управления доступом с либеральным мандатным контролем целостности

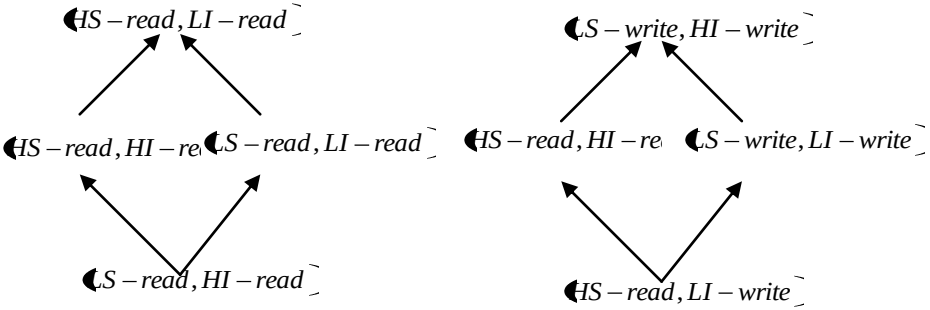


Рис. 3. Либеральное мандатное управление доступом и мандатный контроль целостности

Типовые задачи

Задание 1. Пусть в некоторой системе, построенной на основе модели мандатного ролевого управления доступом, субъект с высоким текущим уровнем доступа может назначать любые права доступа к сущности некоторой роли, доступной в качестве текущей субъекту с низким уровнем доступа. Постройте пример реализации информационного потока по времени от сущности с высоким уровнем конфиденциальности к сущности с низким уровнем конфиденциальности с использованием прав доступа такой роли.

Решение. Пусть субъекту-процессу S_{high} (с высоким текущим уровнем доступа) необходимо передать один бит данных субъекту-процессу s_{low} (с низким текущим уровнем доступа). Пусть существует роль r, на которую могут авторизоваться сессии S_{high} и S_{low} может администрировать права доступа роли r к сущности-файлу f_{low}. Тогда в согласованный момент времени субъектами-процессами S_{high} и S_{low} может быть реализована следующая последовательность действий (рис. 4).

Шаг 1. Если субъекту-процессу S_{high} необходимо передать 0, он ничего не предпринимает, когда надо передать 1, он дает роли r право доступа *read* к f_{low}

Шаг 2. Субъект-процесс s_{low} запрашивает доступ на чтение *read* к сущности-файлу f_{low}. Если он запрещен, то передан 0, иначе — передана 1.

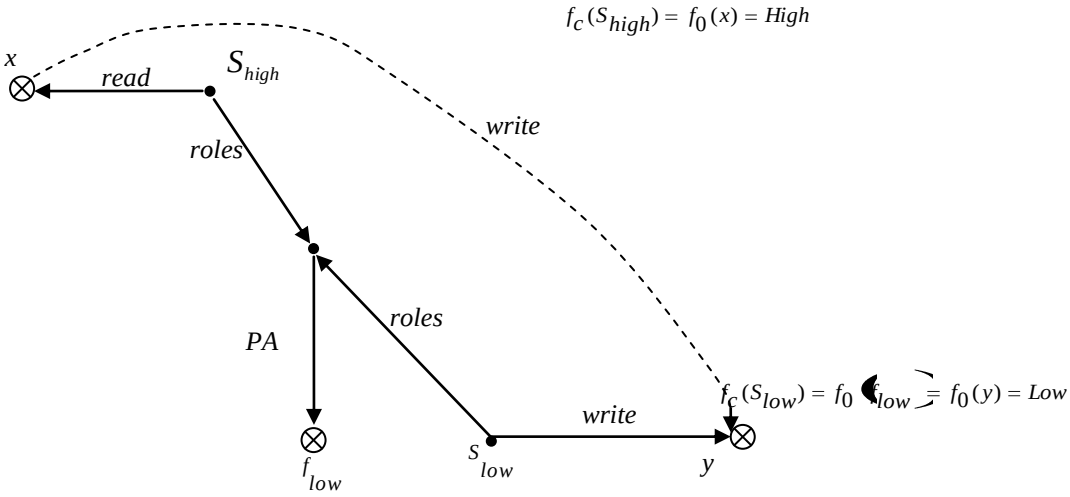


Рис. 4. Илюстрация решения задания 1

Задание 2. Постройте пример иерархии индивидуальных ролей учетных записей пользователей для случая, когда $LC = (\{1, 2\}, \{a, b\})$ (решетка уровней конфиденциальности из двух элементов линейной шкалы и двух неиерархических категорий, задаваемых маской из двух битов).

Решение. Построим иерархию индивидуальных ролей учетной записи пользователя $u \in U$ такой, что $f_u(u) = (1,11)$ и $i_u(u) = i\_high$ (рис. 5).

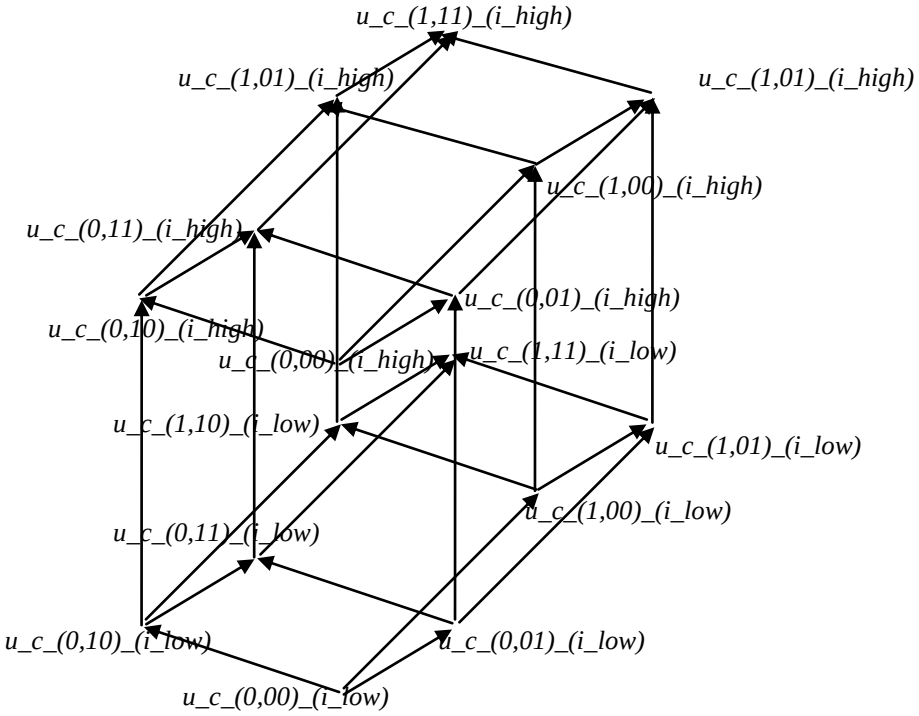


Рис. 5. Илюстрация решения задания 2

Задачи для самостоятельного решения

1. Докажите, что при соответствии модели ролевого управления доступом требованиям либерального или строгого мандатного управления доступом для каждого доступа *(o, write)* $\in P$ существует единственная роль x_write такая, что $(o, write) \in PA(x\_write)$ здесь $x = c(o)$.

2. Каким образом в определениях либерального или строгого мандатного управления доступом модели ролевого управления доступом реализованы *ss*-свойство и *-свойство, определенные в классической модели Белла-ЛаПадулы?

3. Постройте графы иерархии ролей для модели мандатного ролевого управления доступом для решеток уровней конфиденциальности $(L, \leq) = \{S, MS, HS\}$ и уровней целостности $(L, \leq) = \{I, MI, HI\}$.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Каковы основные недостатки классической модели Белла-ЛаПадулы?

2. Какой вид политики управления доступом используется в качестве основы автоматной модели безопасности информационных потоков?

3. Какие основные проблемы определения правил изменения иерархии ролей рассматриваются в модели администрирования ролевого управления доступом?

4. Какие основные угрозы безопасности информации рассматриваются в теории компьютерной безопасности?

5. Приведите примеры наиболее распространенных в современных ОС и СУБД запрещенных информационных потоков по памяти и по времени.

6. Какие основные виды политик безопасности рассматриваются в теории компьютерной безопасности?

7. В чем отличие структуры ядра безопасности в классических моделях безопасности КС от структуры ядра безопасности в субъектно-ориентированной модели ИПС?

8. Сформулируйте основные отличия политик безопасного администрирования и абсолютного разделения административных и пользовательских полномочий.

9. Сформулируйте задачи реализации и контроля выполнения правил политики безопасности.

10. Приведите классификацию основных формальных моделей политик безопасности.

11. В чём заключаются базовые принципы построения формальных моделей управления разграничения и контроля доступа к информации?

12. Каковы условия применимости классической модели Белла-ЛаПадулы в зависимости от уровня конфиденциальности объекта?

13. Перечислите базовые элементы классической модели мандатного управления доступом (Белла-ЛаПадулы).

14. Какие изменения в состояние системы разрешается вносить по запросу в модели мандатного управления доступом?

15. Какие информационные потоки, условия возникновения которых анализируются в КС с мандатным управлением доступом, являются запрещенными?

16. Могут ли и каким образом правила дискреционного управления доступом быть использованы в КС с мандатным управлением? Справедливо ли обратное утверждение?

17. Охарактеризуйте ролевое управление доступом с точки зрения связи с дискреционным управлением.

18. Перечислите и дайте краткую характеристику элементам базовой модели ролевого управления доступом (Role-Based Access Control).

19. Что подразумевается под либеральным и строгим видами мандатного ролевого управления доступом?

20. Как организован либеральный и строгий виды контроля целостности при мандатном доступе?

ЗАКЛЮЧЕНИЕ

Основное внимание в методических указаниях уделено формальному описанию основных политик управления доступом. Рассмотрены так же технические аспекты управления ИБ к которым отнесены управление логическим доступом пользователей к активам организации, управление защищенной передачей данных и операционной деятельностью, разработкой и обслуживанием информационных систем с учетом требований к их ИБ, управление конфигурациями, изменениями и обновлениями в активах организации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Девянин, П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах [Текст] / П. Н. Девянин. — М.: Радио и связь, 2006. — 176 с. .
2. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Текст]: учеб. пособие для вузов; 2-е изд., испр. и доп. / П. Н. Девянин. – М.: Горячая линия – Телеком, 2013. – 338 с.
3. Девянин, П. Н. Теоретические основы компьютерной безопасности [Текст]: учеб. пособие для вузов / П. Н. Девянин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков. – М.: Радио и связь, 2000. – 192 с. .
4. Зегжда, Д. П. Основы безопасности информационных систем [Текст] / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2000. – 452 с.
5. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью [Текст]: учеб. пособие для ВУЗов; 2-е изд., испр. / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – М.: Горячая линия – Телеком, 2014. – 214 с.
6. Носов, В. А. Основы теории алгоритмов и анализа их сложности. Курс лекций [Текст] / В. А. Носов. – М: МГУ, 1992. – 140 с.
7. Фороузан, Б. А. Криптография и безопасность сетей [Текст] / Б. А. Фороузан. – М.: БИНОМ. Лаборатория знаний, 2010. – 784 с.
8. Bell, D. E. Secure Computer Systems: Unified Exposition and Multics Interpretation [Text] / D. E. Bell, L. J. LaPadula. – Bedford, Mass.: MITRE Corp., 1976. – MTR-2997 Rev. 1.
9. Frank, J. Extending The Take-Grant Protection System [Text] / J. Frank, M. Bishop // Department of Computer Science. — University of California at Davis, 1984.
10. McLean, J. The Specification and Modeling of

Computer Security [Text] / J. McLean //Computer. 1990. Vol. 23, № 1. Sandhu R. Rationale for the RBAC96 family of access control models// Proceeding of the 1st ACM Workshop on Role-Based Access Control. - ACM, 1997.

11. Sandhu, R. Role-Based Access Control, Advanced in Computers [Text] / R. Sandhu // Academic Press. 1998. Vol. 46.

12. Sandhu, R. The typed access matrix model [Text] / R. Sandhu // In Proceeding of the IEEE Symposium on Research in Security and Privace, Oakland, CA, May 1992. — P. 122-136.

13. Управление ключами шифрования и безопасность сети: Информация [Электронный ресурс] – Режим доступа: http://www.intuit.ru/studies/courses/553/409/info

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к практическим занятиям № 5–6 по дисциплине
«Управление информационной безопасностью»
для студентов специальности
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Составитель
Разинкин Константин Александрович

В авторской редакции

Подписано к изданию 28.11.2014
Уч.-изд. л. 3,1

ФГБОУ ВПО «Воронежский государственный
технический университет»
394026 Воронеж, Московский просп., 14