S.A. Lapin
Altai State University, 656049, Barnaul, Lenin Ave, 61,
e-mail: lapinsa567@gmail.com

Access control model to the systems containing the interchangeable objects

Keywords: mathematical models of security, access control, interchangeable objects.
This article describes the access control model which extends TBAC. The model is applied in the systems containing the interchangeable objects. Model elements and properties, are defined formally.

С.А. Лапин
Алтайский государственный университет, 656049, Барнаул, пр. Ленина, 61,
e-mail: lapinsa567@gmail.com

МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА ДЛЯ СИСТЕМ, СОДЕРЖАЩИХ РАВНОЗНАЧНЫЕ ОБЪЕКТЫ

Ключевые слова: математические модели безопасности, контроль доступа, равнозначные объекты
В настоящей статье представлена модель контроля доступа, расширяющая TBAC. Модель применяется в системах, содержащих равнозначные объекты. Формально определены элементы модели и её свойства.

При построении системы обеспечения информационной безопасности, важным ее компонентом является система разграничения доступа, цель которой - предотвращение несанкционированного доступа. Широко применяется модель контроля доступа на основе ролей (RBAC) [1-3], с помощью которой возможно выполнить тонкую настройку правил контроля доступа [4]. Однако применение классической модели RBAC в динамических системах является затруднительным [5-7]. Такая проблема разрешается путем использования модели TBAC [8], в которой права доступа предоставляются в зависимости от контекста задачи [9].

В существующих моделях разграничения доступа предполагается, что одна и та же задача будет решена субъектом системы через использование одного множества объектов, к которому ему предоставляется доступ. Однако такие модели не учитывают, что в системе могут присутствовать равнозначные объекты, которые имеют одинаковые функциональные возможности, но различные характеристики. Такие объекты по некоторому признаку, например по функциональности, объединяются в несколько подмножеств множества объектов, которые назовем группами равнозначных объектов. Как правило, это свойственно системам, имеющим динамический характер функционирования, и могут быть ориентированы на выполнение некоторого множества задач, для решения которых могут применяться определенные требования.

Примером такой системы может являться учреждение здравоохранения, где субъектами системы являются врачи, предоставляющие услуги лечения пациента, а объектами - лекарственные препараты. При лечении одного и того же заболевания в распоряжение врача могут предоставляться различные препараты, имеющие одинаковые функциональные возможности (обезболивающие, успокоительные и пр.), но различные характеристики (стоимость, влияние на организм, побочные эффекты, привыкание и др.). Поэтому к процессу лечения пациента применяются определенные требования. В подобного рода системах, от того каким объектом при решении задачи воспользуется субъект, зависит как безопасность решения задачи, так и безопасность всей системы в целом.

В работе [10] неформально описывается модель, учитывающая перечисленные особенности. Однако, требуется её формальное определение. Т.о. целью представленной

работы является формальное описание модели контроля доступа, удовлетворяющей следующим условиям:

1. права доступа должны предоставляться субъектам на основе решаемых ими задач;
2. каждый субъект при решении поставленной перед ним задачи, должен иметь минимальному множеству объектов системы, позволяющих выполнить поставленную перед ним задачу. Другими словами, при наличии в системе равнозначных объектов, доступ при решении каждой задачи должен предоставляться только к одному объекту из каждой группы;
3. выполнение операций администрирования (таких как добавление/удаление субъектов, объектов, задач) в системе должно приводить к минимальным изменениям политики безопасности.

Предлагаемая модель состоит из следующих элементов:

S – множество субъектов;

T – множество задач;

O – множество объектов;

$G = \{g_i\} \mid \forall g_i \subseteq O$ и $\forall g_i, g_j \in G$ выполняется $g_i \cap g_j = \varnothing$ – множество групп объектов. При этом $g_1 \cup g_2 \cup ... g_n = O$, где $n = |G|$;

R – множество видов доступа (например $read, write, execute$);

$P = 2^{G \times R}$ – множество операций над группами объектов;

D – множество требований;

L – множество решеток уровней требований и свойств объектов;

$ST : S \to 2^T$ – функция, определяющая для каждого субъекта множество задач, которые он может выполнять;

$TP : T \to 2^P$ – функция, определяющая для каждой задачи права доступа;

$TD : T \to 2^D$ – функция, определяющая для каждой задачи множество требований, которые должны быть выполнены при ее выполнении;

$DL : D \to L, \forall d \in D \ \exists!(l_d, \leq) \in L : DL(d) = (l_d, \leq)$ – функция, задающая для каждого требования решетку, на которой определяется его уровень;

$f_d : d \to (l_d, \leq) \cup \{none\}, DL(d) = (l_d, \leq)$ – функция, определяющая уровень требования, где $none$ означает, что уровень требования не определён;

$OL : O \to L, \forall o \in O \ \exists!(l_d, \leq) \in L : OL(o) = (l_d, \leq)$ – функция, задающая для каждого объекта решетку его свойств. При этом, если $\forall o_i, o_j \in g$ верно $OL(o_i) = OL(o_j)$;

$f_o : o \to (l, \leq), OL(o) = (l, \leq)$ – функция, определяющая свойство объекта;

Определение 1: Требование $d \in D$ называется значимым для объектов из группы $g \in G$, если $\forall o \in g$ выполняется равенство $DL(d) = OL(o)$.

$DO \subset D \times O \mid \forall (d, o) \in DO \ \ DL(d) = OL(o)$ – множество пар значимых требований и объектов;

Для любой пары $(d, o) \in DO$ определим двойку функций $(f_d, f_o) \in DL(d) \times DO(o)$, определяющих уровень требования $d \in D$ и уровень свойств объекта , для которого такое требование является значимым.

Тогда $(s, t, (f_d, f_o)) \in Y \subset S \times T \times (DL(d) \times DO(o))$, где $(d, o) \in DO$ — тройка, определяющая уровень требования $d \in D$ к объекту $o \in O$, при решении задачи $t \in T$ субъектом $s \in S$.

$B \subseteq 2^{S \times O \times R}$ – множество возможных множеств текущих доступов в системе;

$CT \subseteq 2^{S \times T}$ – множество текущих задач в системе;

Структура элементов предлагаемой модели представлена на рис 1.

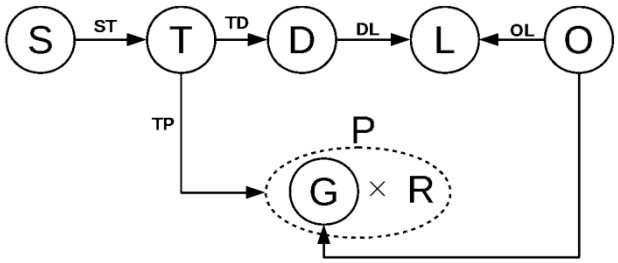

Рисунок 1 Структура элементов модели

Определение 2: Пусть определены: множества субъектов S, объектов O, задач T, групп объектов G, видов доступа R, операций P, требований D, решеток требований и свойств объектов L, множество доступов B, а так же функции задающие задачи для субъектов ST, права доступа задач TP, требования для задач TD, решетки для требований DL, решетки свойств для объектов OL, а также функция Y. Тогда $V = (S, O, T, G, R, P, D, L, ST, TP, TD, DL, OL, CT, B, Y)$ – состояние системы;

Введем обозначения:

Q – множество команд в системе;

$W : Q \times V \to V$ – функция переходов, где $W(q, v) = v^*$ означает, что система по команде $q \in Q$ из состояния v перешла в состояние v^*;

Определение 3: Под системой будем понимать конечный автомат $\sum(Q, V^*, W, z_0)$ – где V^* - множество всех возможных состояний системы, где z_0 – начальное состояние системы.

Предположение 1: В модели предполагается, что множества S, T, O, G, R, P, D, L и функции TP, TD, DL, OL не меняются в процессе функционирования системы.

Принимая во внимание предположение 1, будем использовать сокращенное обозначение для состояния системы $V = (CT, B, Y)$;

В модели предполагается, что в состоянии z_0:

- $CT = \varnothing$ – выполняемые задачи в данный момент времени отсутствуют;
- $B = \varnothing$ субъекты не имеют прав доступа на объекты системы;
- $\forall (d, o) \in DO \ (f_d = none, f_o) => \forall (s, t, (f_d, f_o)) \in Y$ верно $(s, t, (f_d = none, f_o))$ – уровни требований не определены.

В модели рассматриваются следующие запросы, входящие во множество Q:

- $set\_demad(s, t, d, val)$ – запрос, задающий уровень для требования $d \in D$ при выполнении задачи $t \in T$ субъектом $s \in S$;
- $start\_task(s, t)$ – запрос запуска процесса решения задачи $t \in ST(s)$ субъектом $s \in S$;
- $stop\_task(s)$ – запрос прекращения решения задач субъектом $s \in S$.

Безопасность системы определяется с помощью четырех свойств:

- d -свойства (свойство требования);
- t -свойства (свойство задачи);
- f -свойства (свойство полноты);
- !-свойства (свойство единственности);

Определение 4: Объект $o \in O$ называется соответствующим значимому требованию $d \in D$ относительно (f_d, f_o), если $f_d = f_o$.

Определение 5: Объект $o \in O$ называется минимально удаленным от уровня значимого требования относительно $(f_d \neq none, f_o)$, когда $f_o < f_d$ и $o' \in O \mid o', o \in g$, для которого выполняется $f_o < f_{o'} \leq f_d$.

Определение 6: Объект $o \in O$ обладает d-свойством относительно (f_d, f_o), если $o \in O$ соответствует значимому требованию $d \in D$ или минимально удален от него.

Определение 7: Доступ $(s,o,r) \in S \times O \times R$ обладает d-свойством относительно $(s,t,(f_d, f_o)) \in Y$, когда объект $o \in O$ обладает d-свойством.

Определение 8: Состояние системы $(CT, B, Y) \in V$ обладает d-свойством, когда выполняется одно из условий:

- если $CT \neq \varnothing$, то каждый элемент $(s,o,r) \in B$ обладает d-свойством относительно $(s,t,(f_d, f_o)) \in Y$;
- если $CT = \varnothing$, то $B = \varnothing$.

Обладание системой в каждом ее состоянии d-свойством означает, что любой субъект $s \in S$ в каждый момент времени при выполнении задачи $t \in T$ имеет доступ к объектам, которые максимально могут удовлетворить предъявляемые требования.

Определение 9: Доступ $(s,o,r) \in S \times O \times R$ обладает t-свойством относительно $(s,t) \in S \times T$, когда выполняются два условия:

1. $t \in ST(s)$;
2. $\exists g \in G \mid o \in g$ и $(g,r) = p \in TP(t)$.

Определение 10: Состояние системы $(CT, B, Y) \in V$ обладает t-свойством, когда выполняется одно из условий:

- если $CT \neq \varnothing$, то каждый элемент $(s,o,r) \in B$ обладает t-свойством относительно элемента $(s,t) \in CT$;
- если $CT = \varnothing$, то $B = \varnothing$.

Обладание системой в каждом ее состоянии t-свойством означает, что каждый доступ, который присутствует в данном состоянии системы, относится к выполнению задачи $t \in T$ субъектом $s \in S$.

Определение 11: Состояние системы $(CT, B, Y) \in V$ обладает f-свойством, когда выполняется одно из условий:

- если $CT \neq \varnothing$, то $\forall (s,t) \in CT$ и $\forall g \in G \mid (g,r) = p \in TP(t)$, верно что $\exists! o \in g \mid (s,o,r) \in B$;
- если $CT = \varnothing$, то $B = \varnothing$.

Обладание системой в каждом её состоянии f-свойством означает, что каждый субъект в любой момент времени, при выполнении задачи, имеет все необходимые доступы к объектам

Определение 12: Множество текущих задач CT обладает !-свойством, когда выполняется условие: $\forall s \in S$ верно $| CT \cap (s \times T) | \leq 1$.

Определение 13: Состояние системы $(CT, B, Y) \in V$ обладает !-свойством, когда CT обладает !-свойством.

Обладание системой в каждом ее состоянии !-свойством означает, что любой субъект $s \in S$ в каждый момент времени может выполнять не более одной задачи $t \in T$.

Определение 14: Состояние системы $(CT, B, Y) \in V$ называется безопасным, когда оно обладает одновременно d-свойством, f-свойством, t-свойством и !-свойством;

Определение 15: Система $\sum(Q, V^*, W, z_0)$ называется безопасной, когда каждое ее состояние безопасно;

В модели определено множество объектов системы. При этом объекты по некоторому признаку, например по функциональности, объединяются, образуя не пересекающееся множество групп G. Операции, которые возможно выполнять над группой в процессе решения задачи, определяет функция TP. Если над группой $g \in G$ возможно выполнить операцию $p \in P$, то такую операцию можно выполнить над любым объектом $o \in G$.

В модели представлено множество требований D. Отображение TD ставит в соответствие каждой задачи подмножество требований, которые должны быть выполнены при ее выполнении. Каждое требование может иметь различный уровень. Поэтому для каждого требования существует своя решетка уровней $(l_d, \leq) \in L$. Уровень требования определяется значением функции f_d.

Каждый объект из каждой группы имеет уровень характеристик своих свойств относительно некоторого требования. Уровень таких свойств отображается на решетку уровня требования функцией f_o. В одной группе не может существовать несколько объектов, имеющих одинаковый уровень характеристик. В группе, может не существовать объекта с уровнем своих характеристик, совпадающий с требуемым уровнем значимого для них требования. В таком случае из группы предоставляется доступ на объект, уровень свойств которого минимально отличается от требуемого и не превышает его.

Состояние системы может изменяться только путем применения в ней трех команд. Команда $set\_demad(s, t, d, val)$ устанавливает значение функции f_d для требования $d \in D$. Значение этой функции определяет, к какому объекту будет предоставлен доступ субъекту $s \in S$ при выполнении задачи $t \in T$. Изменение уровня требования в процессе выполнения задачи субъектом, не влияет на его текущие доступы в системе. $start\_task(s, t)$ запускает процесс решения задачи $t \in ST(s)$ субъектом $s \in S$. При выполнении такой команды в системе субъекту предоставляются все необходимые доступы, которые удовлетворяют обозначенным четырем свойствам. $stop\_task(s)$ прекращает выполнение всех задач в системе субъектом $s \in S$. Т.к. из свойства !-свойства следует, что в системе может выполняться только одна задача одним субъектом, то при выполнении данной команды, система переходит в состояние, из которого исключены все доступы субъекта s. Стоит обратить внимание, что важен порядок использования данных команд: не допускается применение команды $start\_task(s, t)$ если в системе субъект $s \in S$ уже выполняет какую-либо задачу.

В настоящей статье предложена и формально определена модель, расширяющая TBAC. Формально определены множество элементов, из которых состоит модель, а так же свойства представленной модели, описывающие безопасность системы.

Основной особенностью представленной модели, является то, что в ней учитывается наличие равнозначных объектов в системе. Права субъектам выделяются в зависимости от требований, предъявляемых к процессу решения задачи. При этом, как и в TBAC, права пользователю предоставляются только на период времени, в который он выполняет поставленную пред ним задачу, т.е. права доступа не являются постоянными, а меняются с учетом специфики задач. Стоит отметить, что в зависимости от требований, для решения одной и той же задачи, субъекту могут предоставляться различные доступы к

равнозначным объектам. Модель предоставляет механизм, позволяющий выделить минимальные права доступа субъектам системы к равнозначным объектам.

СПИСОК ЛИТЕРАТУРЫ:

1. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. Пособие для вузов. – 2-е изд., испр. и доп. – М.: Горячая линия-Телеком, 2013.
2. Sandhu R. Role-based Access Control // Advances in Computers. 1998. V. 46. P. 237.
3. Ferraiolo D., Sandhu R., Gavrila S., Kuhn R., Chandramouli, R. Proposed NIST Standard for Role-based Access Control // ACM Trans. Inf. Syst. Secur 2001. V. 4. No 3. P. 224.
4. Головин А.В., Поляков В.В., Лапин С.А. Ролевое разграничение доступа для автоматизированного рабочего места пользователя при оперативном удаленном управлении конфиденциальной информацией// Доклады Томского государственного университета систем управления и радиоэлектроники. 2010. №1. С. 143.
5. Лепешкин О.М., Харечкин П.В. Анализ моделей разграничения доступа, реализованных в современных социотехнических системах// Инфо-коммуникационные технологии. 2008. Т.6. №2. С. 91.
6. Zhang C., Hu Y., Zhang G. Task-role based dual system access control model// IJCSNS International Journal of Computer Science and Network Security. 2006. V. 6. №7 P. 211.
7. Freudenthal E., Pesin T., Port L., Keenan E., Karamcheti V. dRBAC: distributed rolebased access control for dynamic coalition environments// Proceedings of the 22 Nd International Conference on Distributed Computing Systems (ICDCS'02). 2002. P. 411.
8. Thomas R. K., Sandhu R. S. Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management// Proceedings of the IFIP TC11 WG11.3 Eleventh International Conference on Database Securty XI: Status and Prospects. 1997. P. 166.
9. Cvrˇcek D. Access Control in Workflow Systems// MOSIS'99 Proceedings. Roˇznov pod Radhoˇstˇem. 1999. P 93.
10. Лапин С. А. Неформальное описание модели разграничения доступа на основе задач с учетом требований к их выполнению// Проблемы правовой и технической защиты информации. 2015. № 3. С. 52.

REFERENCES:

1. Devyanin P.N. Modeli bezopasnosti kompyuternyx sistem. Upravlenie dostupom i informacionnymi potokami: ucheb. Posobie dlya vuzov. – 2-e izd., ispr. i dop. – M.: Goryachaya liniya-Telekom, 2013.
2. Sandhu R. Role-based Access Control // Advances in Computers. 1998. V. 46. P. 237.
3. Ferraiolo D., Sandhu R., Gavrila S., Kuhn R., Chandramouli, R. Proposed NIST Standard for Role-based Access Control // ACM Trans. Inf. Syst. Secur 2001. V. 4. No 3. P. 224.
4. Golovin A.V., Polyakov V.V., Lapin S.A. Rolevoe razgranichenie dostupa dlya avtomatizirovannogo rabochego mesta polzovatelya pri operativnom udalennom upravlenii konfidencialnoj informaciej// Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. 2010. No 1. P. 143.
5. Lepeshkin O.M., Xarechkin P.V. Analiz modelej razgranicheniya dostupa, realizovannyx v sovremennyx sociotexnicheskix sistemax// Info-kommunikacionnye texnologii. 2008. V.6. No 2. P. 91.
6. Zhang C., Hu Y., Zhang G. Task-role based dual system access control model// IJCSNS International Journal of Computer Science and Network Security. 2006. V. 6. №7 P. 211.
7. Freudenthal E., Pesin T., Port L., Keenan E., Karamcheti V. dRBAC: distributed rolebased access control for dynamic coalition environments// Proceedings of the 22 Nd International Conference on Distributed Computing Systems (ICDCS'02). 2002. P. 411.
8. Thomas R. K., Sandhu R. S. Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management// Proceedings of the IFIP TC11 WG11.3 Eleventh International Conference on Database Securty XI: Status and Prospects. 1997. P. 166.
9. Cvrˇcek D. Access Control in Workflow Systems// MOSIS'99 Proceedings. Roˇznov pod Radhoˇstˇem. 1999. P 93.
10. Lapin S. A. Neformalnoe opisanie modeli razgranicheniya dostupa na osnove zadach s uchetom trebovanij k ix vypolneniyu// Problemy pravovoj i texnicheskoj zashhity informacii. 2015. No 3. P. 52.