ляют при этом выбрать стратегию управления рисками и подобрать адекватные меры защиты для противодействия информационным угрозам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Системы управления информационной безопасностью. Ч. 3: Руководство по управлению рисками информационной безопасности BS 7799-3:2006. – С. 70.

2. *Kosko, B* Fuzzy Cognitive Maps / B. Kosko // Int. J. of Man-Machine Studies. – 1986. – Vol. 1. – P. 65 – 75.

3. *Хрусталёв Е.* Когнитивные технологии в теории и практике стратегического управления (на примере оборонно-промышленного комплекса) / Е. Хрусталёв, Д. Макаренко // Проблемы теории и практики управления. – М.: Общество с ограниченной ответственностью «Международная Медиагруппа», 2007. – С. 25–33.

Евстафьев Георгий Александрович
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: georg@evstafiev.name.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; аспирант.

Evstafiev George Aleksandrovich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: georg@evstafiev.name.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
The Department of IT Security; post-graduate student.

УДК 004.056.52

О.М. Лепешкин, П.В. Харечкин

ФУНКЦИОНАЛЬНО-РОЛЕВАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ В СОЦИОТЕХНИЧЕСКИХ СИСТЕМАХ

Представлена функционально-ролевая модель управления доступом, реализующая динамическое назначение полномочий. Модель учитывает понятие задачи, для каждой задачи определяются роли и полномочия. Представлено формальное описание модели и пример ее реализации.

Модель разграничения доступа; активное управление доступом; роль; социотехническая система; функциональная безопасность.

O.M. Lepeshkin, P.V. Kharechkin

FUNCTIONAL-ROLE-BASED ACCESS CONTROL MODEL IN SOCIOTECHNICAL SYSTEMS

The paper gives the functional-role based access control model that realizes permission dynamic management. Task is core in this model, task associates role and per-

mission. This paper also gives the formal description of this model, and gives application example.

Access control model; active access control; role; sociotechnical system; functional safety.

С развитием информационных технологий и все более широким распространением информационных систем актуальным является вопрос обеспечения информационной безопасности в рамках защиты от несанкционированного доступа. В данном случае обеспечение информационной безопасности осуществляется посредством применения моделей управления доступом.

В истории развития математических моделей управления доступом выделяют следующие направления.

1. Модели, основанные на организационно-штатной структуре предприятия и структуре информационных ресурсов.

2. Модели, управление доступом в которых основывается на структуре его бизнес-процессов (workflow).

Таким образом, появление направления, которое отличается от направления развития классических моделей разграничения доступа [1], привело к разделению управления доступом на статическое (пассивное) и динамическое (активное).

Понятие динамического управления доступом представлено в [2]. Авторы вводят понятие задачно-ориентированного управления доступом (TBAC) как расширение контроля доступа, базирующегося на ролях (RBAC).

Основой RBAC является понятие роли [3]. Системный администратор создает различные роли согласно политике безопасности и назначает ролям соответствующие полномочия, а пользователю назначает роль в соответствии с его должностными обязанностями. RBAC реализует иерархию ролей, принцип минимальных привилегий и принцип разделения ответственности.

В TBAC основным понятием является задача, причем полномочия не являются статичными и постоянными – они изменяются в соответствии с контекстом задачи. TBAC предоставляет динамическое управление доступом в режиме реального времени в процессе выполнения задачи.

Модель TBAC может быть описана пятью кортежами: (S, O, P, L, AS), где S – субъект, O – объект, P – полномочия, L – период жизни, AS – этап авторизации.

Поскольку выполнение задачи всегда ограничено по времени, в TBAC полномочия пользователей также имеют период жизни. До активации AS его полномочия не могут быть задействованы.

Благодаря AS TBAC обеспечивает выполнение принципа минимальных привилегий. При выполнении задачи пользователь наделяется только необходимыми для этого правами, а когда задача не выполняется, прав на доступ у пользователя нет.

В современных социотехнических системах (СТС), для того чтобы реализовать концепцию BPM как управленческую методологию [4], необходимо внедрять и RBAC, и TBAC в одно и то же время. Если положение (роль) пользователя в системе меняется, то также меняется и набор функций (полномочия) пользователя, что реализуется с помощью RBAC. Но когда тот же пользователь выполняет определенную задачу, встает вопрос взаимосвязей выполнения задач текущего процесса workflow, что решает, в свою очередь, модель TBAC. Недостатком RBAC является отсутствие понятия потока работ (workflow), и только комбинируя данную

модель с TBAC, можно решить проблему взаимосвязи задач во время выполнения процесса workflow.

Преимущества статического и динамического управления доступом реализованы в функционально-ролевой модели управления доступом, представленной на рис. 1.

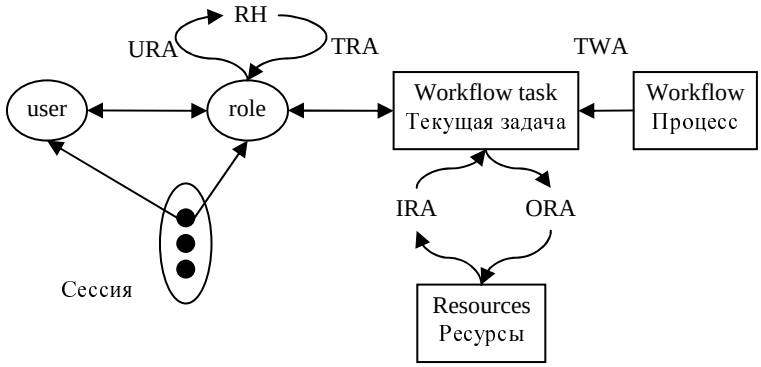

Рис. 1. Функционально-ролевая модель управления доступом

Основные положения модели:

1. User (U): пользователь в СТС описывается множеством

$$U = \{u1,u2,u3,\ldots,un\}.$$

2. Role (R): роль соответствует набору операций, которые необходимо выполнять в рамках какой-либо служебной обязанности пользователя:

$$R = \{r1,r2,r3,\ldots rn\}.$$

3. Task (T): задача из набора задач отдельного процесса СТС.

4. Permission (P): полномочия – набор прав доступа, необходимый пользователю для выполнения текущей задачи процесса в СТС:

$$P = \{p1,p2,p3,\ldots pn\}.$$

5. Session (S): сессия – отображение пользователя на роль. Сессия начинается каждый раз, как пользователь задействует конкретную роль, пользователь может активировать мультироли:

$$U: S \rightarrow U, R:S \rightarrow 2^R.$$

6. Задача описывается тремя позициями: входящий информационный поток IRA – ресурсы, необходимые пользователю для выполнения задачи; полномочия и исходящий информационный поток ORA – ресурсы, которые необходимо передать другим пользователям в рамках общей задачи и общего процесса СТС.

Формальное описание модели соответствует следующим положениям:

1. User-Role Assignment (URA): отображение множества пользователей на множество ролей. Пользователь может иметь несколько ролей, роль может быть назначена нескольким пользователям. Связаны отношением многие ко многим:

$$URA \subseteq U \times T.$$

2. Task-Role Assignment (TRA): отображение множества задач на множество ролей. Задача может быть ассоциирована с мультиролями, а роль может быть подписана на мультизадачи. Задача и роль связаны отношением многие ко многим:

$$TRA \subseteq T \times R.$$

3. Permission-Task Assignmeng (PTA): отображение множества полномочий на множество задач:

$$PTA \subseteq P \times T.$$

4. Task Workflow Assignmeng (TWA): Workflow-процесс – поток работ, состоящий из задач:

$$TWA = \{T1,T2,T3,\ldots Tn\}.$$

5. Role Hierarchylayer (RH): иерархия ролей может быть представлена с помощью примитива $((R_{I+1}, R_I) >)$, где R_{I+1} является непосредственным наследником R_I, знак > означает «содержит»:

$$RH \subseteq R \times R.$$

На рис. 2 представлена функция СТС F, описанная схемой процесса workflow на сетях Петри [5], управление доступом в которой осуществляется на основе функционально-ролевой модели.

Функция F состоит из набора задач $TWA = \{T_0, T_1, T_2, T_3, T_4, T_5\}$.

В СТС определены пользователи $S = \{s_1, s_2, s_3\}$, причем пользователям s_1, s_2 назначена роль r_1, пользователю s_3 – роль r_2. Для каждой задачи T определены входные $IRA = D_{in}$ и выходные $ORA = D_{out}$ данные.

Согласно схеме задачу T_0 через переход t_1 может выполнить субъект s_1. Нескольким субъектам можно назначить переход, например переход t_7 может быть выполнен тремя субъектами s_1, s_2, s_3. Субъекту s_3 необходимы данные d_2, чтобы выполнить переход t_3. При выполнении t_3 s_3 создает d_3. Значения D_{in} и D_{out} могут быть пустыми: $D_{in}(t_1) = \varnothing$. В этом случае никакие данные не нужны, чтобы выполнить действия, связанные с переходом.

Внедрение процессного подхода системы управления доступом позволяет ограничивать доступ к ресурсам не только на основе полномочий, но и в зависимости от текущего состояния СТС рамками задачи. Описание СТС взаимосвязанными процессами и задачами решает вопрос контроля информационных потоков и

позволяет оценить функциональную безопасность СТС и определить, будет ли соответствовать выполнение задачи установленным для системы требованиям и ограничениям.

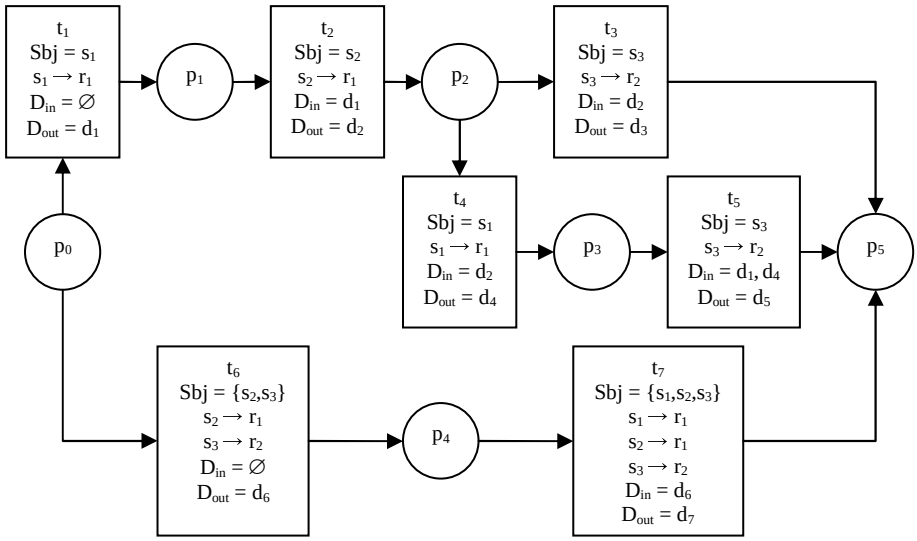

Рис. 2. Схема управления доступом на основе сетей Петри

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Лепешкин О.М., Харечкин П.В.* Анализ моделей разграничения доступа, реализованных в современных социотехнических системах // Периодический научно-технический и информационно-аналитический журнал «Инфотелекоммуникационные системы». Т. 6. – Самара, 2008. – №2. – С 91 – 93.

2. *Thomas R.K., Sandhu R.S.* Task-based Authorization Controls (TBAC): Models For Active and Enterpriseoriented Authorization Management. In Proceedings of the 11th IFIP WG 11.3 Conference on Database Security, Lake Tahoe, CA, August 1997.

3. *Гайдамакин Н.А.* Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Изд-во Уральского ун-та, 2003. – 328 с.

4. *Александров Д.В., Костров А.В., Макаров Р.И., Хорошева Е.Р.* Методы и модели информационного менеджмента. – М.: Финансы и статистика, 2007. – 336 с.

5. *Харечкин П.В.*Подход к описанию динамической системы управления доступом в социотехнических системах на основе сетей Петри // Материалы Первой всероссийской молодежной конференции по проблемам информационной безопасности «Перспектива – 2009». – Таганрог, 2009. – С. 323.

Лепешкин Олег Михайлович
Научно-исследовательская лаборатория Ставропольского военного института связи и ракетных войск.
E-mail: lom@stavsu.ru.
355000, г. Ставрополь, проезд Северный, 13.
Тел.: 8 (905) 4100255.
Начальник.

Lepeshkin Oleg Mihailovich
Research laboratory Stavropol Military Institute of Connection and Rakete Troops .
E-mail: lom@stavsu.ru.
13, North Passage, Stavropol, 355000, Russia.
Phone: 8 (905) 4100255.
Head.

Харечкин Павел Владимирович
Ставропольский государственный университет.
E-mail: amirtimur@gmail.com.
355044, г. Ставрополь, пер. Шеболдаева, 11, кв.48.
Тел.: +7 (905) 44 78 661.
Аспирант.

Kharechkin Pavel Vladimirovich
Stavropol State University
E-mail: amirtimur@gmail.com.
App. 48, 11, Sheboldaeva side str., Stavropol, 355044, Rusia.
Phone: +7 (905) 44 78 661.
Post-graduate student.