Раздел VIII. Прикладные вопросы информационной безопасности

УДК 004.056.52

П.В. Харечкин

МЕТОДИКА ОЦЕНКИ БЕЗОПАСНОГО ВЫПОЛНЕНИЯ КОЛЛЕКТИВНЫХ ИНФОРМАЦИОННЫХ ЗАДАЧ В СОЦИОТЕХНИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Представлена методика оценки безопасного выполнения коллективных информационных задач для функционально-ролевой модели управления доступом, реализующей динамическое назначение полномочий. Методика основана на показателях полноты и доступности информации, своевременности информационных потоков и времени выполнения коллективных информационных задач. Внедрение процессного подхода в системы управления доступом на основе функционально-ролевой модели способствует выполнению коллективных задач в заданном порядке, снижению накопления неполной информации в потоке коллективных задач и, в итоге, снижению величины опасности нарушения целостности неполных информационных объектов.

Активное управление доступом; роль, социотехническая система; информационная задача; функциональная безопасность.

P.V. Kharechkin

EVALUATION METHOD OF COLLECTIVE INFORMATION TASKS SAFETY PERFORMANCE IN SOCIOTECHNICAL INFORMATION SYSTEMS

The paper gives the evaluation method of collective information tasks safety performance for the functional-role based access control model that realizes permission dynamic management. The evaluation method is based on indicators of completeness and availability of information, the timeliness of information flows and execution time of collective information tasks. Introduction of process approach in the access control system based on functional role model contributes to the collective tasks in the specified order, reduce accumulation of incomplete information in the stream collective tasks and, ultimately, reduce the risk of violation of the integrity of the incomplete information objects.

Active access control; role; sociotechnical system; information task; functional safety.

Основу обеспечения безопасного функционирования современных информационных систем (ИС) составляют формальные модели разграничения доступа, которые реализуют субъектно-объектный подход в построении систем защиты информации. Вклад в развитие данного направления внесли многие отечественные и зарубежные исследователи, такие как В.А. Герасименко, А.А. Грушо, L.J. LaPadula, D.E. Bell, Hoffman J., Sandhu, Uhlman J. др. Кроме того, разработаны международные и отечественные стандарты и нормативные документы, регламентирующие обеспечение информационной безопасности и эффективности функционирования ИС.

Характерной особенностью построения защищенных ИС, отвечающих установленным требованиям безопасного функционирования, является доминирование объектно-ориентированного и процессного подходов, которые отодвинули на задний план решаемую пользователем задачу как основную единицу целенаправлен-

ной деятельности. Вместо этого главное внимание при проектировании системы уделяется структурам и потокам данных, событиям, функциям и условиям их выполнения. При этом вопросы активности пользователей и их информационного поведения традиционно относятся только к сфере информационного менеджмента и, таким образом, остаются за рамками проектирования [1]. Тем самым игнорируется социотехнический характер ИС.

Последние исследования показывают [1, 2], что процессы функционирования ИС все больше основываются на коллективных, субъектно-распределенных информационных задачах. Такие задачи для ИС являются критичными, ведь их невыполнение по времени накладывает серьезные ограничения на функционирование ИС в дальнейшем и приводит к появлению уязвимостей в информационных процессах при выполнении ИС своих функций в условиях неполной информации. Таким образом, участвуя в такого рода задачах, пользователи порождают новые виды угроз безопасности, решить которые классический субъект-объектный подход к управлению доступом не способен.

Как отмечают многие ведущие специалисты [1, 3, 4], главная принципиальная трудность здесь заключается в необходимости исследования и проектирования информационных процессов одновременно на двух разных уровнях:

- уровне выполнения субъектами операций над информационными объектами в процессе совместного выполнения задачи;
- уровне взаимодействия между активными субъектами.

При этом появление отношений доступа между пользователями ИС на приведенном выше втором уровне в рамках решения ими коллективной задачи носит зачастую характер коллизии или конфликта, учесть которые классический субъектно-объектный подход не в состоянии. Таким образом, существует необходимость формализации и учета новых отношений доступа в динамичных процессах решения пользователями коллективных информационных задач для обеспечения безопасного выполнения функций социотехнической информационной системы (СТИС).

Решение данной научной задачи было осуществлено на основе разработки новой функционально-ролевой модели разграничения доступа [5, 6], которая ограничивает во времени область конфликтного взаимодействия пользователей рамками выполняемой коллективной задачи с целью устранения угроз функциональной безопасности СТИС через динамическое назначение полномочий.

Динамические отношения модели функционально-ролевого разграничения доступа, в свою очередь, предполагают оценку функциональной безопасности процессов выполнения коллективных задач, что приводит к необходимости разработки методики оценки безопасного выполнения коллективных информационных задач [7] при наличии пользователей, находящихся в диалектически конфликтных парах ролей. Разрабатываемая методика должна отражать эффективность выполнения коллективных информациионных задач в отношении полноты, целостности и доступности информации, своевременности выполнения задач и функций ИС.

В общем случае, особенности выполнения коллективной информационной задачи представлены следующим образом на рис. 1.

Каждая коллективная задача Z характеризуется наличием исходных данных в виде множества информационных объектов D_{in}, осуществляя доступ к которым, участвующие в ней субъекты S предоставляют и обрабатывают сложные информационные объекты $S \rightarrow O_{complex}$ в рамках своих подзадач Z^* для достижения конечной цели – получения выходных данных в виде множества информационных объектов D_{out}, причем выполнение задачи Z ограничено временем t.

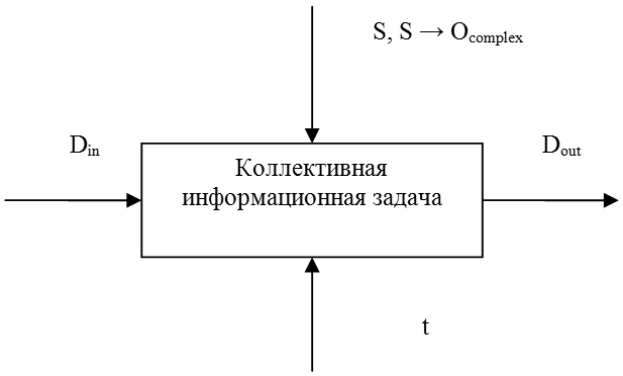

Рис. 1. Общая схема коллективной информационной задачи

Участвующие в выполнении задачи пользователи образуют диалектически конфликтные пары ролей $S_j(R_1) \leftrightarrow S_i(R_2)$ так, что при декомпозиции коллективной информационной задачи Z на неупорядоченное множество частных подзадач $Z \rightarrow \{Z^*\}$, количество таких подзадач Z^n будет равно количеству отношений многие-ко-многим всех пользователей в конфликтных парах ролей: $n = S_j(R_1)^*S_i(R_2)$.

Каждый пользователь характеризуется средой доступа SD и средой взаимодействия SV. Среда доступа содержит только объекты доступа D_{in}. Среда взаимодействия же будет характеризоваться как D_{in}, так и D_{out}. Каждая подзадача Z^* состоит в формировании сложного информационного объекта и носит итерационный характер для ролей, заключающийся в предоставлении и обработке данных. Соответственно для подзадачи Z^* предоставление данных будет иметь вид D^*_{in}, а обработка – D^*_{out}. Структурная схема коллективной задачи, включающей в себя унитарные задачи в виде отношений «клиент-сервер», представлена на рис. 2.

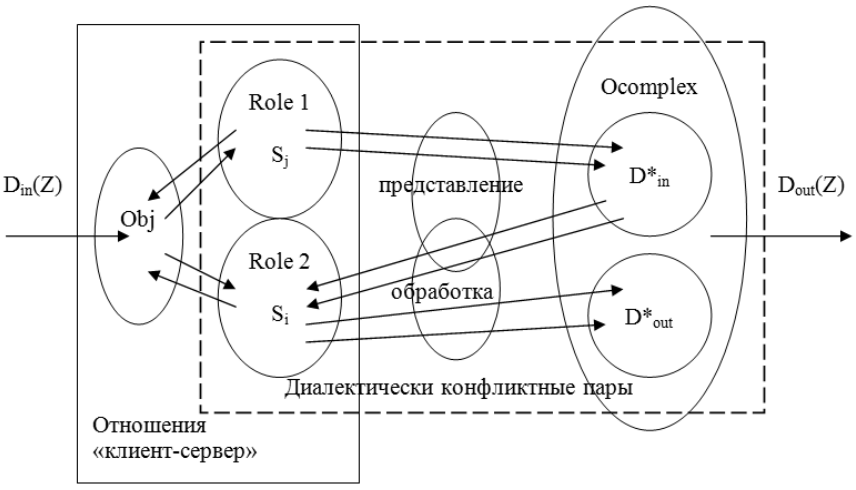

Рис. 2. Структурная схема коллективной задачи

Субъекты, предоставляющие и обрабатывающие информационные объекты, переводят систему из одного состояния в другое, так как порождение информационных потоков способствует решению текущих задач и достижению поставленных функций СТИС. В рамках коллективной задачи это будет соответствовать решению подзадач $\{Z^*\}$, а в рамках функции СТИС – решению коллективных задач $\{Z\}$.

Пусть t – время выполнения коллективной задачи Z, а t_0 – время предоставления пользователями информационных объектов. При выполнении своих подзадач пользователи всегда стремятся к максимальному времени работы, т.е. $t_0 \to t$. Тогда пользователи, осуществляющие итерации обработки, должны выполнить свои подзадачи за время $t - t_0$.

Таким образом, имеет место диалектически конфликтное взаимодействие пользователей как конфликт субъектов с противоположными целями. Отсюда следует, что выделение в информационных процессах СТИС коллективных информационных задач и необходимости обеспечения, помимо информационной безопасности (ИБ), функциональной безопасности (ФБ) приводит к появлению следующего класса угроз СТИС:

- угроза несанкционированного доступа к неполной информации и нарушение ее целостности в рамках ИБ;
- угроза появления неполной информации в условиях динамического потока информационных задач в рамках ФБ.

Выполняя текущие задачи и переходя из одного состояния в другое, СТИС изменяется во времени, т.е. эволюционирует. Движущей силой эволюции в данном случае являются конфликты, которые возникают в системе в случае непредоставления одной социальной подсистемой общих ресурсов другой социальной подсистеме.

С учетом всего сказанного, разрабатываемая методика должна основываться на показателях доступности, полноты информации, своевременности информационных потоков и времени выполнения коллективных информационных задач и в качестве результата оценки определять коэффициент ресурсной координации задачи и величину опасности нарушения целостности неполных информационных объектов потока задач.

Таким образом, цель методики – оценка выполнимости коллективных информационных задач и угроз образования неполной информации и угроз целостности информации на основе показателей полноты, доступности информации, своевременности информационных потоков и времени выполнения коллективных информационных задач.

Результатом оценки является коэффициент ресурсной координации задачи и величина опасности нарушения целостности неполных информационных объектов задачи.

Необходимые входные данные:

Z – коллективная информационная задача;

Z^* – подзадача коллективной информационной задачи Z, характеризующаяся итерациями предоставления и обработки информационных объектов;

$D_{in}(Z)$ – входные данные для задачи Z;

$D_{out}(Z)$ – выходные данные для задачи Z;

D^*_{in} – данные в итерациях предоставления данных;

D^*_{out} – данные в итерациях обработки данных;

ω_1 – важность полноты информационных объектов в итерациях Z^*;

ω_2 – важность полноты информационных объектов всей задачи Z;

α_i – важность задачи Z_i, где $\sum_{i=1}^{z} \alpha_i = 1$;

M – общее количество пользователей-субъектов S;

H – количество ролей;

n – пользователи-субъекты S_j в роли *Role 1*;

k – пользователи-субъекты S_i в роли *Role 2*;

N – количество общих информационных объектов доступа;

ΔN – приращение общих информационных объектов в рамках текущей коллективной задачи Z;

$\Delta N = N\text{-}N_d$, где N_d – количество пустых уникумов-объектов *uNull*;

Role 1 и *Role 2* – диалектически конфликтные пары ролей;

Role 1 – роль-активатор итераций предоставления информационных объектов;

Role 2 – роль-активатор итераций обработки информационных объектов;

S_j – пользователи-субъекты в роли *Role 1*;

S_i – пользователи-субъекты в роли *Role 2*.

Так как взаимодействие конфликтных ролей отражается в подзадачах предоставления и обработки информации. Следовательно, коэффициенты ресурсной координации необходимо определять для каждой из итераций. Порядок расчетов определен следующим образом:

1. Доступность полных информационных объектов для субъекта S_i по отношению к диалектически конфликтному субъекту S_j:

$$K = \frac{P}{N \cdot M}. \tag{1}$$

2. Назначения доступа к информационным объектам P определяется следующим образом

$$P = (R^P \cdot (O^S + I)) \cdot (U \cdot (RH + I))^T, \tag{2}$$

где $P_1 = (R^P \cdot (O^S + I))$ – множество доступов ролей к объектам системы с учетом вложенности объектов в коллективные задачи (размерность P_1 – M×H), $P_2 = (U \cdot (RH + I))^T$ – множество включений пользователей в роли с учетом иерархии ролей (размерность P_2 – N×H, размерность P – N×M);

U – прямоугольная (N×H) матрица вхождения пользователей в роли (u_{ij}=1, если i-й пользователь входит в состав j-й роли; u_{ij} = 0, в противном случае), I – единичная матрица размерности M×M.

Для учета вложенности одних сущностей системы в другие в расчетах используются матрицы смежности O^S и RH. Так, матрица RH будет иметь следующий смысл: если $rh_{ij} = 1$, то i-я роль непосредственно включает j-ю роль, и $rh_{ij} = 0$, в противном случае. Для информационных объектов матрица вложенности интерпретируется как матрица достижимости из одних объектов других за один шаг перехода по иерархической структуре сущностей;

RH – квадратная (H×H) матрица смежности ролей (иерархия ролей);

O^s – квадратная (M×M) матрица смежности объектов доступа.

3. Изменение полноты информационных объектов в динамике выполнения коллективной задачи Z_i в дискретные моменты времени определяются следующим образом:

$$K(t) = \frac{P}{\Delta N \cdot M}. \tag{3}$$

4. Для итерации предоставления данных K^1_{pk} определяется следующим образом:

$$K^1_{pk}(t) = \left(\sum_{\substack{i=1 \\ k>n}}^{M} K_{ik}(t) \right) * \left(1 - \sum_{\substack{i=1 \\ j<k}}^{M} K_{ij}(t) \right)^{-1}, \tag{4}$$

причем для субъектов S_j сумма коэффициентов $\sum_{\substack{i=1 \\ k>n}}^{M} K_{ik}$ является полнотой D^*_{in} и соответствует субъект-объектным отношениям типа «клиент-сервер», и, таким образом, $\sum_{\substack{i=1 \\ k>n}}^{M} K_{ik} = const$, а сумма коэффициентов $\sum_{\substack{i=1 \\ j<k}}^{M} K_{ij}$ – полнотой D_{in} и является переменной величиной.

5. Для итерации обработки данных K^2_{pk} определяется следующим образом

$$K^2_{pk}(t) = \left(\sum_{\substack{i=1 \\ j<k}}^{M} K_{ij}(t) \right) * \left(1 - \sum_{\substack{i=1 \\ k>n}}^{M} K_{ik}(t) \right)^{-1}, \quad (5)$$

причем для субъектов S_i сумма коэффициентов $\sum_{\substack{i=1 \\ j<k}}^{M} K_{ij}(t)$ является полнотой D^*_{out} и соответствует субъект-объектным отношениям типа «клиент-сервер», и, таким образом, $\sum_{\substack{i=1 \\ j<k}}^{M} K_{ij}(t) = const$, а сумма коэффициентов $\sum_{\substack{i=1 \\ k>n}}^{M} K_{ik}(t)$ – полнотой D^*_{in} и является переменной величиной.

6. Коэффициент ресурсной координации K_{pk} коллективной задачи Z_i характеризуется итерациями предоставления и обработки данных, так что с учетом весовых коэффициентов определяется следующим образом:

$$K_{pk}(t) = \omega_1 * K^1_{pk}(t) + \omega_2 * K^2_{pk}(t). \quad (6)$$

Из выражения следует, что:

Следствие 1. Чем меньше объем общих ресурсов, тем ниже коэффициент ресурсной координации, т.е. если $P \to \min$, то $K_{pк} \to \min$.

Следствие 2. Если необходимые ресурсы не предоставляются в соответствии с временным ограничением решения коллективной задачи, то неравенство не выполняется, т.е. $K_{pк} > 1$, что означает появление конфликта в процессе решения коллективной информационной задачи.

7. Функция СТИС состоит из набора задач Z, которые связаны между собой условиями последовательности и параллельности. Тогда коэффициент функциональной безопасности СТИС, отражающий выполнимость функции, будет иметь вид

$$K_{pкФ}(t) = \sum_{i=1}^{z} \alpha_i * K_{pкi}(t). \quad (7)$$

$K_{pк}(t)$ отражает процесс выполнения функции СТИС, состоящей из набора коллективных задач в дискретном времени t. При $K_{pк}(t) < 1$ коллективная задача считается выполненной в момент времени T.

Таким образом, коэффициент ресурсной координации $K_{pк}(t)$ имеет пороговое значение равное 1 такое, что

– $K_{pк}(t) \to 1$;

– $K_{pкФ}(t) \to 1$.

8. Каждая коллективная задача характеризуется двумя матрицами потребностей: предоставления и обработки

$$\begin{pmatrix} K_{11} & \dots & K_{1n} & K_{1n+1} & \dots & K_{1m} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ K_{m1} & \dots & K_{mn} & K_{mn+1} & \dots & K_{mm} \end{pmatrix}. \quad (8)$$

Тогда величина опасности образования неполной информации будет равна

$$T_{обр} = K_{ij}(t) - K_{ij}. \quad (9)$$

Матрица опасности неполноты будет иметь вид

$$\begin{pmatrix} K_{11}(t)-K_{11} & \dots & K_{1n}(t)-K_{1n} & K_{1n+1}(t)-K_{1n+1} & \dots & K_{1m}(t)-K_{1m} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ K_{m1}(t)-K_{m1} & \dots & K_{mn}(t)-K_{mn} & K_{mn+1}(t)-K_{mn+1} & \dots & K_{mm}(t)-K_{mm} \end{pmatrix}. \quad (10)$$

9. Опасность несанкционированного доступа для итераций предоставления и обработки информации будет описываться разностью элементов матриц

$$T_{on} = K_{ik}(t) - K_{ik}. \quad (11)$$

10. Для итерации предоставления данных T_{on}^1 будет определяться следующим образом:

$$T_{on}^1(t) = \sum_{\substack{i=1 \\ j<k}}^{M} (K_{ij}(t) - K_{ij}). \quad (12)$$

11. Для итерации обработки данных T_{on}^2 будет определяться следующим образом:

$$T_{on}^2(t) = \sum_{\substack{i=1 \\ k>n}}^{M} (K_{ik}(t) - K_{ik}). \quad (13)$$

12. Величина опасности несанкционированного доступа T_{on} коллективной задачи Z_i характеризуется итерациями предоставления и обработки данных так, что с учетом весовых коэффициентов определяется следующим образом

$$T_{on}(t) = \omega_1 * T_{on}^1(t) + \omega_2 * T_{on}^2(t). \quad (14)$$

13. Величина опасности несанкционированного доступа к неполной информации в текущей задаче Z_i будет равна

$$T_{on}(Z_i) = T_{on}(Z_{i-1}) + T_{on}(Z_{i-2}) + \dots + T_{on}(Z_1). \quad (15)$$

14. Значение величины опасности нарушения целостности неполных информационных объектов в текущей задаче Z_i будет определяться площадью под кривой функции $T_{on}(t)$, ограниченной снизу пороговым значением T_{on}=1, и будет вычисляться следующим образом:

$$S_{on} = \int_0^t (T_{on}(t) - 1)dt. \quad (16)$$

Данную методику применим для оценки выполнения коллективных информационных задач на примере «Объединенной системы оперативного диспетчерского управления в чрезвычайных ситуациях». На рис. 3 и 4 приводятся значения величины опасности нарушения целостности неполных информационных объектов коллективных задач.

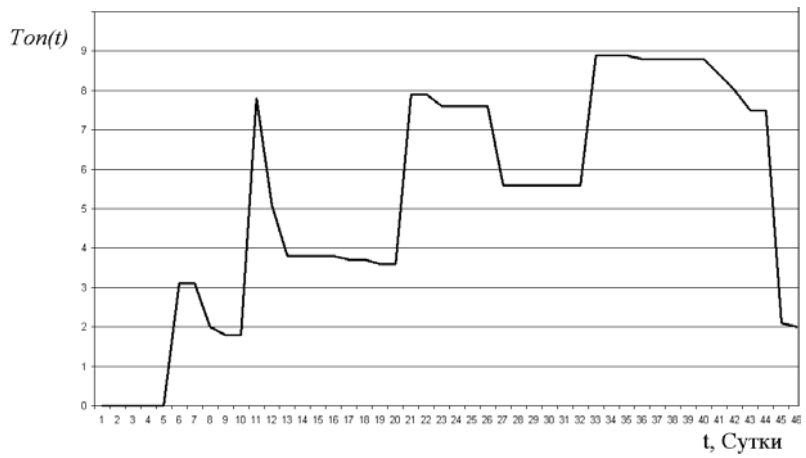

Рис. 3. Величина опасности нарушения целостности неполных информационных объектов потока задач без применения модели функционально-ролевого разграничения доступа

В первом случае отсутствие ограничений действий пользователей рамками коллективной задачи приводит к накоплению неполной информации, и величина опасности в данном случае будет характеризоваться площадью под кривой, равной 86 условным единицам. Во втором случае, при введении правил функционально-ролевой модели разграничения доступа на динамическое назначение полномочий в коллективных информационных задачах, величина опасности будет характеризоваться площадью под кривой, равной 57 условным единицам.

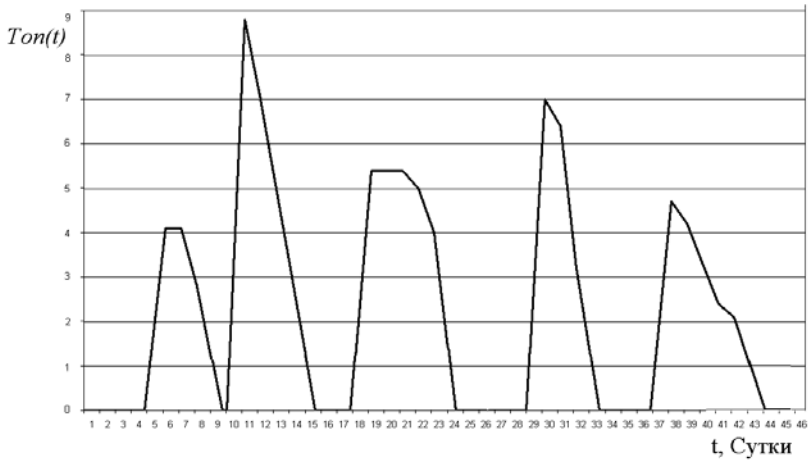

Рис. 4. Величина опасности нарушения целостности неполных информационных объектов потока задач при применении модели функционально-ролевого разграничения доступа

Таким образом, внедрение процессного подхода в системы управления доступом на основе функционально-ролевой модели способствует выполнению коллективных задач в заданном порядке, снижению накопления неполной информации в потоке коллективных задач и, в итоге, снижению величины опасности нарушения целостности неполных информационных объектов на 34 % для объединенной системы оперативного диспетчерского управления в чрезвычайных ситуациях.

Использование коэффициента ресурсной координации и величины опасности нарушения целостности неполных информационных объектов потока задач позволяет оценивать конфликтные ситуации, возникающие в СТИС в процессе ее функционирования в режиме реального масштаба времени. Оценка выполнимости функций и задач СТИС необходима для организации активного управления доступом при реализации функционально-ролевой модели разграничения доступа в рамках процессного подхода к моделированию динамических СТИС.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Столбов А.П.* Денотационные модели процессов коллективного решения информационных задач в социотехнических системах: Дис. д-ра техн. наук: 05.13.17. – М.: РГБ, 2006.
2. *Скобелев П.О.* Моделирование холонических систем. – Труды II Международной конференции "Проблемы управления и моделирования в сложных системах", Россия. – Самара, 20-23 июня 2000 г. – С. 73-79.
3. *Konstantin Knorr.* Dynamic Access Control through Petri NetWorkflows. In Proceedings of the 16th Annual Computer Security Applications Conference. – New Orleans, LA, December 2000. – P. 159-167.
4. *Thomas R.K. and 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.
5. *Харечкин П.В., Лепешкин О.М.* Функционально-ролевая модель управления доступом в социотехнических системах // Известия ЮФУ. Технические науки. – 2009. – №11 (100). – С. 52-57.
6. *Харечкин П.В.* Разработка активатора монитора безопасности функционально-ролевой модели разграничения доступа в социотехнической системе // Вестник Ставропольского государственного университета. – Ставрополь: Изд-во СГУ, 2010. – № 70 (5). – С. 137-144.
7. *Харечкин П.В., Лепешкин О.М.* Управление конфликтным процессом решения коллективной задачи социотехнической информационной системы в условиях ресурсной координации // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 2. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 89-93.

Статью рекомендовал к опубликованию к.т.н., профессор А.П. Жук.

Харечкин Павел Владимирович
Ставропольский государственный университет.
E-mail: harechkin@stavsu.ru.
355009, г. Ставрополь, ул. Пушкина, 1.
Тел.: 89054478661.
Заместитель директора научной библиотеки СГУ.

Harečkin Pavel Vladimirovich
Stavropol State University.
E-mail: harechkin@stavsu.ru.
1, Pushkin Street, Stavropol, 355009, Russia.
Phone: +7 9054478661.
Deputy Director of Scientific library of the Stavropol State University.

УДК 681.3

Е.А. Пакулова

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ДИСПЕТЧЕРИЗАЦИИ ПОДВИЖНЫХ И СТАЦИОНАРНЫХ ОБЪЕКТОВ

Основной целью данной статьи является разработка способа оценки эффективности систем диспетчеризации подвижных и стационарных объектов, направленных на повышение безопасности перевозок пассажиров и опасных грузов. Предложен средневзве-