УДК 004.056.52

ОПИСАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ ЭТАЛОННОЙ МОДЕЛИ ЗАЩИЩЕННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

© **И.А. Губин, С.С. Губина, А.С. Дубровин, В.И. Сумин**

Ключевые слова: математическая модель; автоматизированная информационная система; защита информации; дискреционная политика безопасности; ролевое разграничение доступа.

Рассматривается математический аппарат политики безопасности эталонной модели защищенной автоматизированной системы. Предлагаемая концепция базируется на основах дискреционной модели политики безопасности, субъектно-ориентированной модели изолированной программной среды. Предлагаются пути дальнейшего развития рассматриваемой модели политики безопасности.

В соответствии с [1], характерной особенностью любой автоматизированной информационной системы (АИС) является политика безопасности (ПБ), определённая на ней. ПБ регламентирует методы, процессы, способы работы и функционирования АИС таким образом, чтобы поддерживать информационную безопасность на необходимом уровне.

Основная аксиома теории защиты информации: все вопросы безопасности информации описываются доступами субъектов к объектам [3].

В настоящее время специалисты всё чаще прибегают к использованию дискреционной ПБ, а точнее сказать, к её усовершенствованной модели - ролевой ПБ. Тем не менее, всегда присутствует угроза несанкционированного доступа и потери данных за счет несовершенности структуры самой АИС. В связи с этим целесообразно применять концепцию эталонной модели защищенной автоматизированной системы (ЭМЗАС).

ЭМЗАС предлагается применять для разработки АИС [2]. В результате получаем максимальную степень защиты за счёт доступа к информации реализованного путем последовательного спуска по уровням детализации ресурсов. Доступ реализуется цепочкой авторизованных доступов компонентов более высокого уровня к ресурсам компонентов более низкого уровня.

Используем следующие обозначения:

U — множество уровней ЭМЗАС в данном случае $U = 13$;

u — номер уровня ЭМЗАС, $u \in U$, $u = \overline{1, U}$;

I — индекс модуля, (модули u-го уровня ЭМЗАС индексируются индексами порядка $(13 - u)$);

$K[I]$ — количество нижних модулей блока соответствующего верхнего модуля;

a — номер авторизации, $a = \overline{1, A}|(A = 10)$;

S_a — множество авторизаций (ролей); $|S_a| = 10$;

$r[I, a]$ — признак возможности допустимости авторизации a в модуле с индексом I. Если этот признак равен значению $<< 1 >>$ то доступ к этому модулю с данной авторизацией разрешён, а если $<< 0 >>$ то доступ запрещён.

Y — множество модулей суперблока $S_{b7..13}(I_0)$ ЭМЗАС.

Модуль ЭМЗАС представляет собой субъект соответствующего уровня l ЭМЗАС, который осуществляет доступ только к подчинённому модулю (субъекту) нижестоящего уровня $l - 1$.

Уровневая дискреционная ПБ ЭМЗАС (D) — полномочия дискреционного доступа заданной авторизации к объектам данного уровня (полномочия данного пользователя в данной роли по использованию ресурсов данного уровня) [2].

$$D = R_7(S_{b7..13}(I_0)) = \left\{ r[0.i_1.i_2.i_3.i_4.i_5.i_6, a] \right|$$

$$a = \overline{1, A}, i_1 = \overline{1, K[0]}, i_2 = \overline{1, K[0.i_1]}, ..., i_6 = \overline{1, K[0.i_1.i_2.i_3.i_4.i_5]} \}, \quad (1)$$

где $R_7(S_{b7..13}(I_0))$ — множество допустимых авторизаций седьмого информационного уровня, $r[0.i_1.i_2.i_3.i_4.i_5.i_6, a]$ — разрешающая позиция модуля с индексом $I = 0.i_1.i_2.i_3.i_4.i_5.i_6$ авторизации a, $K[0.i_1]$ - количество модулей подчинённых модулю с индексом $I = 0.i_1$.

Подиндексом E модуля y с индексом I будем называть часть индекса модуля, если индекс I имеет следующую структуру: $I = E.i_1.i_2...i_n$, то есть запись обозначения индекса I начинается с записи обозначения подиндекса E. Обозначение подиндекса $E : E \subset I$ или $I \supset E$.

Дискреционная ПБ складывается из комплекса уровневых дискреционных ПБ, предусматривающих соблюдение правил доступа от модуля к модулю, согласно разрешающим позициям. Таким образом, для авторизации управление субъектом нижнего уровня предусматривает обязательную её легальность на текущем уровне. Если для субъекта невозможно получить определенную авторизацию, то и для управляемого субъекта данная авторизация будет закрыта. Обозначим выводы в виде отношений:

$$(r\,[I, a] \in D) \Rightarrow (\forall E \subset I)(r\,[E, a] \in D), a = \overline{1, A}, I = I(y), y \in Y \setminus Y_U. \quad (2)$$

$$(r\,[I, a] \notin D) \Rightarrow (\forall E \subset I)(r\,[E, a] \notin D), a = \overline{1, A}, I = I(y), y \in Y \setminus Y_1. \quad (3)$$

Из (2) следует, что при формальном задании дискреционной ПБ выполняется следующее правило: если данная авторизация допустима для управляемого субъекта, то для управляющего субъекта данная авторизация должна быть тем более допустима. Из (3) можем определить: если для авторизации закрыт доступ к модулю верхнего уровня, то он будет закрыт для нее и ко всем нижестоящим подчинённым модулям.

Чтобы однозначно определить систему субъектно-объектных отношений в ЭМЗАС применяется модель изолированной программной среды, которая учитывает возможности субъектов по изменению конфигурации или параметров функционирования АИС, которые могут привести к нарушению ПБ. Предоставляется описание субъектно-объектных отношений посредством монитора безопасности объекта (МБО) и монитора безопасности субъекта (МБС). Данные элементы ПБ применяются для фильтрации множества информационных потоков и выделения из их числа только характеризующихся легальным доступом [3]. В целях повышения удобства администрирования АИС, разработанных по принципам ЭМЗАС, предлагается дополнить модель ПБ некоторым математическим аппаратом. Данный функционал будет описывать взаимодействие МБС с иерархической структурой ПБ при добавлении в МБС операций (которые ранее не содержал МБС), которые могут изменить структуру АИС и нарушить заданные правила ПБ. В качестве примера рассмотрим операцию по добавлению роли:

Пусть a' - новая роль, тогда для поддержания ПБ в процессе перехода системы из одного состояния $B(S_a = S_a \setminus \{a'\})$ в другое $B'(S'_a = S_a \cup \{a'\})$ необходимо указать множество разрешающих позиций авторизации по всем уровням ЭМЗАС:

$$(r\left[I, a'\right] \in D), I = I(y), y \in Y.$$

Обозначим ситуацию нарушения ПБ:

$$(\forall r = r\,[I, a] \in R_7\ G), Z\,[I, a] = 0, \quad (4)$$

где $Z = Z[I, a]$ - переменная, определяющая выходную позицию модуля, которая будет либо разрешать использование нижнего модуля, либо нет.

Также в процессе добавления новой роли необходимо осуществить проверку условий, описанных выражениями (2) и (3) при $S'_a = S_a \cup \{a'\}$, чтобы убедиться в согласованности субъектно-объектных отношений, заданных ПБ. Так же необходимо осуществить проверку на отсутствие ситуации нарушения ПБ (4), описанной выражением (1) при $S'_a = S_a \cup \{a'\}$.

Таким образом, мы показали, что надежность ПБ ЭМЗАС достигается за счет синтезирования некоторых элементов традиционных ПБ и указали пути дальнейшего развития данной модели.

ЛИТЕРАТУРА

1. *Губин И.А.,* Дубровин А.С., Мирошина И.Е. Стохастическое варьирование коэффициентом контроля целостности в эталонной автоматизированной системе обработки данных // Вестник Воронежского института ФСИН России. Воронеж, 2012. № 1. С. 75-78.

2. *Губин И.А.* О контроле целостности информационных процессов автоматизированной системы торговой организации // Научный рецензируемый журнал «Научные ведомости Белогородского государственного университета». Белгород, 2014. № 22 (165). Вып. 28/1. С. 179-185.

3. *Девянин П.Н.* Модели безопасности компьютерных систем // Учеб. пособие для студ. высш. учеб. заведений. Москва: Академия, 2005. 144 с.

4. *Вяткин В.Б.* К вопросу взаимоотношений теории информации и теории вероятностей // Вестник Тамбовского Университета. Серия Естественные и технические науки. Тамбов, 2013. Т. 18. Вып. 5. С. 2477-2478.

Поступила в редакцию 2 июня 2015 г.

Gubin I.A., Gubina S.S., Dubrovin A.S., Sumin V.I. THE SECURITY POLICY DESCRIPTION FOR THE REFERENCE MODEL OF THE PROTECTED AUTOMATED SYSTEM

We consider the mathematical apparatus of the security policy of the protected automated system reference model. This concept is based on the discretionary security policy model, subject-oriented model of the isolated software environment. The ways of improvement of the model are discussed.

Key words: mathematical model; an automated information system; information security; discretionary security policy; role-based access.

Губин Игорь Алексеевич, Воронежский государственный педагогический университет, г. Воронеж, Российская Федерация, аспирант кафедры информатики и методики преподавания математики, email: kennik@mail.ru

Gubin Igor Alekseevich, Voronezh State Pedagogical University, Voronezh, the Russian Federation, Post-graduate Student of the Department of Informatics and Mathematics Teaching Methods, email: kennik@mail.ru

Губина Светлана Сергеевна, Военный учебно-научный центр военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина», г. Воронеж, Российская Федерация, кандидат физико-математических наук, преподаватель кафедры математики, e-mail: rydanova_vrn@mail.ru

Gubina Svetlana Sergeevna, Air Force Academy named after Professor N.E. Zhukovsky and Yu.A. Gagarin, Voronezh, the Russian Federation, Candidate of Physics and Mathematics, Lecturer of the Mathematics Department, e-mail: rydanova_vrn@mail.ru

Дубровин Анатолий Станиславович, Воронежский институт ФСИН России, г. Воронеж, Российская Федерация, доктор технических наук, профессор факультета внебюджетного образования, email: asd_kiziltash@mail.ru

Dubrovin Anatolii Stanislavovich, Voronezh Institute of the Federal Penitentiary Service (VIFSIN), Voronezh, the Russian Federation, Doctor of Techniques, Professor of the Faculty of Extrabudgetary Education, email: asd_kiziltash@mail.ru

Сумин Виктор Иванович, Воронежский институт ФСИН России, г. Воронеж, Российская Федерация, доктор технических наук, профессор кафедры управления и информационно-технического обеспечения, email: viktorsumin51@yandex.ru

Sumin Viktor Ivanovich, Voronezh Institute of the Federal Penitentiary Service (VIFSIN), Voronezh, the Russian Federation, Doctor of Techniques, Professor of the Management and Information Technology Department, email: viktorsumin51@yandex.ru

УДК 517.988.6

ОБ ОПЕРАТОРНЫХ УРАВНЕНИЯХ С СЮРЪЕКТИВНЫМИ КВАЗИОБРАТИМЫМИ ОПЕРАТОРАМИ

© **С.С. Губина**

Ключевые слова: квазиобратимый оператор; сюръективный оператор; топологическая степень; операторное уравнение.

В настоящей статье изучается операторное уравнение с линейным сюръективным оператором A, который может быть не замкнут, но обладает непрерывным правым обратным отображением. Рассматривается теорема существования множества решений операторного уравнения $A(x) = f(x)$, где A — линейный сюръективный оператор, а f — вполне непрерывное отображение, и приводятся приложения этой теоремы.

Пусть E_1, E_2 — банаховы пространства, $A : D(A) \subset E_1 \longrightarrow E_2$ — линейный сюръективный оператор.

О п р е д е л е н и е 1. Будем говорить, что оператор A является квазиобратимым, если у оператора A существует правое обратное непрерывное отображение $p : E_2 \to E_1$, т. е. такое отображение p, что $A(p(y)) = y$ для любого $y \in E_2$. В этом случае отображение p будем называть квазиобратным к оператору A.

В дальнейшем будем полагать, что оператор $A : D(A) \subset E_1 \longrightarrow E_2$ квазиобратим и p является отображением квазиобратным к A.

Примеры квазиобратимых операторов и их свойства приведены в [1], [2], [3].

Пусть $V \subset E_1$ — ограниченное открытое множество, $f : \overline{V} \to E_2$ — непрерывное отображение. $N(A, f)$ — множество решений уравнения $A(x) = f(x)$.

О п р е д е л е н и е 2. Будем говорить, что отображение f является (A, p)-вполне непрерывным, если композиция $p \circ f$ является вполне непрерывным отображением.

Т е о р е м а 1. *Пусть существует такое квазиобратное к оператору A отображение p, что отображение f является (A, p)-вполне непрерывным отображением и $q = p \circ f : \overline{V} \to E_1$ не имеет неподвижных точек на ∂V.*

Если топологическая степень $\gamma(i - q, \partial V) \neq 0$, то $N(A, f) \neq \emptyset$.

Если же кроме этого $dim(Ker(A)) > 0$, то $N(A, f) \cap \partial V \neq \emptyset$ и $dim(N(A, f)) \geqslant \geqslant dim(Ker(A))$.

При доказательстве этой теоремы используются свойства топологической степени вполне непрерывных отображений [4] и теоремы о топологической размерности множества неподвижных точек многозначных отображений, доказанные в работе [5]. Доказательство теоремы 1 см. [1].

Рассмотрим следствие из теоремы 1.