УДК 004.056.52

ИСПОЛЬЗОВАНИЕ МОДЕЛИ ХАРРИСОНА-РУЗЗО-УЛЬМАНА В РАЗРАБОТКЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ТОРГОВОЙ ОРГАНИЗАЦИИ

© **И.А. Губин**

Ключевые слова: дискреционная политика безопасности; модель Харрисона–Руззо–Ульмана; математическая модель; автоматизированная информационная система; торговая организация.

Рассматривается математическая модель политики безопасности автоматизированной информационной системы торговой организации, которая разработана по принципам эталонной модели защищенной автоматизированной системы. Данная модель политики безопасности опирается на положения модели Харрисона–Руззо–Ульмана, позволяющие описать ее структуру с учетом изменения множества прав, объектов и субъектов. Предлагается использовать данный математический аппарат для эффективного управления информационными процессами с максимальной степенью защищенности.

Торговая организация (ТО) — организация различных организационно-правовых форм, осуществляющая торговую деятельность, включая необходимые средства и работников с распределением ответственности, полномочий и взаимоотношений (ГОСТ 51303-2013).

Автоматизированная информационная система (АИС) — это система, состоящая из персонала и комплекса средств автоматизации его деятельности, необходимого для выполнения его функций при помощи информационных технологий (ГОСТ 34.003-90).

Для ТО АИС является основой деятельности, так как включает в себя контроль над финансовыми потоками, товарными запасами, документами, персоналом.

Согласно [1], все многообразие угроз безопасности АИС организации можно представить в виде целой связки ключей и отмычек, а систему защиты информации от несанкционированного доступа (СЗИ НСД) организации как сейф, в котором содержатся данные. Можно подобрать ключ — получить пароль и доступ к данным. Если умело использовать отмычку, то получиться открыть сейф, взломав пароль.

Недостатки стандартных моделей политик безопасности (ПБ) были устранены путём разработки нового математического аппарата моделирования СЗИ НСД – ЭМЗАС [2]. Необходимо все процессы доступа к ресурсам распределить по уровням эталонной модели, в итоге получим защищенную модель АИС организации с минимальным уровнем уязвимости.

В [3] предполагалось использование ЭМЗАС для разработки защищенной АИС, используемой в особых сферах человеческой деятельности: военной, силовых структур, банковской и прочих. Отличием вышеописанных АИС является недопустимость сбоя их работы или утечки информации, вызванные неправомерными действиями третьих лиц. В данный момент рассматривается модель АИС ТО, которая только отчасти может относиться к вышеперечисленным специализированным АИС. Ущерб от НСД к ресурсам АИС ТО нельзя назвать фатальным, но из-за уязвимостей системы в итоге страдают и обычные сотрудники, и руководители, и учредители, и, в некоторой степени, государственная экономическая система. Развивать концепцию ЭМЗАС предоставляется возможным за счет использования ее принципов в решении вопросов информационной безопасности АИС различных видов.

Другой особенностью АИС ТО является возможная частая изменчивость самой структуры организации, а также структуры АИС. Например, открытие нового отдела компании, сотрудники которого будут осуществлять финансовый контроль, у которых должны быть

соответствующие новые роли с необходимым набором привилегий. Или добавление новой базы данных для автоматизации управления товарами на складах, к которой будет иметь доступ ряд сотрудников. Такие изменения обязательно отразятся на структуре АИС ТО. Следовательно, модель ПБ, должна быть гибкой и предусматривать возможность изменения структуры без нарушения заданных правил.

Для эффективного использования АИС ТО, построенной по принципам ЭМЗАС необходимо разработать математическую модель, которая будет описывать процедуры изменения структуры АИС. Опираясь на положения модели Харрисона–Руззо–Ульмана и модели типизированной матрицы доступов (ТМД), определим элементы данной модели и процедуры, без которых невозможно эффективно использовать АИС ТО и, которые могут нарушить заданную ПБ.

O — множество объектов модели (модули текущего уровня ЭМЗАС).

S — множество субъектов (авторизованные, стоящие на 1 уровень выше модули).

Rt — права роли на авторизацию в модуле.

M — матрица доступов, строки которой соответствуют объектам, столбцы — субъектам. $M[o,s] \subset Rt | Rt = \{1\}$. $M[o,s] = 1$ - для данной роли возможна авторизация в модуле, $M[o,s] = \varnothing$ — для данной роли авторизация в модуле не возможна.

x — оператор, определяющий переход из начального состояния $t(S,O,M)$ в результирующее состояние $t'(S',O',M')$, обозначим как $t_x \mapsto t'$. Ниже приведем базовые операторы.

«Установить право» $rt \in Rt$ в $M[o,s]$. Результат: $S' = S, O' = O$; $M'[o,s] = M[o,s] \cup \{rt\}$; для $(o',s') = (o,s)$ справедливо $M'[o',s'] = M[o',s']$. Поясним: изменения права коснулось только пары субъект-объект, для которых оно было установлено.

«Удалить право» $rt \in Rt$ из $M[o,s]$. Результат: $S' = S, O' = O$; $M'[o,s] = M[o,s] \backslash \{rt\}$; для $(o',s') = (o,s)$ справедливо $M'[o',s'] = M[o',s']$.

«Создать субъект» $s' \notin S$. Результат: $S' = S \cup \{s'\}, O' = O$; для $(o,s) = O \times S$ справедливо $M'[o,s] = M[o,s]$; для $o \in O'$ справедливо $M'[o,s'] = \varnothing$.

«Создать объект» $o' \notin O$. Результат: $S' = S, O' = O \cup \{o'\}$; для $(o,s) = O \times S$ справедливо $M'[o,s] = M[o,s]$; для $s \in S'$ справедливо $M'[o',s] = \varnothing$.

«Уничтожить субъект» $s' \in S$. Результат: $S' = S \setminus \{s'\}, O' = O$; для $(o,s) = O' \times S'$ справедливо $M'[o,s] = M[o,s]$.

«Уничтожить объект» $o' \in O$. Результат: $S' = S, O' = O \setminus \{o'\}$; для $(o,s) = O' \times S'$ справедливо $M'[o,s] = M[o,s]$.

Из базовых операторов составляются команды, реализующие необходимые операции. Например, добавим модуль с индексом I, и предоставим право авторизации роли под номером 3.

command «Добавить модуль» $(I = 0.i_1.i_2.i_3.i_4.i_5.i_6, a = 3)$:

Создать объект $o'(I = 0.i_1.i_2.i_3.i_4.i_5.i_6)$;

Установить право $M[I = 0.i_1.i_2.i_3.i_4.i_5.i_6, a = 3]$;

end.

В результате выполнения данной команды, по определенным правилам на седьмом уровне ЭМЗАС будет создан модуль и единственной ролью, в которой выступает пользователь, способный получить к нему доступ, будет роль под номером 3.

Следует учитывать, что если при выполнении некоторой команды с набором параметров $c(p_1,p_2,...,p_n)$, характеризующей переход $t_{c(p_1,p_2,...,p_n)} \mapsto t'$, выполняется базовый оператор *«Установить право»*, вносящий rt в элемент матрицы M, до этого rt не содержавший, то возможна утечка права rt. Это предполагает наличие задачи построения алгоритма проверки безопасности системы. На основании [4] можно сказать, что дальнейшее развитие

данных положений нужно вести в русле концепции типов. Это позволит смягчить условия, при которых возможна проверка безопасности системы.

ЛИТЕРАТУРА

1. *Дубровин А.С., Губин И.А.* Модуль режима коммерческой тайны как дополнительный элемент системы защиты информации торговой организации // Современные проблемы науки и образования. 2014. № 5. URL: http://www.science-education.ru/119-15166.

2. *Губин И.А., Сумин В.И., Колыхалин В.М., Исаев О.В.* 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. *Дубровин А.С.* Модели и методы комплексного обеспечения надежности информационных процессов в системах критического применения: автореф. дисс. ... док-ра. тех. наук. // Воронеж, 2011. 433 с.

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

5. *Симонов П.М., Федоров А. В.* Об эффективности использования информационных технологий // Вестник Тамбовского университета. Серия Естественные и технические науки. Тамбов, 2013. Т. 18. Вып. 5. С. 2672-2674.

Поступила в редакцию 1 июня 2015 г.

Gubin I.A. THE USE OF MODELS HARRISON–RUZZO–ULLMAN IN DEVELOPMENT OF INFORMATION SECURITY SYSTEMS TRADE ORGANIZATION

The mathematical model of the security policy of an automated information system Trade Organization which is designed according to the principles of the Reference Model secure automated system is considered. This model of security policy bases on the assumptions of the model Harrison–Ruzzo–Ullman allowing to describe its structure to reflect changes in the set of rights, objects and subjects. It is proposed to use the mathematical apparatus for efficient information management with the maximum degree of security.

Key words: discretionary security policy model Harrison–Ruzzo–Ullman; mathematical model; automated information system; trade organization.

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