L.R. Tuliganova, I.V. Mashkina

The Formal Description of Information Interaction between Subjects and Objects in the Industrial Enterprise Virtualization Segment

Keywords: virtualization segment, mathematical model, access control

The method of information subjects and objects interaction rules formalization in the industrial enterprise virtualization segment has been developed. It is based on mathematical model of mandatory role-based access control. As a result of the investigation we have defined set of user roles and developed roles hierarchy. To ensure information security in the virtualization segment of industrial enterprise information system have been designed the matrix of user access rights and administrative roles functions have been formed.

Л.Р. Тулиганова, И.В. Машкина

ФОРМАЛИЗОВАННОЕ ОПИСАНИЕ ВЗАИМОДЕЙСТВИЯ ИНФОРМАЦИОННЫХ СУБЪЕКТОВ И ОБЪЕКТОВ В СЕГМЕНТЕ ВИРТУАЛИЗАЦИИ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

В настоящее время всё большую популярность набирает технология виртуализации. Используя технологию виртуализации, предприятия могут сократить расходы на развитие и поддержку своей физической инфраструктуры, обеспечить непрерывность бизнес-процессов, упростить администрирование.

Применение технологии виртуализации в информационных системах (ИС) предприятий с высокой степенью доступности информации требует решения проблемы обеспечения конфиденциальности и целостности информационных активов, обрабатываемых в виртуальных средах. Меры по защите среды виртуализации должны исключать несанкционированный доступ к компонентам виртуальной инфраструктуры и информации, обрабатываемой в виртуальной среде [1]. Для обеспечения безопасности данных в кластере виртуализации администратор безопасности должен создать, внедрить, обеспечить функционирование и поддерживать в актуальном состоянии, в соответствии с деловыми процессами предприятия, политику разграничения доступа в сегменте виртуализации.

Кроме того, существует необходимость предотвращения несанкционированного доступа и контроля административных ролей в виртуальной среде.

Политика разграничения доступа в виртуальной среде связана с необходимостью разработки формализованного описания правил взаимодействия между информационными субъектами и объектами в сегменте виртуализации. Правила взаимодействия разработаны на основе математической модели мандатного ролевого разграничения доступа (МРРД) [2]. Основными ее элементами в соответствии с этой моделью являются: U – множество пользователей виртуальных машин; R – множество ролей в среде виртуализации; P – множество прав доступа к объектам виртуальной среды; S – множество сессий пользователей.

Применение данной математической модели к рассматриваемому объекту защиты – сегменту виртуализации ИС промышленного предприятия – требует, в первую очередь, проведения следующих исследований: формирование множества пользователей – субъектов доступа сегмента виртуализации, определение множества ролей пользователей – должностных обязанностей сотрудников различных отделов промышленного предприятия. В рамках проведенных исследований составлены иерархии ролей пользователей и административных ролей. Множество ролей пользователей сегмента

виртуализации ИС промышленного предприятия включает следующие роли: r_N – начальники соответствующих отделов промышленного предприятия, в частности, отделов: системно-технического обеспечения, информационных технологий, материально-технического обеспечения, финансовый, разработчиков и проектировщиков вертолетных двигателей; r_Z – заместители начальников соответствующих отделов; r_U – руководители соответствующих отделов; r_I – старшие инженеры соответствующих отделов; r_S – сотрудники соответствующих отделов (проектировщики, разработчики, инженеры, финансисты); где r_N, r_Z, r_U, r_I, $r_S \in R$. Далее на определенном для сегмента виртуализации ИС промышленного предприятия множестве ролей пользователей сформирована иерархическая структура ролей пользователей.

Иерархия ролей пользователей сегмента виртуализации ИС промышленного предприятия задает на множестве R отношение частичного порядка «≤», при котором выполняется условие: для $u \in U$, если r_i, $r_j \in R$, $r_j \in UA(u)$ и $r_i \le r_j$, то $r_i \in UA(u)$. При этом для $r_i \le r_j$ выполняется одно из условий: 1) $r_i = x_i$_read, $r_j = x_j$_read, $x_i \le x_j$; 2) $r_i = x_i$_write, $r_j = x_j$_write, $x_j \le x_i$. Для иерархии ролей пользователей сегмента виртуализации ИС промышленного предприятия выполняются определенные ограничения, в соответствии с которыми следует, что соблюдаются требования либерального мандатного разграничения доступа. Согласно [2], если модель взаимодействия информационных субъектов и объектов соответствует либеральному или строгому мандатному разграничению доступа, то в ней для o_i, $o_j \in O$, таких, что $c(o_i) > c(o_j)$, невозможно возникновение информационных потоков от o_i к o_j. Это означает, что невозможна утечка конфиденциальной информации.

С учетом приведенных выше условий и ограничений разработана матрица доступа ролей пользователей сегмента виртуализации ИС промышленного предприятия к множеству объектов доступа. Правила администрирования сформированы и представлены в виде рассчитанных значений функций can-assign, can-revoke, can-assignp, can-revokep, can-assigna, can-revokea, can-assigng и can-revokeg.

На основе разработанной методики формализации взаимодействия информационных субъектов и объектов формируются локальные политики безопасности для сегмента виртуализации ИС промышленного предприятия, реализуемые в используемых на исследуемом объекте средствах защиты информации. Благодаря использованной в работе математической модели МРРД в разработанной методике отсутствуют противоречия [3]. Следовательно, возможно теоретическое доказательство безопасности сегмента виртуализации ИС промышленного предприятия как объекта защиты.

СПИСОК ЛИТЕРАТУРЫ:

1. Тулиганова Л. Р., Машкина И. В.Численная оценка риска нарушения информационной безопасности в сегменте виртуализации информационной системы предприятия // Материалы XXII Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы». 2015. № 1.С. 113–114.
2. Девянин П. Н.Модели безопасности компьютерных систем. М.: Издательский центр «Академия», 2005.
3. Яндыбаева Э. Э., Машкина И. В. Методика формализации правил взаимодействия информационных субъектов и объектов в системе электронной торговой площадки // Материалы XXII Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы». 2015. № 1.С. 119–121.

REFERENCES:

1. TuliganovaL. R., MaskinaI. V. Chislennaya ocenka riska narusheniya informacionnoy bezopasnosti v segmente virtualizacii informacionnoy sistemy predpriyatiya // Materiali XXII Vserossiyskoy nauchno-prakticheskoy konferencii «Problemy informacionnoy bezopasnosti v sisteme vysshey shkoly». 2015. №1. Pp. 113–114.
2. Devyanin P.N. Modeli bezopasnosti kompyuternyh system. M.: Akademiya, 2005.
3. Yandybaeva E.E., Mashkina I.V. Metodika formalizacii pravil vzaimodeystviya informacionnyh sub'ektov i ob'ektov v sisteme elektronnoy torgovoy ploschadki // Materiali XXII Vserossiyskoy nauchno-prakticheskoy konferencii «Problemy informacionnoy bezopasnosti v sisteme vysshey shkoli». 2015. № 1. Pp. 119–121.