Методика формирования единой схемы разграничения доступа к гетерогенным информационным ресурсам в облачных инфраструктурах

Technique of forming a common scheme of access control to heterogeneous information resources in cloud infrastructures

Саенко / Saenko I.
Игорь Борисович
(ibsaen@mail.ru)
доктор технических наук, профессор.
ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
ведущий научный сотрудник.
г. Санкт-Петербург

Бирюков / Biryukov M.
Михаил Александрович
(urgent.ma@gmail.com)
ФГКВОУ ВО «Военная академия связи им. Маршала Советского Союза С. М. Буденного»,
преподаватель.
г. Санкт-Петербург

Ясинский / Yasinsky S.
Сергей Александрович
(yasinsky777@mail.ru)
доктор технических наук, доцент.
ЗАО «Институт телекоммуникаций»,
ведущий специалист.
г. Санкт-Петербург

Ключевые слова: разграничение доступа – access control; облачная инфраструктура – cloud infrastructure; ролевая модель разграничения доступа – role-based access control model; генетический алгоритм – genetic algorithm.

Рассматривается методика разграничения доступа к информационным ресурсам в облачных инфраструктурах. Определяются этапы формирования схемы разграничения доступа. Приводится описание указанных этапов. Предлагается реализовывать разграничение доступа в облачных инфраструктурах средствами ролевой модели доступа.

The technique of access control to heterogeneous information resources in cloud infrastructures are considered. Stages of forming the access control scheme are defined. The description of these stages is given. It is proposed to implement the access control in cloud infrastructures with a role-based access control model.

Введение

Совместно эксплуатируемые автоматизированные системы (АС), как правило, по своим функциональным возможностям и техническим характеристикам в значительной степени разрознены, организационно, информационно и технологически не взаимоувязаны и не образуют единую облачную инфраструктуру (ОИ). Исходя из этого можно сделать вывод, что они не могут в полной мере соответствовать концепции облачных инфраструктур в плане обеспечения защищенности информационных ресурсов (ИР) от несанкционного доступа (НСД) в ОИ. Это обусловлено целым рядом причин, среди которых можно выделить следующие: отсутствие системной увязки всех средств и комплексов автоматизации; относительная автономность их создания, включая отсутствие информационно-технического взаимодействия; фрагментарность автоматизации информационных процессов в существующих интегрируемых системах; отсутствие единого автоматизированного цикла информационного обмена в полном объеме; недостаточный уровень комплексной обработки разнородной информации; отсутствие единого механизма разграничения доступа к совместно разделяемым информационным ресурсам [1].

Одним из направлений устранения отмеченных недостатков является разработка методики разграничения доступа к гетерогенным информационным ресурсам ОИ с помощью гетерогенного алгоритма оптимизации (ГАО), которая приведена на рис. 1. Центральным этапом данной методики является создание единой схемы разграничения доступа (СхРД) к гетерогенным

1 2019.indd 77 20.03.2019 11:50:48

информационным ресурсам облачной инфраструктуры (ОИ) на базе избранной модели доступа. Предназначение методики заключается в построении СхРД к информационным ресурсам облачных инфраструктур на базе единой ролевой модели доступа (*Role-Based Access Control, RBAC*), средствами которой могут быть выражены принятые в существующих АС дискреционная (*Discretionary access control, DAC*) и мандатная (*Mandatory access control, MAC*) модели доступа.

При этом следует заметить, что для любой облачной инфраструктуры существует жизненный цикл, состоящий из постановки задачи, проектирования, эксплуатации и модернизации (ликвидации). При решении поставленной задачи целесообразно рассматривать облачную инфраструктуру на всех этапах ее проектирования и эксплуатации.

Обоснование исходных данных

К облачным инфраструктурам предъявляется целый ряд требований [2], среди которых выделяются экономичность, гибкость, адаптивность (эластичная архитектура), высокая готовность, производительность, мониторинг и безопасность. Следует заметить, что требования по безопасности играют одну из ведущих ролей в системе требований к облачным инфраструктурам. В настоящее время уже подготовлен проект ГОСТ «Требования по защите информации, обрабатываемой с использованием технологии облачных вычислений» [3]. Несмотря на то, что этот документ еще не введен в действие, его уже можно использовать в качестве источника информации при планировании защищенной облачной инфраструктуры. Данный стандарт выделяет следующие угрозы, требующие особого внимания:

– отсутствие защищенного доступа (как следствие, повышается угроза атак типа «человек посредине» либо опасность «фишинга»);

– несогласованность политик безопасности (вследствие использования децентрализованной облачной инфраструктуры политики безопасности для различных элементов инфраструктуры могут отличаться. Например, одно средство защиты может закрывать доступ к определенного элементу инфраструктуры, а другое, наоборот, может предоставить такой доступ);

– приостановка оказания услуг вследствие технических сбоев (к данной угрозе относится временная или полная недоступность облачного сервиса конечному потребителю в период сбоя или администрирования);

– невозможность миграции из-за несовместимости оборудования или программного обеспечения (используются различные модели доступа на разных вычислительных платформах);

– общедоступность инфраструктуры (так как пользователи облачных услуг, в том числе конкурирующие между собой, делят одну и ту же инфраструктуру, то возникают угрозы нарушения конфиденциальности или целостности данных путем осуществления прямого доступа к защищаемым данным пользователей);

– нарушение доступности облачного сервиса (в соответствии с сервис-ориентированным подходом, реализуемым в облачных инфраструктурах, в случае нарушения доступности облачной инфраструктуры будет прекращено оказание облачных услуг всем потребителям).

Для нейтрализации выявленных угроз безопасности необходимо построить систему защиты информации облачной инфраструктуры, учитывающую в качестве исходных данных решения по разграничению доступа в интегрируемых автоматизированных системах, к которым относятся множество пользователей и ресурсов ОИ, а также используемые модели доступа и конкретные СхРД.

Преобразование исходных данных

При проектировании облачной инфраструктуры основными этапами являются формирование требований и разработка концепции облачной инфраструктуры. На этих этапах задаются начальные условиях формирования инфраструктуры, формулируется концептуальный и логический уровни представления данных, определяются требования по формирования СхРД логического представления данных. При грамотном планировании и задании исходных данных необходимость в их преобразовании пропадает.

На этапе эксплуатации сложных систем возникают условия, требующие интеграции нескольких АС в рамках единой облачной инфраструктуры. Для гетерогенных АС свойственно иметь различные модели доступа. В зависимости от количества пользователей и объема ресурсов выбирается дискреционная, мандатная или ролевая модель доступа. Для решения задачи оптимизации возникает необходимость в преобразовании исходных данных и приведении исходных моделей доступа к базовой, в данном случае ролевой модели (RBAC). Выбор указанной модели обусловлен возможностью выражать средствами ролевой модели дискреционную и мандатную модели.

На выход алгоритма преобразования исходных моделей в ролевую [4] поступают ролевые СхРД. Для проектирования единой ролевой модели в качестве исходных данных принято использовать [5]:

$U = \{u_i\}, i = 1,...,m, m = |U|$ – множество пользователей;

$PRMS = \{p_j\}, j = 1,...,n, n = |PRMS|$ – множество полномочий;

$ROLES = \{r_l\}, l = 1,...,k, k = |ROLES|$ – множество ролей.

$UA \subseteq U \times ROLES$ – отображения множества пользователей на множество ролей;

$PA \subseteq PRMS \times ROLES$ – отображение множества полномочий на множество ролей;

$UPA \subseteq U \times PRMS$ – отображение множества пользователей на множество полномочий.

Следует отметить, что результат последовательного применения друг за другом отображений *UA* и *PA* может отличаться от *UPA*, если ролевая схема имеет

1-2019.indd 78 20.03.2019 11:50:48

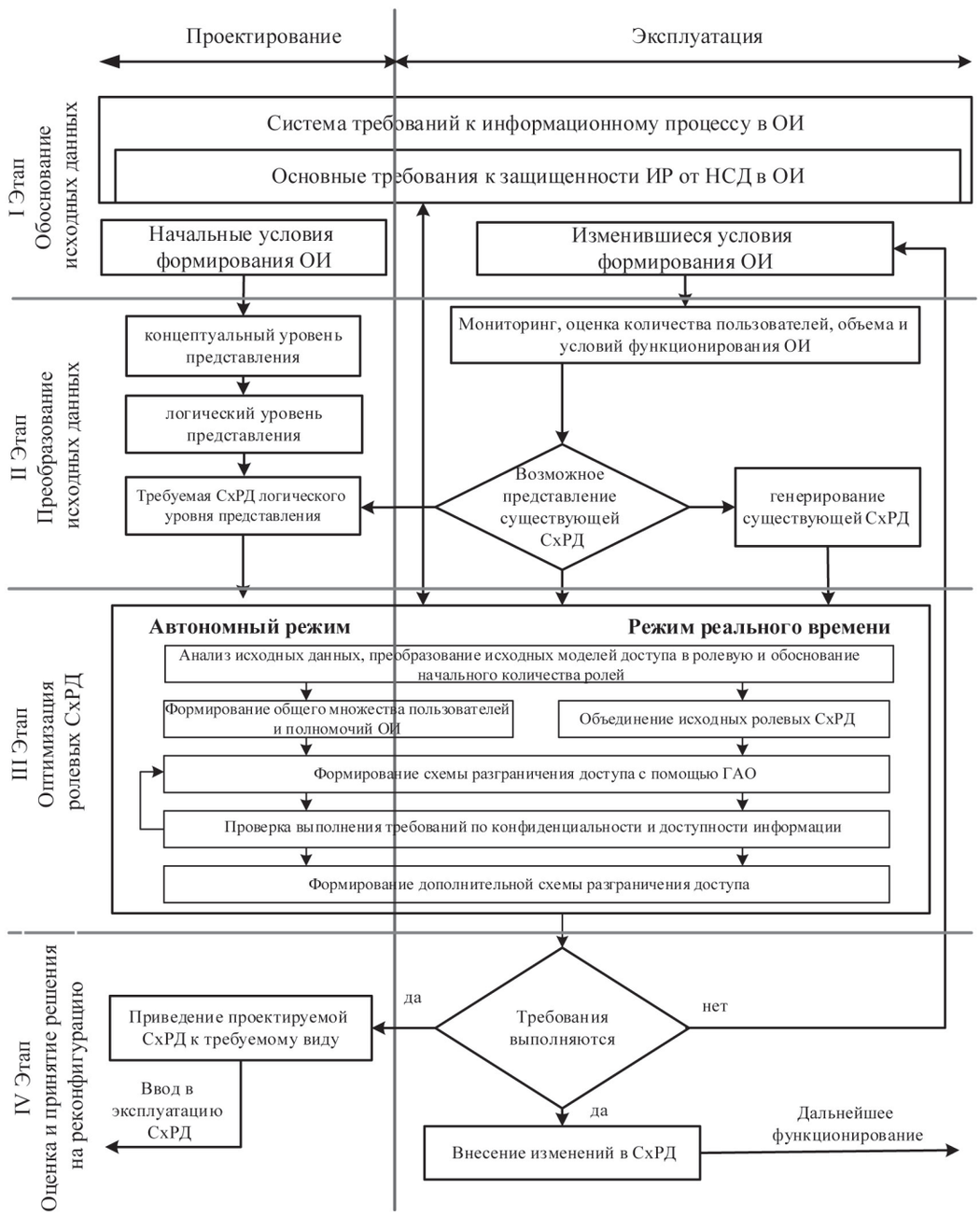

Рис. 1. Методика разграничения доступа к ресурсам ОИ

1 2019.indd 79 20.03.2019 11:50:50

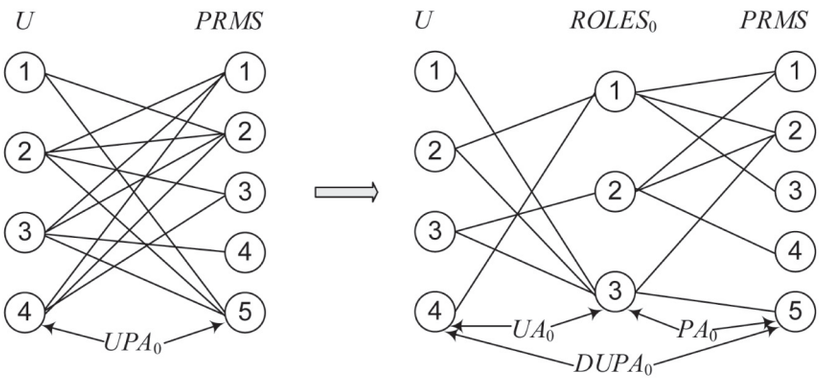

Рис. 2. Отображение ролевой модели RBAC

некоторые ограничения или она сформирована администратором некорректно. Поэтому для такого отображения принято использовать обозначение *DUPA* [6], что означает *Direct UPA* (рис. 2). Совокупность *<U, PRMS, ROLES, UA, PA>* называется схемой *RBAC*.

Оптимизация ролевых СхРД

На этом этапе определяется режим формирования СхРД. Как было описано выше, одним из требований к облачной инфраструктуре является обеспечение ее бесперебойной работы. Поэтому целесообразно ввести два режима формирования СхРД. В режиме реального времени единая СхРД должна строиться «прозрачно» при эксплуатации, без прекращения использования услуг с минимальными отказами. В автономном режиме облачная инфраструктура приостанавливает свою деятельность на непродолжительную профилактику, или функционирует зеркальная структура.

В автономном режиме процедура формирования единой RBAC схемы доступа заключается в следующем.

Исходными данными являются:

1) $\{RBAC_s\}, s = 1, \ldots, S$ – множество локальных схем доступа;

2) $\mathbf{A} = \bigcup \mathbf{A}_s$ – единая политика контроля доступа в пространстве данных, объединяющая локальные политики.

Требуется: найти матрицы **X** и **Y**, удовлетворяющие следующим условиям:

$$\begin{cases} x_{11} \cdot y_{11} \oplus x_{12} \cdot y_{21} \oplus \ldots \oplus x_{1k} \cdot y_{k1} = a_{1n} \\ \ldots \\ x_{m1} \cdot y_{1m} \oplus x_{m2} \cdot y_{2m} \oplus \ldots \oplus x_{mk} \cdot y_{kn} = a_{mn} \end{cases},$$

где количество ролей $k \Rightarrow \min$.

Поясним эту постановку задачи графически на примере объединения в единое пространство данных двух локальных АС.

Пусть одна АС имеет схему контроля доступа $RBAC_1$, показанную на рис. 3-a, а вторая – схему $RBAC_2$, показанную на рис. 3-b.

В схемах $RBAC_1$ и $RBAC_2$ полагается (для удобства их дальнейшего рассмотрения), что кардинальности соответствующих множеств пользователей, полномочий и ролей совпадают. При этом пользователи u_3 и u_4 входят в оба множества U_1 и U_2, а множество состоит из шести элементов. Аналогично, полномочия p_4 и p_5 входят в оба множества $PRMS_1$ и $PRMS_2$, а множество состоит из восьми элементов. Множества ролей $ROLES_1$ и $ROLES_2$ не имеют общих элементов. Каждое из этих множеств состоит из трех элементов.

При решении поставленной задачи в автономном режиме могут использоваться известные способы оптимизации, например генетические алгоритмы [7, 8]. Результатом решения этой задачи являются матрицы **X** и **Y**, отвечающие заданным условиям.

Данный способ при большой размерности задачи, характерной для пространства данных, требует большого времени. Из-за этого в ходе решения задачи работа системы контроля доступа приостанавливается. Поэтому применять этот способ следует в автономном режиме.

В качестве функции пригодности F_{AP} генетического алгоритма в этом случае предлагается использовать выражение

$$F_{\text{AP}} = w_1 k + w_2 \sum_{i=1}^{n} \sum_{j=1}^{m} \left| a_{ij} - \sum_{l-1}^{k} x_{il} y_{lj} \right|,$$

где k – количество ролей в *RBAC* схеме, которую отражает текущая особь генетического алгоритма; $\{a_{ij}\}$ – элементы заданной матрицы A; $\{x_{il}\}$ – элементы матрицы X; $\{y_{lj}\}$ – элементы матрицы **Y**; w_1 и w_2 – весовые коэффициенты. Между весовыми коэффициентами устанавливается соотношение $w_1 << w_2$. Это гарантирует, что в ходе работы генетического алгоритма в первую очередь происходит поиск решений, у которых выполняются заданные условия, а затем происходит поиск решений с более малым количеством ролей.

1-2019.indd 80 20.03.2019 11:50:50

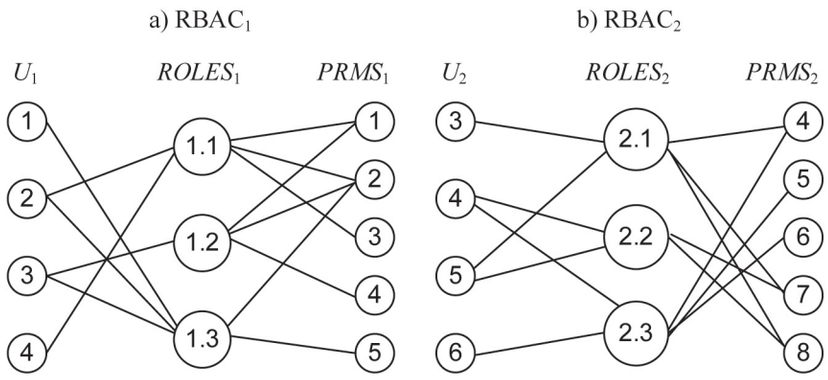

Рис. 3. Схемы контроля доступа $RBAC_1$ и $RBAC_2$

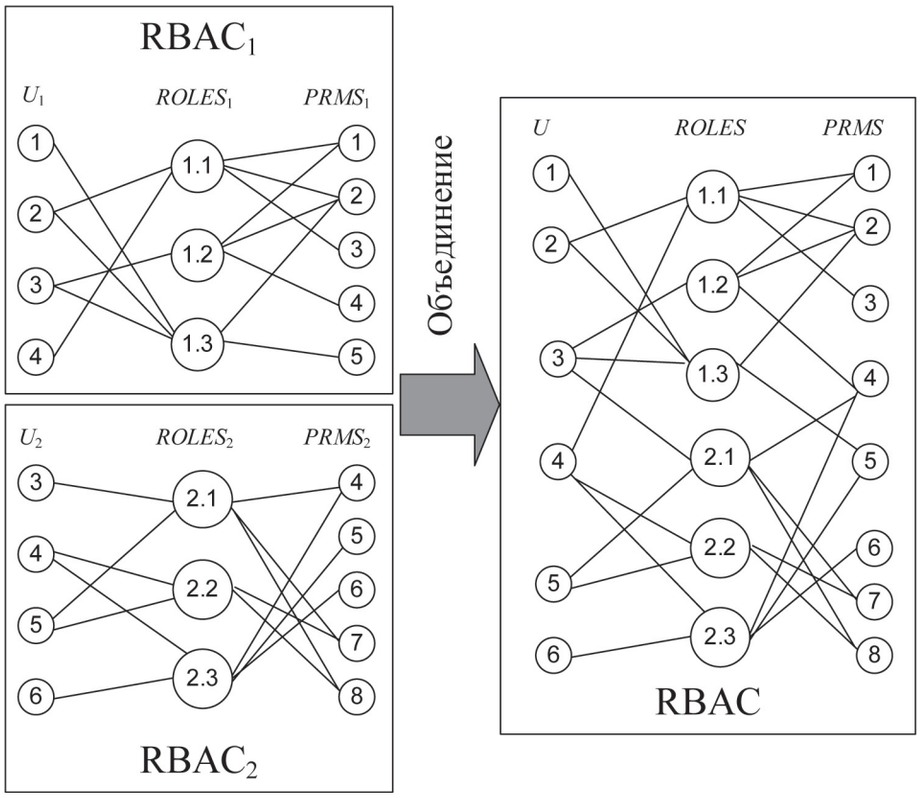

Рис. 4. Формирование единой RBAC схемы контроля доступа

1-2019.indd 81 20.03.2019 11:50:51

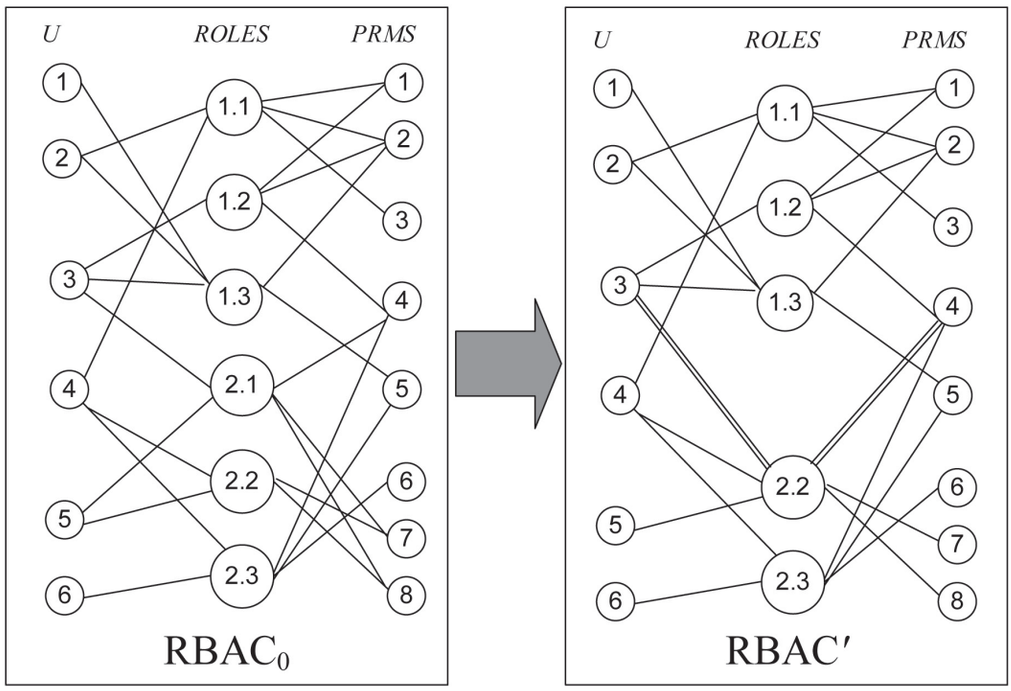

Рис. 5. Переход к схеме RBAC'

Решая задачу реконфигурирования *RBAC* в режиме реального времени, учитываем, что начальные значения матриц (X_0, Y_0) получены путем объединения (X_1, Y_1) и (X_2, Y_2). Порядок формирования для единой *RBAC* схемы контроля доступа (X_0, Y_0) показан на рис. 4, где пунктиром показаны связи между элементами множеств пользователей, ролей и полномочий в схеме $RBAC_1$ и их место в схеме *RBAC*.

При втором способе решения задачи осуществляется последовательный переход от *RBAC* схемы, задаваемой с помощью (X_0, Y_0), к новой схеме $RBAC'$, задаваемой (X', Y'), которая имеет количество ролей, меньшее на единицу. При этом выбирается то решение, при котором количество изменений, которое следует сделать при переходе от (X_0, Y_0) к (X', Y'), будет минимальным. В результате второй способ не требует приостановки работы системы контроля доступа. Он может выполняться в режиме реального времени. Условия перехода от (X_0, Y_0) к (X', Y') записываются в следующем виде: каждая пара матриц (X_0, Y_0) к (X', Y') удовлетворяет заданным условиям; если обозначить k – количество ролей в схеме ($\mathbf{X}_0$, $\mathbf{Y}_0$) и k' – количество ролей в схеме ($\mathbf{X}'$, $\mathbf{Y}'$), то должно выполняться следующее равенство:

$$k - k' = 1,$$

которое является условием выполнения минимальных изменений в *RBAC* схеме при переходе к схеме ($\mathbf{X}'$, $\mathbf{Y}'$). Критерий поиска решения имеет вид

$$\left\|\mathbf{X}_0 \oplus \mathbf{X}'\right\|_1 + \left\|\mathbf{Y}_0 \oplus \mathbf{Y}'\right\|_1 \to \min,$$

где символ $\oplus$ означает булеву операцию «исключающее ИЛИ».

Пример перехода от схемы (X_0, Y_0) к схеме (X', Y') приведен на рис. 5.

Как видно из рис. 5, в новой схеме $RBAC'$ из множества ролей *ROLES* убрана роль $r_{2.1}$. Однако для того, чтобы соответствовать требуемой СхРД, в схему добавлены связи (u_3, $r_{2.2}$) и ($r_{2.2}$, p_4), которые выделены двойной линией. Следовательно, в силу малого количества необходимых изменений переход на $RBAC'$ схему не требует приостановки работы системы контроля.

Функция пригодности F_{PPB} генетического алгоритма в этом случае имеет следующий вид:

$$F_{\text{PPB}} = w_1 F_1 + w_2\left(k - k'+1\right) + w_3 F_3,$$

где частные функции F_1 и F_3 рассчитываются следующим образом:

$$F_1 = \sum_{i=1}^{m}\sum_{l=1}^{K}\left|x0_{il} \oplus x'_{il}\right| + \sum_{j=1}^{n}\sum_{l=1}^{K}\left|y0_{jl} \oplus y'_{jl}\right|,$$

$$F_3 = \sum_{i=1}^{n}\sum_{j=1}^{m}\left|a_{ij} - \sum_{l=1}^{k} x'_{il}\, y'_{lj}\right|.$$

Параметры этих функций имеют следующий смысл: $\{x_{0il}\}$ и $\{x_{0jl}\}$ – элементы матриц X_0, и Y_0, соответственно; $\{x'_{il}\}$ и $\{y'_{jl}\}$ – элементы матриц X' и Y', соответственно; k' – количество ролей в $RBAC'$ схеме; w_1, w_2 и w_3 – весовые коэффициенты, между которыми устанавливаются соотношения $w1 << w_2$ и $w_2 << w_3$, обеспечивающие, что

1 2019.indd 82 20.03.2019 11:50:51

при поиске решений в первую очередь будут находиться X' и Y', отвечающие заданным условиям.

Оценка и принятие решения на реконфигурацию

В процессе формирования требуемой схемы разграничения доступа на каждой итерации генетического алгоритма полученная матрица сравнивается с требуемой матрицей A. Оценка полученной СхРД заключается в ее непротиворечивости требуемой СхРД. На этапе проектирования полученная схема вводится в эксплуатацию вместе с ОИ. Если же конфигурирование происходило на этапе эксплуатации, то вносятся необходимые изменения в функционирующую СхРД.

Заключение

Предлагаемая методика разграничения доступа к информационным ресурсам, в отличие от известных решений в облачных инфраструктурах, позволяет обеспечить требуемую защищенность ресурсов от несанкционированного доступа как на этапе проектирования, так и при непосредственной эксплуатации ОИ в режиме реального времени. Этот результат обеспечивается за счет формирования единой схемы разграничения доступа к гетерогенным информационным ресурсам ОИ в условиях бесперебойной работы пользователей. Дальнейшие исследования связываются с разработкой системы управления пространством данных, в котором разработанная методика будет находить автоматизированную реализацию.

Работа выполнена при поддержке РФФИ (проект 18-07-01369) и бюджетной темы № АААА-А16-116033110102-5.

Литература

1. Бородакий, Ю. В. Проблемы и перспективы создания автоматизированных систем в защищенном исполнении / Ю.В. Бородакий, А.Ю. Добродеев // Известия ЮФУ. Технические науки. – 2007. – № 4 (76). – С. 3–6.

2. Fehling, F. Your Coffee Shop Uses Cloud Computing / F. Fehling, F. Leymann, R. Retter. // IEEE Internet Computing. – 2014. – Vol. 18, No. 5. – P. 52–59.

3. Проект ГОСТ Р Анализ ГОСТ «Требования по защите информации, обрабатываемой с использованием технологии облачных вычислений» [Электронный ресурс] // ECM Journal. – URL: https://ecm-journal.ru/docs/Analiz-GOST-Trebovanija-po-zashhite-informacii-obrabatyvaemojj-s-ispolzovaniem-tekhnologii-oblachnykh-vychislenijj.aspx [Дата обращения: 15.10.2018], свободный. – Загл. с экрана.

4. Модель администрирования схем разграничения доступа в облачных инфраструктурах / И.Б. Саенко [и др.] // Информация и Космос. – 2017. – № 1. – С. 121–126.

5. Frank, M. On the Definition of Role Mining / M. Frank, J.M. Buhmann, D. Basin // Proceedings of the 15th ACM symposium on access control models and technologies. – 2010. – P. 35–44.

6. Vaidya, J. The Role Mining Problem: Finding a Minimal Descriptive Set of Roles / J. Vaidya, V. Atluri, Q. Guo // 12th ACM symposium on access control models and technologies. – 2007. – P. 175–184.

7. Saenko, I. Design and Performance Evaluation of Improved Genetic Algorithm for Role Mining Problem / I. Saenko, I. Kotenko // Proceeding of the 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (PDP 2012). – 2012. – P. 269–274.

8. Kotenko, I. Improved genetic algorithms for solving the optimization tasks in access scheme design for computer networks / I. Kotenko, I. Saenko // Int. J. Bio-Inspired Computation. – 2015. – Vol. 7, No. 2. – P. 98–110.

1-2019.indd 83 20.03.2019 11:50:51