УДК 004.056

МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА К СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

А.И. ГОССА, А.Е. ЛАГУТИН

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 31 октября 2018

Аннотация. Разработана модель разграничения доступа системы облачных вычислений. Основой для нее явилась математическая модель разграничения доступа. Описана политика информационной безопасности. Определены множества объектов и субъектов доступа для системы облачных вычислений. Определены перечни возможностей для объектов и субъектов доступа, построена иерархическая структура ролей.

Ключевые слова: система облачных вычислений, модель разграничения доступа, иерархия ролей.

Введение

Постоянное усложнение сетевой инфраструктуры, увеличивающаяся скорость процессов обмена данными и широкое использование технологий распределенных сервисов предъявляют высокие требования к эффективности функционирования систем разграничения доступа (РД) к информационным ресурсам. В Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, определено, что под информационной безопасностью является состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [1]. Данное понятие является первичным и основным для определения компетенции государственных органов по обеспечению информационной безопасности, а также для установления государственной политики в информационной сфере. Фундаментальным понятием в сфере защиты информации компьютерных систем является политика безопасности. Под ней понимают интегральную совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает состояние защищенности информации в заданном пространстве угроз [1]. Формальное выражение политики безопасности (математическое, схемотехническое, алгоритмическое и т.д.) называют моделью безопасности. Среди программно-технических методов защиты информации в первую очередь выделяют разграничение доступа. Разграничение доступа непосредственно обеспечивает конфиденциальность информации, а также снижает вероятность реализации угроз целостности и правомерной доступности. На сегодняшний день разработано множество моделей разграничения доступа, основанных на различных признаках (матрицы доступа, роли, задачи, события и пр.), что объясняется обширной природой современных систем. Каждая из моделей имеет свои достоинства и недостатки при ее использовании в той или иной системе.

Актуальность разработки модели разграничения доступа и частных политик информационной безопасности (ИБ) объясняется необходимостью планирования и управления ИБ на всех этапах жизненного цикла информационной системы. В случае разработки частной политики безопасности информационных систем облачных технологий (ИСОТ) на основе модели разграничения доступа необходимо учитывать специфику межоблачных взаимодействий между поставщиком и потребителем услуг. С помощью правильно составленной политики ИБ можно обеспечить безопасное, доверенное и адекватное управление системой облачных вычислений (СОбВ), поддержку непрерывности межоблачного взаимодействия, повышение

уровня доверия потребителя к поставщику облачных услуг и, как следствие, минимизацию рисков нарушения информационной безопасности в системе облачных вычислений. Основой построения модели разграничения доступа является модель ролевого разграничения доступа или RBAC – технология контроля доступа, использование которой актуально в современных компьютерных средах. В ролевой политике разрешения ассоциированы с ролями, и пользователи соотносятся с соответствующими ролями, получая таким образом разрешения ролей. Это упрощает управление всей СОбВ в целом. Кроме того, ролевая политика безопасности позволяет избежать угроз информационной безопасности, связанных с неопределенностью ответственности в СОбВ.

Постановка решаемой задачи

В статье решаются задачи усовершенствования ролевой модели разграничения доступа и разработки матрицы доступа к информационным объектам в СОбВ. Для этого необходимо определить множество сущностей в СОбВ (информационные субъекты и информационные объекты), а также построить иерархию ролей и сформировать матрицу разграничения доступа.

Построение иерархической структуры ролей

Основными элементами математической модели ролевого разграничения доступа являются [2]:

– U – множество пользователей;

– R – множество ролей;

– P – множество прав доступа к объектам СОбВ;

– S – множество межоблачных сессий пользователей;

– $(L, \geq)$ – решетка уровней конфиденциальности информации;

– $PA: R \to 2^P$ – функция, определяющая для каждой роли множество прав доступа, при этом для каждого $p \in P$ существует $r \in R$ такая, что $p \in PA(r)$;

– $UA: U \to 2^R$ – функция, определяющая для каждого пользователя множество ролей, на которые он может быть авторизован в облаке;

– $user: S \to U$ – функция, определяющая для каждой межоблачной сессии пользователя, от имени которого она авторизована;

– $roles: U \to 2^R$ – функция, определяющая для каждого пользователя множество ролей, на которые он авторизован в данной межоблачной сессии, при этом в каждый момент времени для каждого $s \in S$ выполняется условие $roles(s) \subseteq UA(user(s))$;

– c: $U \to L$ – функция уровня доступа пользователя;

– c: $O \to L$ – функция уровня конфиденциальности объекта облака;

– $A = \{read, write\}$ – виды доступа;

– AR – множество административных ролей $(AR \cap R = \varnothing)$;

– AP – множество административных прав доступа $(AP \cap P = \varnothing)$;

– $ARA: AR \to 2^{AR}$ – функция, определяющая для каждой административной роли множество административных прав доступа, при этом для каждого $p \in AP$ существует $r \in R$ такая, что $p \in ARA(r)$;

– $AUA: U \to 2^{AR}$ – функция, определяющая для каждого пользователя множество административных ролей;

– $roles: S \to 2^R \cup 2^{AR}$ – функция, определяющая для пользователя множество ролей, на которые он авторизован в данной межоблачной сессии, при этом в каждый момент времени для каждого $s \in S$ выполняется условие $roles(s) \subseteq UA(user(s)) \cup UA(user(s))$.

Для реализации модели ролевого разграничения доступа в СОбВ необходимо установить уровни конфиденциальности, а также определить множество специфических для СОбВ информационных объектов доступа и сформировать множество возможных субъектов доступа.

Установим три уровня конфиденциальности СОбВ и примем для них следующие обозначения: ОИ – открытая информация, К – конфиденциально, СК – строго конфиденциально.

В результате исследований разработано и предложено множество информационных объектов доступа для системы облачных вычислений (табл. 1).

Таблица 1. **Множество информационных уровней СОбВ**

Обозначение	Наименование	Уровень конфиденциальности
o1	Сайт поставщика облачных услуг	ОИ
o2	Множество логинов и паролей личных кабинетов сотрудников потребителя облачных услуг	К
o3(1)	Образы виртуальных машин отдела потребителя облачных услуг, осуществляющего работу по проекту 1	СК
o3(2)	Образы виртуальных машин отдела потребителя облачных услуг, осуществляющего работу по проекту 1	СК
o4(1)	Информационные ресурсы по проекту 1, хранящиеся в облачном хранилище	СК
o4(2)	Информационные ресурсы по проекту 2, хранящиеся в облачном хранилище	СК
o5	Файлы СОбВ, относящиеся к конфигурированию собственных виртуальных машин	СК
o6(1)	Файлы СОбВ, относящиеся к управлению внутриоблачным пространством, осуществляемым поставщиком облачных услуг	СК
o6(2)	Файлы СОбВ, относящиеся к сервисам безопасности поставщика облачных услуг	СК
o7	Данные о серверном времени, скорости данных, объем в хранимых данных	К
o8	Данные о фактическом распределении доступа в фактическом пуле облака	СК
o9	Объем предоставленных потребителю услуг	К
o10(1)	Информационные ресурсы по проекту 1, хранящиеся на стороне потребителя облачных услуг	К
o10(2)	Информационные ресурсы по проекту 2, хранящиеся на стороне потребителя облачных услуг	К
o11(1)	Экземпляры отдела, работающего по проекту 1, запускаемые в физической операционной среде (физическом кластере поставщика облачных услуг)	СК
o11(2)	Экземпляры отдела, работающего по проекту 2, запускаемые в физической операционной среде (физическом кластере поставщика облачных услуг)	СК

Множество ролей пользователей (субъектов доступа) системы облачных вычислений, разработанное в ходе исследований, представлено в табл. 2

Таблица 2. **Множество субъектов доступа в СОбВ**

Обозначение	Наименование	Уровень доступа
1	2	3
*L*1	Технический директор поставщика облачных услуг	СК
*LT*1	Сотрудник первой линии техподдержки поставщика облачныхных услуг	К
*LT*2	Сотрудник второй линии техподдержки поставщика облачныхных услуг	СК
*LT*3	Сотрудник третей линии техподдержки поставщика облачныхных услуг	К
*S*1	Руководитель службы автоматизации ИСОТ	СК
*S*2	Главный специалист по ИСОТ	СК
*S*3	Администратор инфраструктуры ИСОТ	К
*S*4	Эксперт по виртуализации в облачных вычислениях	К
*AV*1	Начальник службы безопасности облачного поставщика	СК
*AV*2	Специалист по защите программного обеспечения и платформ поставщика услуги SaaS	К
*AV*3	Специалист по защите облачной инфраструктуры поставщика услуги SaaS	К
*AV*4	Специалист по защите кластера физических серверов поставщика	К
*P*1	Технический директор потребителя облачных услуг	СК
*P*2,*P*3	Руководители подразделений потребителя облачных услуг, осуществляющих эксплуатацию СОбВ в соответствии с бизнес процессами	СК

Продолжение таблицы 2

1	2	3
*A*1	Начальник отдела автоматизации и безопасности потребителя	СК
*A*2	Администратор безопасности потребителя облачных услуг	СК
*A*3	Работник, осуществляющий интеграцию и сопровождение SaaS ИСОТ (менеджер ИСОТ)	СК
*A*4	Администратор средств защиты потребителя	К
*P*4,*P*5	Сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по проекту 1 в соответствии с бизнес-процессами предприятия	К
*P*6,*P*7	Сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по проекту 2 в соответствии с бизнес-процессами предприятия	К
*P*8,*P*9	Сотрудники потребителя облачных услуг, работающие по проектам 1 и 2 соответственно, не имеющие права эксплуатировать СОбВ в соответствии с бизнес-процессами.	ОИ
*P*10	Сотрудники потребителя облачных услуг, не работающие по проектам 1 и 2 соответственно и не имеющие права эксплуатировать СОбВ в соответствии с бизнес-процессами	ОИ

На рис. 1 представлена разработанная иерархическая структура ролей для множества субъектов доступа в СОбВ.

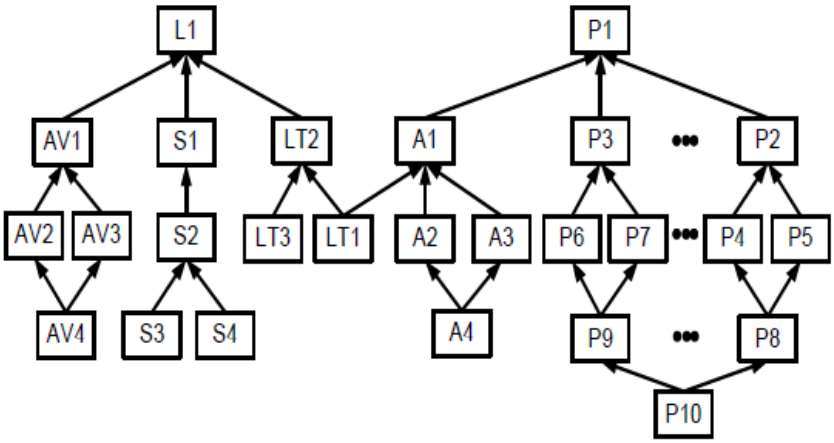

Рис. 1. Иерархическая структура ролей в СОбВ

Так как система облачных вычислений – это система, в которой взаимодействуют поставщик и потребитель облачных услуг, будем модифицировать ролевую модель разграничения доступа таким образом, что каждая из представленных сторон (потребитель и поставщик) имеет свою максимальную роль в иерархии, в отличие от известной ролевой модели разграничения доступа, где максимальная роль в иерархи может быть только одна. Для поставщика облачных услуг максимальной ролью является роль технического директора поставщика (*L*1), для потребителя, − роль технического директора потребителя облачных услуг (*P*1).

В общем случае иерархия ролей потребителя будет иметь больше уровней и будет более распределенной. В примере, проиллюстрированном иерархией ролей на рис. 1, потребитель облачных услуг имеет два подразделения, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами. В каждом из подразделений минимальная роль отводится сотрудникам потребителя облачных услуг, не имеющим права эксплуатировать СОбВ в соответствии с бизнес-процессами (*P*8, *P*9, *P*10), а максимальная − руководителям подразделений потребителя облачных услуг, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами (*P*2, *P*3). Кроме того, в иерархии учтено, что два подразделения потребителя могут выполнять работу в СОбВ над разными проектами (проекты 1 и 2), которые, в соответствии с бизнес-процессами, не имеют общих и пересекающихся ресурсов и активов. Таким образом, сотрудники подразделения, работающего по проекту 1, не имеют доступ к информационным ресурсам и активам СОбВ подразделения, работающего по проекту 2, и наоборот.

В иерархии потребителя облачных услуг, помимо двух подразделений, работающих по проектам 1 и 2, есть третье подразделение, отвечающее за автоматизацию и информационную

безопасность компании. Максимальная роль в этом подразделении отводится начальнику отдела автоматизации и безопасности потребителя облачных услуг (*A*1), а минимальная – администратору штатных средств защиты (*A*4), под которыми понимаются традиционные средства защиты, не входящие в систему безопасности облачной среды потребителя.

Иерархия поставщика облачных услуг, где максимальная роль отведена техническому директору поставщика (*L*1), состоит из трех служб-отделов: служба поддержки потребителей облачных услуг, службы автоматизации облачной среды и службы информационной безопасности поставщика облачных услуг.

Служба поддержки потребителей состоит из трех линий поддержки (*LT*1, *LT*2, *LT*3 соответственно), которые взаимодействуют напрямую с потребителями облачных услуг и помогают конкретному поставщику решать возникающие вопросы и проблемы в реальном масштабе времени. В ходе исследований были выделены три возможные линии технической поддержки облаков [3]:

– сотрудники первой линии техподдержки поставщика облачных услуг, которые при обращении к ним потребителя ликвидируют технические сбои в инфраструктуре, влияющие на предоставляемые пользователям сервисы; эти сотрудники не обладают высокими привилегиями в СОбВ, не имеют доступа к сервисам безопасности СОбВ;

– сотрудники второй линии техподдержки поставщика облачных услуг – группа специалистов высокого профиля, которые обладают достаточной компетенцией и способны решать проблемы как с инфраструктурой СОбВ, так и с сервисами;

– сотрудники третьей линии техподдержки поставщика облачных услуг являются сотрудниками разработчика и производителя технологии облачных вычислений (Amazon, Google, Microsoft).

Служба автоматизации облачной среды отвечает за разработку и процесс интеграции в SaaS облачных вычислений со стороны потребителя облачных услуг; сотрудники службы занимаются вопросами оптимального управления облачными сервисами в условиях существующих ограничений сети потребителя облачных услуг. Максимальной ролью в данной службе будет обладать руководитель службы автоматизации ИСОТ (*S*1), а минимальными ролями – администратор инфраструктуры ИСОТ (*S*3) и эксперт по виртуализации в облачных вычислениях (*S*4).

Служба информационной безопасности поставщика облачных услуг отвечает за безопасность облачной среды со стороны поставщика облачных услуг [3]. В данной службе роли распределены на три составляющие защиты облака: защита программного обеспечения и платформ поставщика услуги SaaS (роль *AV*2), защита облачной инфраструктуры поставщика услуги SaaS (роль *AV*3) и защита кластера физических серверов поставщика облачных услуг (роль *AV*4). Максимальной в данной службе будет роль начальника службы безопасности облачного поставщика (*AV*1), а минимальной – роль специалиста по защите кластера физических серверов поставщика облачных услуг (*AV*4).

Иерархия ролей пользователей СОбВ задает на множестве R отношения частичного порядка «$\le$», 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) $r_i = x_i \_ write, r_j = x_j \_ write, x_j \le x_i,$

где U – множество пользователей, R – множество ролей.

Модель контролирует назначение пользовательской роли посредством отношения $can-assign \subseteq ARxCRx2^R$. Отношение $can-assign(x, y, \{a, b, c\})$ означает, что член административной роли *x* (или член административной роли, которая является старшей для *x*), может назначать пользователя, текущее членство (или отсутствие членства) которого в постоянных ролях удовлетворяет условию необходимой предпосылки *y*, членом постоянных ролей *a, b* или *c*.

Для иерархии ролей пользователей СОбВ выполняются следующие ограничения:

1) ограничение функции UA – для каждого пользователя $u \in U$ выделяется роль:

$x\_read = \oplus(UA(u) \cap \{y\_read \mid y \in L\})UA(u)$ (здесь $x = c(u)$) и

$x\_write = \oplus\{y\_write \mid y \in L\} \in UA(u)$ (здесь $x = \oplus L$);

2) ограничения функции roles – для каждой сессии $s \in S$ выделяется множество ролей:

$roles(s) = \{x\_read, x\_write\};\ x = c(o)$

3) ограничения функции PA – для каждого $x \in L$ доступ $(o, read) \in PA(x\_read)$ тогда и только тогда, когда доступ $(o, write) \in PA(x\_write);$ для каждого доступа $(o, read)$ существует единственная роль $x\_read : (o, read) \in PA(x\_read)$ (здесь $x = c(o)$).

Разработана матрица доступа ролей пользователей (субъектов доступа) СОбВ к множеству объектов доступа (рис. 2).

	o1	o2	o3 (1)	o3 (2)	o4 (1)	o4 (2)	o5	o6 (1)	o6 (2)	o7	o8	o9	o10 (1)	o10 (2)	o11 (1)	o11 (2)
L1	rw	w	-	-	-	-	-	rw	rw	rw	rw	rw	-	-	-	-
LT2	rw	w	-	-	-	-	-	rw	-	rw	rw	rw	-	-	-	-
LT1	r	-	-	-	-	-	-	-	-	rw	rw	r	-	-	-	-
LT3	r	-	-	-	-	-	-	w	-	-	-	-	-	-	-	-
S1	rw	-	-	-	-	-	-	rw	-	rw	rw	rw	-	-	-	-
S2	rw	-	-	-	-	-	-	rw	-	r	rw	r	-	-	-	-
S3	r	-	-	-	-	-	-	rw	-	r	-	r	-	-	-	-
S4	r	-	-	-	-	-	-	rw	-	r	r	r	-	-	-	-
AV1	r	w	-	-	-	-	-	r	rw	r	r	r	-	-	-	-
AV2	r	w	-	-	-	-	-	r	rw	-	-	-	-	-	-	-
AV3	r	-	-	-	-	-	-	-	rw	r	r	r	-	-	-	-
AV4	r	-	-	-	-	-	-	-	rw	-	-	-	-	-	-	-
P1	r	rw	rwe	rwe	rw	rw	rw	-	-	rw	rw	r	rw	rw	rw	rw
A1	r	rw	rw	rw	-	-	rw	-	-	rw	rw	-	-	-	rw	rw
A3	r	rw	-	w	-	-	rw	-	-	rw	-	-	-	-	w	w
A2	r	rw	-	w	-	-	-	-	-	r	-	-	-	-	w	w
A4	r	rw	-	-	-	-	-	-	-	r	-	-	-	-	-	-
P2	r	rw	re	-	rw	-	-	-	-	r	-	r	rw	-	rw	-
P4,5	r	r	re	-	rw	-	-	-	-	-	-	-	rw	-	rw	-
P8	r	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
P3	r	rw	-	re	-	rw	-	-	-	r	-	r	-	rw	-	rw
P6,7	r	r	-	re	-	rw	-	-	-	-	-	-	-	rw	-	rw
P9	r	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Рис. 2. Матрица прав доступа ролей пользователей СОбВ

Заключение

Представлены результаты разработки усовершенствованной модели разграничения доступа, которая была описана частной политикой информационной безопасности системы облачных вычислений. Предложенная модель построена с помощью формальной модели, основанной на математической модели ролевого разграничения доступа. Ее достоинством является возможность исключения пользователей, получающих по иерархии ролей права суперпользователей, которые могут напрямую обращаться к результирующим потокам данных потребителя облачных услуг, а также управлять всеми конфигурационными файлами СОбВ. Предложено ввести в иерархию формальной модели две максимальные роли: одну – со стороны поставщика облачных услуг (роль технического директора поставщика облачных услуг) и одну – со стороны потребителя облачных услуг (роль технического директора потребителя облачных услуг), которые имели бы одновременно и максимально необходимую роль в собственном подразделении облака сообщества и минимально необходимую роль для поддержки бизнес-процессов СОбВ. Соблюдение требований частной политики безопасности СОбВ позволит существенно снизить риски использования облачных вычислений как со стороны поставщика, так и со стороны потребителя облачных услуг, и как следствие, позволит увеличить доверие потенциальных потребителей к ИСОТ.

MODEL OF ACCESS CONTROL TO CLOUD COMPUTING ENVIRONMENT

A.I. GOSSA, A.E. LAGUTIN

Abstract. Model for access control of a cloud computing system was developed. The basis for the model was a mathematical model of access control. Information security policy was described. The sets of objects and subjects of access for a cloud computing system were defined. The lists of opportunities for objects and subjects of access were defined, a hierarchical structure of roles was built.

Keywords: cloud computing system, access control model, role hierarchy.

Список литературы

1. Указ президента Республики Беларусь от 9.11.2010 № 576 «Об утверждении концепции национальной безопасности».
2. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.:2012.
3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. М.: 2011.