ISSN 1992-6502 (Print) Вестник УГАТУ ISSN 2225-2789 (Online)
2016. Т. 20, № 2 (72). С. 134–142 http://journal.ugatu.ac.ru

УДК 004.77:004.056

РАЗРАБОТКА ЧАСТНОЙ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

А. Ю. СЕНЦОВА[1], И. В. МАШКИНА[2]

[1] sentsova.alina@yandex.ru, [2] mashkina.vtzi@gmail.com

ФГБОУ ВО «Уфимский государственный авиационный технический университет» (УГАТУ)

Поступила в редакцию 20.01.2016

Аннотация. Работа посвящена разработке частной политики информационной безопасности системы облачных вычислений. Для описания частной политики предлагается использовать математическую модель ролевого разграничения доступа. Определены множество объектов доступа и множество субъектов доступа для системы облачных вычислений. Определены перечни возможностей для субъектов и объектов доступа, которые могут составлять основу для написания политики разграничения доступа в системе облачных вычислений.

Ключевые слова: система облачных вычислений, частная политика информационной безопасности, ролевое разграничение доступа, иерархия ролей.

ВВЕДЕНИЕ

Сегодня в индустрии информационных технологий можно наблюдать стремительные темпы развития информационных систем, построенных на основе облачных технологий (ИСОТ), однако при этом недостаточно широко освещаются проблемы использования облачных сервисов с точки зрения информационной безопасности (ИБ). Вместе с тем использование средств, обеспечивающих функционирование облачных вычислений, позволяет говорить о новых потенциально возможных угрозах информационной безопасности, которые будут являться специфическими для облачных сред.

Многими экспертами отмечается, что потребитель облачных услуг имеет тот уровень защищенности в облачной среде, который обеспечивается поставщиком [1, 2]. Однако для гарантии защиты пользовательских рабочих мест на стороне потребителя облачных услуг особое внимание необходимо уделить разработке политики безопасности всей системы облачных вычислений (СОбВ), под которой понимается информационная система взаимодействия поставщика и потребителя облачных услуг [3].

Политика информационной безопасности организации − совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которые регулируют управление, защиту и распределение ценной информации [4].

Политика информационной безопасности любой организации зависит от конкретной технологии обработки информационных активов предприятия и от используемых в данной системе информационных потоков, реализующих деловые процессы предприятия. При составлении политики безопасности, необходимо учитывать, какая именно услуга предоставляется потребителю (SaaS, PaaS, IaaS или иная услуга) и какая именно модель облачного размещения реализуется в конкретном случае (частное, публичное, общественное облако, облако сообщества или иная модель) [4]. Критически важно, чтобы поставщики не пользовались и не навязывали универсальный подход в обеспечении информационной безопасности для всех моделей и для всех потребителей. Для устранения угроз, связанных с неопределенностью при распределении ответственности, поставщику облачных услуг необходимо тщательно прорабатывать политику безопасности.

Работа поддержана грантом РФФИ 14-07-00928-а.

АКТУАЛЬНОСТЬ РАЗРАБОТКИ ЧАСТНОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ ДЛЯ СИСТЕМЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Как отмечается в [6], политика безопасности любой информационной системы (ИС) при разработке информационно-безопасных технологий состоит из множества *частных политик*, направленных на конкретные аспекты безопасности ИС. Частные политики безопасности, детализирующие положения политики ИБ, формируются на основе принципов, требований и задач, определенных в политике информационной безопасности, с учетом дополнительной классификации активов и угроз, определения владельцев критичных активов, анализа, оценки рисков и возможных последствий реализаций угроз в границах области действия регламентируемой области или технологии [7].

Актуальность разработки частных политик информационной безопасности объясняется необходимостью планирования и управления ИБ на всех этапах жизненного цикла информационной системы. В случае разработки частной политики безопасности ИСОТ необходимо учитывать специфику межоблачных взаимодействий между поставщиком и потребителем облачных услуг. С помощью правильно составленной политики ИБ можно обеспечить безопасное, доверенное и адекватное управление системой облачных вычислений, поддержку непрерывности межоблачного взаимодействия, повышение уровня доверия потребителя к поставщику облачных услуг и, как следствие, минимизировать риски нарушения информационной безопасности в СОбВ.

Таким образом, для обеспечения безопасного функционирования СОбВ необходимо создание частной политики информационной безопасности, которая должна неукоснительно соблюдаться как поставщиком, так и потребителем облачных услуг.

В статье предлагается разработка частной политики безопасности применительно к СОбВ (политики разграничения доступа) с использованием формальной модели, основанной на математической модели ролевого разграничения доступа, которая описана в [8].

Модель ролевого разграничения доступа – многообещающая технология контроля доступа для современной компьютерной среды. В ролевой политике разрешения ассоциированы с ролями, и пользователи соотносятся с соответствующими ролями, таким образом, получая разрешения ролей. Это упрощает управление всей СОбВ в целом. Кроме того, ролевая политика безопасности позволяет избежать угроз информационной безопасности, связанных с неопределенностью ответственности в системе облачных вычислений. Организация безопасности информации от таких угроз затруднена тем, что их реализация способна привести к существенным разногласиям между поставщиком и потребителем облачных услуг по вопросам, связанным с определением их прав и обязанностей. Для устранения угроз информационной безопасности, связанных с неопределенностью ответственности, поставщику облачных услуг необходимо не только *тщательно прорабатывать политику безопасности*, но и уделять особое внимание *проработке иерархии ролей*.

Роли задаются для различных должностей в облаке, и пользователи соотносятся к ролям, основанным на ответственности и профессионализме. Пользователи могут быть переназначены на другую роль. Роли могут наделяться новыми разрешениями по мере подключения новых приложений и заказе потребителем новых услуг, разрешения могут отбираться у ролей, когда это необходимо потребителю или поставщику услуг.

ПОСТАНОВКА РЕШАЕМОЙ ЗАДАЧИ

В статье решается задача разработки матрицы доступа к информационным объектам в системе облачных вычислений. Для этого необходимо сформулировать множество сущностей в системе облачных вычислений: информационных субъектов и информационных объектов, а также построить иерархию ролей и сформировать матрицу разграничения доступа.

ПОСТРОЕНИЕ ИЕРАРХИЧЕСКОЙ СТРУКТУРЫ РОЛЕЙ ДОСТУПА

Основными элементами математической модели ролевого разграничения доступа являются [8]:

– U – множество пользователей;

– R – множество ролей;

– P – множество прав доступа к объектам СОбВ;

– S – множество межоблачных сессий пользователей;

– (L, ≤) – 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 $roles(s) \subseteq UA(user(s))$;

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

– $O \to L$ – 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: $AR \to 2^{AP}$ – 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 в 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 объектов доступа СОбВ

Обозн.	Наименование	Ур. конф.
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 2	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 конкретным потребителем облачных услуг	СК
o6 (1)	Файлы СОбВ, относящиеся к управлению внутриоблачным пространством поставщиком облачных услуг	СК
o6 (2)	Файлы СОбВ, относящиеся к сервисам безопасности поставщика облачных услуг	СК
o7	Данные о серверном времени, скорости доступа и обработки данных, объем хранимых в хранилище данных	К
o8	Данные о фактическом распределении доступа в едином 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

Обозн.	Наименование	Ур. дост.
1	*2*	*3*
L1	Технический директор поставщика облачных услуг	СК
LT1	Сотрудник первой линии техподдержки поставщика облачных услуг	К
LT2	Сотрудник второй линии техподдержки поставщика облачных услуг	СК
LT3	Сотрудник третьей линии техподдержки поставщика облачных услуг	К
S1	Руководитель службы автоматизации ИСОТ	СК
S2	Главный специалист по ИСОТ	СК
S3	Администратор инфраструктуры ИСОТ	К
S4	Эксперт по виртуализации в облачных вычислениях	К
AV1	Начальник службы безопасности облачного поставщика	СК
AV2	Специалист по защите программного обеспечения и платформ поставщика услуги SaaS	К
AV3	Специалист по защите облачной инфраструктуры поставщика услуги SaaS	К
AV4	Специалист по защите кластера физических серверов поставщика	К
P1	Технический директор потребителя облачных услуг	СК
P2, P3	Руководители подразделений потребителя облачных услуг, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами	СК
A1	Начальник отдела автоматизации и безопасности потребителя	СК
A2	Администратор безопасности потребителя облачных услуг	СК
A3	Работник, осуществляющий интеграцию и сопровождение SaaS ИСОТ (менеджер ИСОТ)	СК
A4	Администратор штатных средств защиты потребителя	К
P4, P5	Сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по проекту 1 в соответствии с бизнес-процессами предприятия	К
P6, P7	Сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по проекту 2 в соответствии с бизнес-процессами предприятия	К
P8, P9	Сотрудники подразделений потребителя облачных услуг, работающие по проектам 1 и 2 соответственно, не имеющие права эксплуатировать СОбВ в соответствии с бизнес-процессами	ОИ
P10	Сотрудник подразделения потребителя облачных услуг, не работающие по проектам 1 и 2, и не имеющие права эксплуатировать СОбВ в соответствии с бизнес-процессами	ОИ

Окончание табл. 2

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

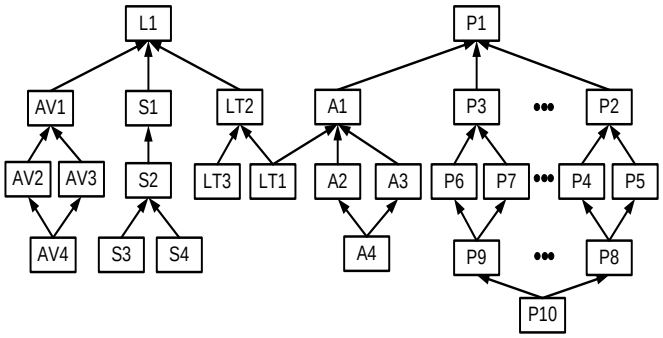

Рис. 1. Иерархическая структура ролей в СОбВ

Так как система облачных вычислений – это система, в которой взаимодействуют поставщик и потребитель облачных услуг, в статье предложено 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 (L1), для потребителя, соответственно, – технического директора потребителя облачных услуг (P1).

В общем случае иерархия ролей потребителя будет иметь больше уровней и будет более распределенной. В примере, проиллюстрированном иерархией ролей на рисунке 1, потребитель облачных услуг имеет два подразделения, осу-

ществляющих 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 (P8, P9, P10), а максимальная – руководителям подразделений потребителя облачных услуг, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами (P2, P3). 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 (A1), а минимальная – администратору штатных средств защиты (A4), 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 (L1), 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 (LT1, LT2, LT3) поддержки, 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 [9]:

– сотрудники *первой линии* техподдержки поставщика облачных услуг (LT1), которые при обращении к ним потребителя ликвидируют технические сбои в инфраструктуре, влияющие на предоставляемые пользователям сервисы; данные сотрудники не обладают высокими привилегиями в СОбВ, не имеют доступа к сервисам безопасности СОбВ;

– сотрудники *второй линии* техподдержки поставщика облачных услуг (LT2) –группа специалистов высокого профиля, которая обладает достаточной компетенцией и способна решать проблемы как с инфраструктурой СОбВ, так и с ее сервисами;

– сотрудники *третьей линии* техподдержки поставщика облачных услуг (LT3) являются сотрудниками разработчика и производителя технологии облачных вычислений (Amazon, Google, Microsoft).

Служба автоматизации облачной среды ответственна 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 (S1), а минимальными ролями будут обладать администратор инфраструктуры ИСОТ (S3) и эксперт по виртуализации в облачных вычислениях (S4).

Служба информационной безопасности поставщика облачных услуг отвечает за безопасность облачной среды со стороны поставщика облачных услуг. В данной службе роли распределены на три составляющие защиты облака: защита программного обеспечения и платформ поставщика услуги SaaS (роль AV2), защита облачной инфраструктуры поставщика услуги SaaS (роль AV3) и защита кластера физических серверов поставщика облачных услуг (роль AV4). Максимальной в данной службе будет роль начальника службы безопасности облачного поставщика (AV1), а минимальной – специалист по защите кластера физических серверов поставщика облачных услуг (AV4).

Иерархия ролей пользователей СОбВ 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 $r_i \leq r_j$, то $r_i \in UA(u)$. При этом для $r_i \leq r_j$ выполняется одно из условий: 1) $r_i = x_i\_read$, $r_j = x_j\_read$, $x_i \leq x_j$; 2) $r_i = x_i\_write$, $r_j = x_j\_write$, $x_j \leq x_i$ [8], где U – множество пользователей, R – множество ролей. Модель контролирует назначение пользовательской роли посредством отношения *can-assign* $ARx\text{-}CRx2^R$.

О*тношение 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) ко-

торого в постоянных ролях удовлетворяет условию необходимой предпосылки ***y***, членом постоянных ролей ***a***, ***b*** или ***c***.

Для иерархии ролей пользователей СОбВ выполняются следующие ограничения [8]:

– ограничение функции UA – для каждого пользователя u ∈ U роль x_read = ⊕ (UA(u) ∩ {y_read | y ∈ L}) UA(u) (здесь x = c(u)) и x_write = ⊕{y_write | y ∈ L} ∈ UA(u) (здесь x = =⊗L);

– ограничения функции roles – для каждой сессии s ∈ S множество ролей roles(s) = ={x_read, x_write};

– ограничения функции PA – должно выполняться для каждого x ∈ L доступ (o, read) ∈ PA(x_read) тогда и только тогда, когда доступ (o, write) ∈ PA(x_write); для каждого доступа (o, read) существует единственная роль x_read: (o, read) ∈ PA(x_read) (здесь x = c(o)).

РАЗРАБОТКА МАТРИЦЫ РАЗГРАНИЧЕНИЯ ДОСТУПА

Поставщик облачных услуг ни в коем случае не должен обладать какими-либо правами доступа к информации, которую обрабатывает потребитель в облаке. К такой информации относятся образы виртуальных машин потребителя, информационные ресурсы, хранящиеся в облачном хранилище, информационные ресурсы, хранящиеся на стороне потребителя облачных услуг и экземпляры, запускаемые в физической операционной среде (физическом кластере поставщика). Кроме того, администраторы безопасности потребителя облачных услуг конфигурируют собственные виртуальные машины и конфигурационные файлы, относящиеся к конкретному потребителю, должны быть скрыты от служб поставщика.

Одновременно с этим поставщик обладает правами на управление и конфигурирование внутриоблачного пространства и собственных сервисов безопасности, чтобы осуществить защиту данных конкретного потребителя не только от злоумышленников, но и от других потребителей услуг облака.

Таким образом, руководитель подразделения и сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по проекту 1 в соответствии с бизнес-процессами предприятия могут читать образы виртуальных машин (o3) по проекту 1 и имеют полный доступ на собственные экземпляры, запускаемые в физической операционной среде (o11). Соответственно, руководитель подразделения и сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по проекту 2 в соответствии с бизнес-процессами предприятия могут читать образы виртуальных машин (o3) по проекту 2 и имеют полный доступ на собственные экземпляры, запускаемые в физической операционной среде (o11). Вносить изменения в настройки конфигурационных файлов образов виртуальных машин и экземпляров, запускаемых в физической операционной среде, обоих проектов могут администратор безопасности потребителя облачных услуг и менеджер ИСОТ. Начальник отдела автоматизации и безопасности потребителя облачных услуг и технический директор обладают полными правами по отношению к образам и экземплярам проектов своей организации.

Информационные ресурсы по проектам, хранящиеся в облачном хранилище (o4), и информационные ресурсы по проектам, хранящиеся на стороне потребителя облачных услуг (o10), доступны с полными правами руководителю соответствующего подразделения и сотрудникам потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по соответствующему проекту в соответствии с бизнес-процессами предприятия, а также техническому директору потребителя облачных услуг.

К файлам СОбВ, относящимся к конфигурированию собственных виртуальных машин конкретным потребителем облачных услуг (o5), имеют полные права менеджер ИСОТ, начальник отдела автоматизации и безопасности потребителя и технический директор потребителя.

Правами на чтение множества логинов и паролей личных кабинетов сотрудников потребителя облачных услуг (o2) обладают сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ в соответствии с бизнес-процессами предприятия. Данное множество доступно для специалиста по защите программного обеспечения и платформ и начальника службы безопасности облачного поставщика с правом вносить правки. Полными правами на доступ ко множеству логинов и паролей обладают руководители подразделений потребителя, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами, начальник отдела автоматизации и безопасности потребителя и технический директор потребителя.

Чтение сайта поставщика облачных услуг (o1) могут осуществить все сотрудники потребителя облачных услуг без исключения. Кроме того, только правами на чтение сайта обладают следующие сотрудники поставщика облачных услуг: эксперт по виртуализации, специалист по

защите кластера физических серверов, специалист по защите облачной инфраструктуры, администратор инфраструктуры ИСОТ, специалисты первой и третьей линии техподдержки потребителя облачных услуг, специалист по защите программного обеспечения и платформ, начальник службы безопасности облачного поставщика. Полными правами на доступ к сайту обладают главный специалист ИСОТ, руководитель службы автоматизации ИСОТ, сотрудник второй линии техподдержки потребителя облачных услуг и технический директор поставщика облачных услуг.

Данные об объеме предоставленных потребителю услуг (о9) доступны по чтению руководителям подразделений потребителя, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами, сотрудникам службы автоматизации ИСОТ и техническому директору потребителя. Кроме того, прочесть эти данные могут специалист по защите облачной инфраструктуры, начальник службы безопасности облачного поставщика, сотрудник первой линии техподдержки, сотрудники службы автоматизации ИСОТ. Правами на чтение и на внесение правок в объем предоставленных потребителю услуг имеют только сотрудник второй линии техподдержки, руководитель службы автоматизации ИСОТ и технический директор поставщика облачных услуг.

Данные о серверном времени, скорости доступа и обработки данных, а также объем хранимых в облачном хранилище данных (о7) доступны по чтению руководителям подразделений потребителя, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами, администратору штатных средств защиты потребителя и администратору безопасности потребителя. Со стороны поставщика эти данные доступны по чтению для специалиста по защите облачной инфраструктуры, начальнику службы безопасности облачного поставщика, главному специалисту ИСОТ, администратору инфраструктуры ИСОТ и эксперту по виртуализации в облачных вычислениях. Полный доступ к объекту 7 имеют менеджер ИСОТ, начальник отдела автоматизации и безопасности потребителя облачных услуг и технический директор потребителя, а также руководитель службы автоматизации облачной среды, сотрудники первой и второй линии техподдержки потребителя облачных услуг и технический директор поставщика облачных услуг.

Данные о фактическом распределении доступа в едином пуле облака (о8) доступны по чтению со стороны поставщика специалисту по защите облачной инфраструктуры, начальнику службы безопасности облачного поставщика и эксперту по виртуализации в облачных вычислениях. Полный доступ к этим данным имеет руководитель и главный специалист службы автоматизации ИСОТ, сотрудники первой и второй линии техподдержки потребителя облачных услуг и технический директор поставщика облачных услуг. Так как начальник отдела автоматизации и безопасности потребителя, а также технический директор потребителя, наследуют все права сотрудника первой линии техподдержки, который в свою очередь является сотрудником поставщика облачных услуг, то они также имеют полный доступ к данным о фактическом распределении доступа в едином пуле облака.

Конфигурационные файлы внутриоблачного пространства и файлы поставщика, отвечающие за конфигурирование собственных средств безопасности поставщика (о6), должны быть закрыты для доступа любому сотруднику потребителя облачных услуг в целях повышения защищенности всей системы облачных вычислений. Вносить правки в файлы СОбВ, относящиеся к управлению внутриоблачным пространством поставщиком облачных услуг, может сотрудник третьей линии техподдержки потребителя, а по чтению они доступны специалисту по защите программного обеспечения и платформ поставщика и начальнику отдела безопасности поставщика. Полным доступом к файлам управления внутриоблачным пространством обладают сотрудники службы автоматизации (руководитель, главный специалист, администратор инфраструктуры и эксперт по виртуализации), сотрудники второй линии техподдержки и технический директор поставщика облачных услуг.

К файлам СОбВ, относящимся к сервисам безопасности поставщика облачных услуг, имеют полный доступ все сотрудники службы безопасности поставщика облачных услуг (начальник службы, специалист защите ПО и платформ, специалист по защите инфраструктуры и специалист по защите кластера физических серверов), а также технический директор поставщика облачных услуг.

С учетом приведенных выше условий и ограничений разработана матрица доступа ролей пользователей (субъектов доступа) СОбВ к множеству объектов доступа (табл. 3).

Таблица 3

Матрица прав доступа ролей пользователей СОбВ

	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	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

ПОЛУЧЕННЫЕ РЕЗУЛЬТАТЫ

Полученные в виде матрицы разграничения доступа результаты применяются при настройке средств контроля доступа в системе облачных вычислений и для определения полномочий прав пользователей (или запущенных ими процессов) на осуществление тех или иных процедур над защищенными данными. В СОбВ используются IP-адреса, каждый из которых ассоциируется с учетной записью клиента облачных вычислений. Для запуска виртуальной машины каждому IP-адресу должны быть присвоены соответствующие атрибуты, указывающие, какие учетные записи облачного web-сервиса имеют право запускать ту или иную конкретную виртуальную машину.

ЗАКЛЮЧЕНИЕ

В данной статье представлены результаты разработки частной политики информационной безопасности системы облачных вычислений.

Достоинством предложенной в статье частной политики информационной безопасности системы облачных вычислений, построенной с помощью формальной модели, основанной на математической модели ролевого разграничения доступа, 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 системы облачных вычислений.

В статье предлагается ввести в иерархию формальной модели две максимальные роли: одну со стороны поставщика потребителя 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.

Дальнейшие исследования предполагается продолжить в направлении разработки иерархической структуры административных ролей в проекции на сформированное множество субъектов и объектов доступа для системы облачных вычислений.

СПИСОК ЛИТЕРАТУРЫ

1. **Шаньгин В. Ф.** Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2012. 592 с. [*V.F. Shangin Information security in computer systems and networks, (in Russian). Moscow: DMK Press,2012.*]

2. **Демурчев Н. Г., Ищенко С. О.** Проблемы обеспечения информационной безопасности при переходе на облачные вычисления // Материалы XI Международной научно-практической конференции «Информационная безопасность»: Ч. 1. Таганрог: Изд-во ТТИ ЮФУ, 2010. С. 147–151. **[** *N. G. Demurchev and S. O. Ishchenko, "Problems of information security in the transition to cloud computing" in Proc. 11th Workshop on Information Security, Taganrog, 2010, vol. 1, pp. 147-151.* **]**

3. **Машкина И. В., Сенцова А.Ю.** Методология экспертного аудита в системе облачных вычислений // Безопасность информационных технологий. 2013. № 4. С. 63–70. **[** *I. V. Mashkina and A. U. Sentsova, "The methodology of expert audit in the cloud computing system," (in Russian), in Besopasnost informacionnyh tehnologiy, no. 4, pp. 63–70, 2013.* **]**

4. **ГОСТ Р 50922-2006.** Защита информации. Основные термины и определения М.: Стандартинформ, 2007. 12 с. *[Protection of information. Basic terms and definitions, (in Russian), Federal standard R ISO/IEC 50922-2006, Moscow, Standatrinform, 2007.* **]**

5. **ГОСТ РХХХХХ-20ХХ** (проект. первая редакция) Защита информации. Требования по защите информации, обрабатываемой с использованием технологий «Облачных вычислений». М.: Стандартинформ. 114 с. *[Protection of information. Requirements for the protection of information processed using the technology of "Cloud computing", (in Russian), Federal standard project, Moscow, Standartinform, 114 pp.* **]**

6. **Варлатая С. К., Шахинова М. В.** Анализ методов описания политики безопасности при разработке информационно-безопасных технологий. // Доклады ТУСУР: Ч. 1 Аудит безопасности, 2010, №1 (21). С. 10–13. **[** S.K. Varlataya and M. V. Shakhinova, "The analysis of methods of the description of the security policy by working out of information-safe tehnologies", (in Russian), Doklady TUSUR,Tomsk, 2010, vol. 1, pp. 10-13. **]**

7. **РС БР ИББС-2.0-2007** Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0. М.: Стандартинформ, 2007. 15 с. *[* Recommendations in standardization of the Bank of Russia. Ensuring the information security of organizations of Bank system of the Russian Federation. Guidelines on documentation to ensure information security in accordance with the requirements of STO BR IBBC-1.0*., (in Russian), Bank Russia standard RC BR IBBS-2.0-2007, Moscow, Standartinform, 2007.* **]**

8. **Шаньгин В.Ф.** Информационная безопасность компьютерных систем и сетей. М.: ДМК Пресс, 2011. 416 с. [*V.F. Shangin Information security in computer systems and networks, (in Russian). Moscow: DMK Press,2011.*]

9. **Методология** организации технической поддержки [Электронный ресурс] URL: http://msbro.ru/index.php/archives/2717 (дата обращения 19.01.2016). **[** Methodology technical support [Online]. Available: http://msbro.ru/index.php/archives/2717**]**

ОБ АВТОРАХ

СЕНЦОВА Алина Юрьевна, дипл. спец. по защите информации (УГАТУ, 2013). Готовит дисс., посвященную экспертному аудиту безопасности в облачных вычислениях.

МАШКИНА Ирина Владимировна, дипл. инж.-э/мех. (УАИ, 1974). Д-р техн. наук (УГАТУ, 2009). Иссл. в обл. управления защитой информации.

METADATA

Title The development private information security policy in the cloud computing system.

Authors: A.U. Sentsova[1], I. V. Mashkina[2]

Affiliation:

[1,2] Ufa State Aviation Technical University (UGATU), Russia.

Email: [1] sentsova.alina@yandex.ru

.**Language:** Russian.

Source: Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), vol. 20, no. 2 (72), pp. 134-142, 2016. ISSN 2225-2789 (Online), ISSN 1992-6502 (Print).

Abstract: The development private information security policy in the cloud computing system is discussed. A mathematical model of role-based access control is proposed to use the algorithm is described. The sets of access objects and access subjects to cloud computing system are defined. The possibilities list for objects access and access subjects, which can be basis for development security policies in cloud computing system, are defined.

Key words: cloud computing system, private information security policy, role based access control, role hierarchy.

About authors:

SENTSOVA, Alina Urievna, Postgrad. (PhD) Student, Dept. of Computing Equipment and Information Protection. Specialist of information protection (UGATU, 2013).

MASHKINA, Irina Vladimarovna, Prof., Dept. of Computing Equipment and Information Protection. Dipl. Electrical engineer (UAI., 1974). Dr. of Tech. Sci. (UGATU, 2009).