УДК 004.056.5

И. В. Машкина, д-р техн. наук, проф., e-mail: mashkina.vtzi@gmail.com,
А. Ю. Сенцова, аспирант, ассистент кафедры ВТиЗИ, e-mail: sentsova.alina@yandex.ru
ФГБОУ ВПО "Уфимский государственный авиационный технический университет", г. Уфа

Обеспечение информационной безопасности системы облачных вычислений*

Работа посвящена разработке модели угроз и частной политики информационной безопасности системы облачных вычислений. Модель угроз разрабатывается в виде нечеткой когнитивной карты, которая позволяет выполнить моделирование процессов распространения угроз информационной системе, построенной с использованием технологии облачных вычислений, через эксплуатируемые уязвимости компонентов ее инфраструктуры. Формирование частной политики безопасности основано на использовании модели ролевого разграничения доступа.

Ключевые слова: *облачные вычисления, облако сообщества, система облачных вычислений, поставщик облачных услуг, потребитель облачных услуг, модель угроз, нечеткая когнитивная карта, частная политика безопасности, иерархия ролей*

Введение

Сегодня в индустрии информационных технологий можно наблюдать стремительные темпы развития информационных систем, построенных на основе технологии облачных вычислений (ИСОТ) [1], однако при этом недостаточно широко освещены 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.

В NIST [2] описываются четыре модели развертывания облачных вычислений: частное облако (*private*), облако сообщества (*community*), публичное облако (*public*), и гибридное облако (*hybrid*). Различные модели развертывания облаков подразумевают различное размещение контролируемого потребителем периметра безопасности и, следовательно, разный уровень контроля, который подписчики могут осуществлять в отношении ресурсов, доверяемых облаку.

В работе рассматривается облако сообщества, которое представляет собой вычислительное облако, используемое несколькими организациями, решающими общие задачи. Облако сообщества может находиться в совместной собственности сообщества, управляться одним или несколькими членами сообщества, а также быть в юрисдикции третьей стороны (поставщика облачных услуг). С точки зрения информационной безопасности облако сообщества можно разделить на несколько систем облачных вычислений (СОбВ) — систем информационного взаимодействия поставщика с конкретным потребителем облачных услуг. В каждой СОбВ обязательно должна быть введена собственная политика информационной безопасности, установлены соответствующие барьеры в целях защиты критичных информационных активов потребителя облачных услуг не только от злоумышленника, неправомерных действий сотрудников служб поставщика облачных услуг и сотрудников потребителя (внутренних нарушителей), но и от неправомерных действий других членов облака сообщества, являющихся в этом случае внешними нарушителями по отношению к СОбВ. Концепция облака сообщества представлена на рис. 1.

Разработка обобщенной архитектуры системы облачных вычислений

Любое вычислительное облако представляет собой систему, построенную на основе клиент-серверной архитектуры. Модель клиент-серверного взаимодействия характеризуется наличием двух взаимодействующих процессов — клиента и сервера. Архитектура облачных вычислений является

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

Рис. 1. Концепция облака сообщества и СОбВ

более современной версией известных схем клиент-серверных взаимодействий.

Есть ряд задач, которые не требуют средств виртуализации, однако решение все равно будет считаться облачным. В каждом случае, для каждого конкретного потребителя облачная архитектура может быть выполнена с использованием различных компонентов, зависящих от конкретных бизнес-процессов, которые будут выполняться в облаке.

Оценить уровень защищенности СОбВ в общем виде, без учета особенностей облачной инфраструктуры не только поставщика, но и потребителя облачных услуг невозможно. В результате проведенного анализа возможных схем клиент-серверных взаимодействий, облачного решения Azure [3] и концепции вычислительного облака для обеспечения услуги SaaS (программное обеспечение как услуга), представленной в ГОСТ [4], в данной работе предложена модель инфраструктуры *системы облачных вычислений* для облака сообщества, представленная на рис. 2.

При разработке варианта инфраструктуры СОбВ учтены требования для типовой ИСОТ и требования архитектуры безопасности.

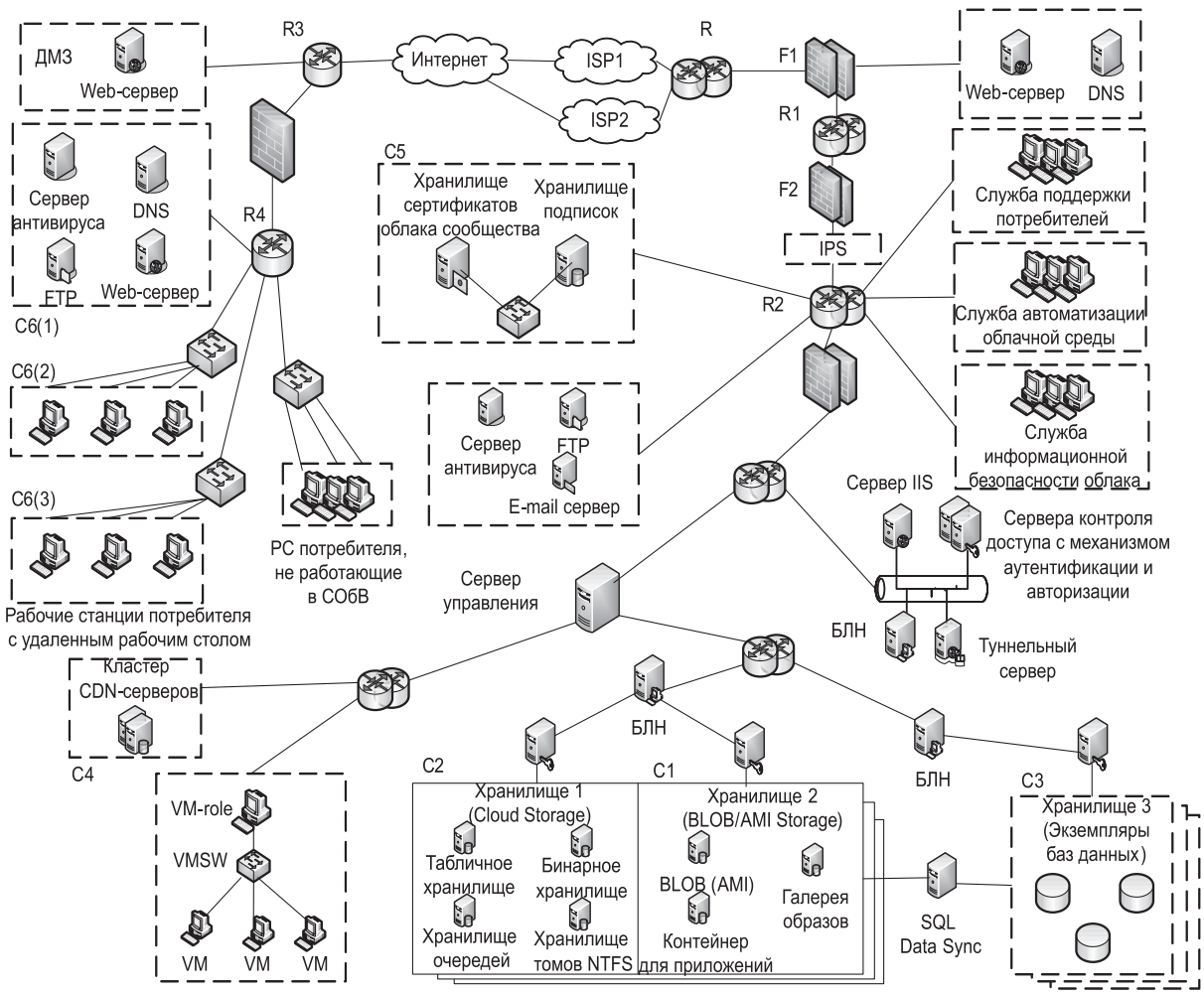

Рис. 2. Модель инфраструктуры системы облачных вычислений

Согласно ГОСТ [4] в состав ИСОТ входят следующие компоненты:

- со стороны потребителя облачных услуг: рабочие станции сотрудников потребителя облачных услуг с удаленным рабочим столом, облачные периферийные устройства и ПО (облачный клиент), сетевое оборудование для осуществления межоблачного взаимодействия;
- со стороны поставщика облачных услуг: пограничный сервер для потребителя (сервер IIS), функциональные серверы для обеспечения бизнес-процессов потребителя облачных услуг, хранилища данных (представлены в архитектуре тремя хранилищами), сетевое оборудование, включая сетевое оборудование для осуществления межоблачного взаимодействия.

Сеть потребителя облачных услуг представлена *минимальным* набором простейших компонентов инфраструктуры.

Инфраструктура информационной системы поставщика включает в себя *пограничный сервер* для связи с конкретным потребителем, реализованный в виде *сервера IIS*, серверы контроля доступа с механизмом аутентификации и авторизации для входа в рабочую часть вычислительного облака потребителя, *тремя службами потребителя облачных услуг,* а также служебными *серверами для выдачи и хранения сертификатов* членов облака сообщества *и данных о подписках* каждого потребителя. Весь трафик аутентификации и авторизации потребителя, а также трафик, содержащий обрабатываемые в облаке критичные активы потребителя облачных услуг, шифруется с помощью туннельного сервера, а доступность сервера IIS гарантируется балансировщиком нагрузки (БЛН).

В рабочей области облака доступ к хранилищам и виртуальным машинам осуществляется с помощью *сервера управления* облаком. *Кластер CDN серверов (Content Delivery Network)* хранит контент сети доставки облака и является отдельно заказываемой функцией облака сообщества для обеспечения более быстрого доступа к наиболее часто используемым данным потребителя.

Администратор потребителя облачных услуг управляет всей сетью виртуальных машин (ВМ) с помощью специализированной ВМ — *VM-role*, к которой через *виртуальный коммутатор* подключены все виртуальные машины потребителя облачных услуг.

Доступ к *хранилищам системы облачных вычислений* осуществляется через БЛН с дополнительной аутентификацией и авторизацией сотрудника потребителя облачных услуг.

Хранилище 1 (*Cloud Storage)* — хранилище, в котором находятся неструктурированные данные потребителя (документы, видеофайлы, чертежи, схемы) и в том числе тома для подключения к вызываемому сотрудником потребителя образу виртуальной машины. Информация для аутентификации и авторизации пользователя для доступа к данному хранилищу прописана в учетной записи пользователя, под именем которого авторизовался в системе сотрудник потребителя облачных услуг.

Хранилище 2 (BLOB/AMI Storage) — хранилище образов виртуальных машин, которое также включает в себя галерею образов и контейнер для приложений. Информация для аутентификации и авторизации пользователя для доступа к данному хранилищу имеет несколько уровней. При низком уровне доступа сотрудник потребителя имеет доступ только к образу виртуальной машины, с которым ему положено работать по бизнес-процессам. Администратор потребителя имеет полный доступ к галерее образов, содержащей "чистые" образы виртуальных машин, а также к контейнеру приложений, в котором находятся все заказанные потребителем облачных услуг приложения, готовые к установке в образ ВМ. Повышение уровня доступа ко второму хранилищу регламентируется политикой безопасности потребителя облачных услуг и находится в юрисдикции компании потребителя облачных услуг.

Хранилище 3 служит для хранения *экземпляров баз данных* потребителя облачных услуг. Для доступа в хранилище также нужно пройти процедуру аутентификации, которая определит конкретный экземпляр базы/баз данных, они должны быть доступны сотруднику потребителя облачных услуг в соответствии с бизнес-процессами.

Совокупность пограничного сервера, функциональных серверов и хранилищ данных, а также сетевого оборудования для поддержки серверов представляет собой *типовой облачный сервер ИСОТ*.

Уровень оборудования представлен маршрутизаторами, коммутаторами и серверами, *уровень управления* — сервером управления и сервисами безопасности, такими как, например, межсетевые экраны, IPS, туннельные серверы шифрования трафика и серверы контроля доступа с механизмами аутентификации и авторизации потребителя облачных услуг.

Типовая *демилитаризованная зона* поставщика облачных услуг включает в себя: публичный web-сервер, DNS-сервер, сервер приложений для управления информационными ресурсами web-портала. В демилитаризованной зоне должна храниться и обрабатываться только общедоступная открытая информация, что отражено в инфраструктуре СОбВ.

Чтобы минимизировать риски потребителя и поставщика в процессе реализации облачных сервисов, внутренний web-сервер для клиент-серверного взаимодействия (сервер IIS) должен быть размещен в другом сетевом сегменте, как и сервер CDN, обеспечивающий временное хранение ресурсов потребителя облачных услуг и позволяющий уменьшить время доступа пользователей к кэшированным данным. В соответствии с требованиями

архитектуры безопасности следует обеспечить сегрегацию этих серверов от общедоступных, располагая их во внутренней защищенной подсети поставщика облачных услуг (во внутренней рабочей области облака).

Разработка частной политики безопасности системы облачных вычислений

Многими экспертами отмечается, что потребитель облачных услуг имеет тот уровень защищенности в облачной среде, который обеспечивается поставщиком [8,9]. Однако для защищенности информации в СОбВ необходимо обратить внимание на разработку политики безопасности всей системы облачных вычислений и гарантированно защитить пользовательские рабочие места на стороне потребителя.

Политика информационной безопасности организации — совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которые регулируют управление, защиту и распределение ценной информации [10].

Политика информационной безопасности разрабатывается на основе сведений о конкретных технологиях обработки информационных активов предприятия, об используемых в данной системе информационных потоках, реализующих деловые процессы. Для устранения угроз, связанных с неопределенностью при распределении ответственности, поставщику облачных услуг необходимо тщательно прорабатывать частную политику безопасности, а именно политику управления доступом, формализованную в виде матрицы доступа. Для составления матрицы доступа необходимо сформировать иерархическую структуру, составленную на основе тщательного анализа возможных ролей поставщика и потребителя облачных услуг.

Как отмечается в работе [11], 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 [12].

Актуальность разработки частных политик информационной безопасности объясняется необходимостью планирования и управления ИБ на всех этапах жизненного цикла ИСОТ и СОбВ. 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, т. е. повысить защищенность информации при обработке ее в СОбВ.

В ходе исследований разработана модель политики информационной безопасности СОбВ, включающая перечень частных политик ИБ с их детализацией:

- политика идентификации и аутентификации субъектов доступа и объектов доступа;
- *политика управления доступом субъектов доступа к объектам доступа*;
- политика ограничения программной среды;
- политика менеджмента инцидентов ИБ;
- политика антивирусной защиты СОбВ;
- политика средств обнаружения вторжений;
- политика по контролю (анализу) защищенности;
- политика обеспечения целостности ПО СОбВ;
- политика информационной безопасности облачного сервера;
- политика межсетевого экранирования;
- политика централизованного управления СОбВ.

Таким образом, для обеспечения защищенности необходимо создание частных политик, которые должны неукоснительно соблюдаться как поставщиком, так и потребителем облачных услуг.

Приведем методику разработки одной из частных политик ИБ СОбВ — политики управления доступом субъектов доступа к объектам доступа, которая строится на основе ролевой модели и детализирована следующим образом:

- реализация необходимых методов и правил разграничения доступа в ходе межоблачного взаимодействия;
- разделение обязанностей, полномочий (ролей), всех линий администраторов поставщика;
- назначение минимально необходимых правил и привилегий пользователям СОбВ и сотрудникам поставщика облачных услуг;
- разграничение доступа к объектам, расположенным за пределами виртуальных машин.

Использование ролевой модели требует решения задач выявления множества субъектов, специфичных объектов доступа для такого объекта защиты как СОбВ, построения иерархических схем ролей с учетом функций субъектов как со стороны поставщика, так и со стороны потребителя облачных услуг. Далее здесь под частной политикой безопасности СОбВ следует понимать политику управления доступом.

Разработка частной политики безопасности СОбВ позволяет избежать угроз информационной безопасности, связанных с неопределенностью от-

ветственности в системе облачных вычислений, реализация которых способна привести к существенным разногласиям между поставщиком и потребителем облачных услуг по вопросам, связанным с определением их прав и обязанностей.

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.

Установим для информационных объектов в СОбВ следующие уровни конфиденциальности:

Таблица 1

Множество информационных объектов доступа 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) ...	Виртуальные машины отдела потребителя облачных услуг, осуществляющего работу по проекту 1	СК
o3 (i)	Виртуальные машины отдела потребителя облачных услуг, осуществляющего работу по проекту *i*	СК
o4 (1) ...	Информационные ресурсы по проекту 1, хранящиеся в облачном хранилище	СК
o4 (i)	Информационные ресурсы по проекту *i*, 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 (i)	Информационные ресурсы по проекту *i*, 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 (i)	Экземпляры отдела, работающего по проекту *i*, запускаемые в физической операционной среде (физическом кластере поставщика облачных услуг)	СК

ОИ — открытая информация, К — конфиденциально, СК — строго конфиденциально

В результате исследований выявлено множество информационных объектов для системы облачных вычислений (табл. 1).

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

Таблица 2

Множество субъектов доступа в СОбВ

Обозначение	Наименование	Уровень доступа
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 SaaSИСОТ (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	Сотрудники подразделения потребителя облачных услуг, не работающие по проектам 1 и 2, и не имеющие права эксплуатировать СОбВ в соответствии с бизнес-процессами	ОИ

Так как система облачных вычислений — это система, в которой взаимодействуют поставщик и потребитель облачных услуг, в работе предложено модифицировать ролевую модель разграничения доступа таким образом, чтобы каждая из представленных сторон (потребитель и поставщик) имела свою максимальную роль в иерархии, в отличие от известной ролевой модели разграничения доступа, где максимальная роль в иерархии может быть только одна. Для поставщика облачных услуг примем, что максимальной ролью является роль технического директора поставщика (L1), для потребителя, соответственно, — технического директора потребителя облачных услуг (P1).

В общем случае иерархия ролей потребителя будет многоуровневой и распределенной. На рис. 3 представлена разработанная иерархическая структура ролей для множества информационных субъектов и объектов при $i = 2$.

В примере, проиллюстрированном рис. 3, 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 (P8, P9, P10), а максимальная роль — 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 доступа 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 роль — 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: службы поддержки потребителей облачных услуг; службы автоматизации облачной среды; 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 [13]:

- 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, и 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. Максимальную роль в данной службе будет иметь руководитель службы автоматизации ИСОТ (S1), а минимальными ролями будут обладать администратор инфраструктуры ИСОТ (S3) и эксперт по виртуализации в облачных вычислениях (S4).

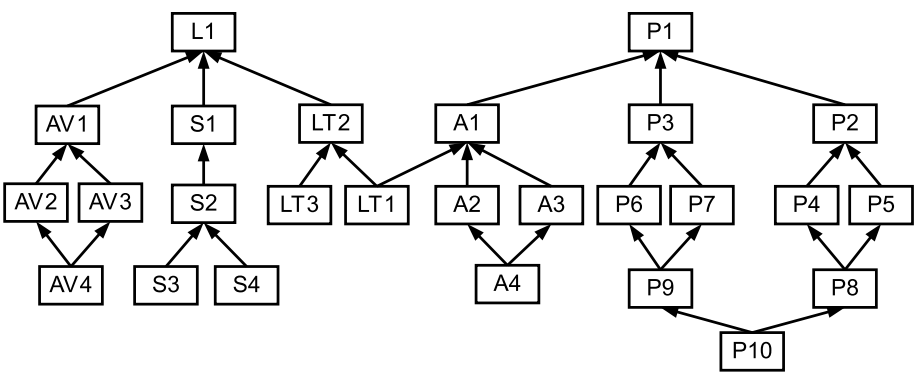

Рис. 3. Иерархическая структура ролей в СОбВ

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: защиты программного обеспечения и платформ поставщика услуги SaaS (роль AV2); защиты облачной инфраструктуры поставщика услуги SaaS (роль AV3); защиты кластера физических серверов поставщика облачных услуг (роль AV4). Максимальной в данной службе будет роль начальника службы безопасности облачного поставщика (AV1), а минимальной — специалиста по защите кластера физических серверов поставщика облачных услуг (AV4).

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 виртуальные машины потребителя, информационные ресурсы, хранящиеся в облачном хранилище, информационные ресурсы, хранящиеся на стороне потребителя облачных услуг, и экземпляры, виртуальные машины, запускаемые в физическом кластере поставщика, конфигурационная и управляющая информация потребителя. Администраторы безопасности потребителя облачных услуг конфигурируют собственные виртуальные машины, и конфигурационные файлы, относящиеся к конкретному потребителю, должны быть скрыты от служб поставщика. Таким образом, в СОбВ используются IP-адреса, каждый из которых ассоциируется с учетной записью клиента, а не с конкретным экземпляром виртуальной машины. Для запуска виртуальной машины ей должен быть присвоен атрибут, указывающий, какие учетные записи облачного web-сервиса имеют право запускать конкретную виртуальную машину.

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 и запускать виртуальные машины (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 и запускать виртуальные машины (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, по обоим проектам 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, осуществляющим эксплуатацию СОбВ по заданному 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 доступа 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 для 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.

Читать сайт поставщика облачных услуг (o1) могут все сотрудники потребителя облачных услуг без исключения. Кроме того, правами только 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. Полные права на доступ к сайту имеют 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 объеме 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 о7 (см. табл. 1) 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, содержащие данные о конфигурировании 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, а также начальнику отдела безопасности поставщика. Полный доступ к файлам управления внутриоблачным пространством имеют 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 защиты ПО и платформ, специалист по защите инфраструктуры и специалист по защите кластера физических серверов), а также технический директор поставщика облачных услуг.

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

Разработка модели угроз СОбВ в виде нечеткой когнитивной карты

Обеспечение защищенности СОбВ при разумных вложениях является серьезной актуальной проблемой как для потребителя, так и для поставщика облачных услуг. Как обеспечить защищенность информации, обрабатываемой в облаке? Как оценить уровень риска нарушения безопасности информации, который обеспечивается поставщиком при предоставлении потребителю облачных услуг? Эти вопросы возникают как при проектировании системы обеспечения информационной безопасности инфраструктур поставщика и потребителя, так и в процессе функционирования СОбВ.

Для решения проблемы управления рисками нарушения ИБ в СОбВ необходимо идентифицировать внешние и внутренние факторы, влияющие на риск, и оценить уровень риска в количественном выражении [5].

В рамках данных исследований СОбВ во внимание принимаются угрозы *несанкционированного доступа*, в результате которых происходит получение информации заинтересованным субъектом (злоумышленником или пользователем-нарушителем облака сообщества), с нарушением прав и правил, т. е. угрозы, связанные с нарушением частной политики безопасности.

Таблица 3

Матрица прав доступа ролей пользователей СОбВ

	*o*1	*o*2	*o*3 (1)	*o*3 (2)	*o*4 (1)	*o*4 (2)	*o*5	*o*6 (1)	*o*6 (2)	*o*7	*o*8	*o*9	*o*10 (1)	*o*10 (2)	*o*11 (1)	*o*11 (2)
*L*1	*rw*	*w*	—	—	—	—	—	*rw*	*rw*	*rw*	*rw*	*rw*	—	—	—	—
*LT*2	*rw*	*w*	—	—	—	—	—	*rw*	—	*rw*	*rw*	*rw*	—	—	—	—
*LT*1	*r*	—	—	—	—	—	—	—	—	*rw*	*rw*	*r*	—	—	—	—
*LT*3	*r*	—	—	—	—	—	—	*w*	—	—	—	—	—	—	—	—
*S*1	*rw*	—	—	—	—	—	—	*rw*	—	*rw*	*rw*	*rw*	—	—	—	—
*S*2	*rw*	—	—	—	—	—	—	*rw*	—	*r*	*rw*	*r*	—	—	—	—
*S*3	*r*	—	—	—	—	—	—	*rw*	—	*r*	—	*r*	—	—	—	—
*S*4	*r*	—	—	—	—	—	—	*rw*	—	*r*	*r*	*r*	—	—	—	—
*AV*1	*r*	*w*	—	—	—	—	—	*r*	*rw*	*r*	*r*	*r*	—	—	—	—
*AV*2	*r*	*w*	—	—	—	—	—	*r*	*rw*	—	—	—	—	—	—	—
*AV*3	*r*	—	—	—	—	—	—	—	*rw*	*r*	*r*	*r*	—	—	—	—
*AV*4	*r*	—	—	—	—	—	—	—	*rw*	—	—	—	—	—	—	—
*P*1	*r*	*rw*	*rwe*	*rwe*	*rw*	*rw*	*rw*	—	—	*rw*	*rw*	*r*	*rw*	*rw*	*rw*	*rw*
*A*1	*r*	*rw*	*rw*	*rw*	—	—	*rw*	—	—	*rw*	*rw*	—	—	—	*rw*	*rw*
*A*3	*r*	*rw*	—	*w*	—	—	*rw*	—	—	*rw*	—	—	—	—	*w*	*w*
*A*2	*r*	*rw*	—	*w*	—	—	—	—	—	*r*	—	—	—	—	*w*	*w*
*A*4	*r*	*rw*	—	—	—	—	—	—	—	*r*	—	—	—	—	—	—
*P*2	*r*	*rw*	*re*	—	*rw*	—	—	—	—	*r*	—	*r*	*rw*	—	*rw*	—
*P*4,5	*r*	*r*	*re*	—	*rw*	—	—	—	—	—	—	—	*rw*	—	*rw*	—
*P*8	*r*	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
*P*3	*r*	*rw*	—	*re*	—	*rw*	—	—	—	*r*	—	*r*	—	*rw*	—	*rw*
*P*6,7	*r*	*r*	—	*re*	—	*rw*	—	—	—	—	—	—	—	*rw*	—	*rw*
*P*9	*r*	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—

При решении проблемы оценивания рисков нарушения ИБ в СОбВ предложено осуществить идентификацию угроз, реализуемых за счет использования уязвимостей компонентов инфраструктуры и сервисов безопасности. Любая реализация системы обеспечения информационной безопасности — это схема, содержащая в себе требования к защите объекта и *модель угроз*, отражающую защищаемую среду и состояние оборонительных барьеров.

В работе приведем результаты построения модели угроз в виде нечетких когнитивных карт (НКК). Нечеткие когнитивные карты были разработаны с учетом всех возможных источников угроз, объектов атак и уязвимостей компонентов инфраструктуры СОбВ, расположенных на путях распространения атак.

Когнитивная карта иллюстрирует возможные пути угроз, реализуемых потенциальным злоумышленником и нарушителем, позволяет провести анализ несанкционированного проникновения к информационным ресурсам: показывает, откуда осуществляется атакующее воздействие, какие информационные объекты могут являться целями проведения атак, какими средствами защищена информационная система, какие уязвимости могут быть использованы во время проведения атаки.

Модель угроз в СОбВ, разработанная на основе построения нечетких когнитивных карт, адекватна объекту защиты и позволяет обеспечить оценку уровней угроз. Преимуществом использования НКК в данном приложении в сравнении с какими-либо другими методами является возможность учесть инфраструктуру СОбВ, организовать знания об особенностях распространения угроз в СОбВ, а также формализовать численно неизмеримые факторы, такие как вероятности угроз.

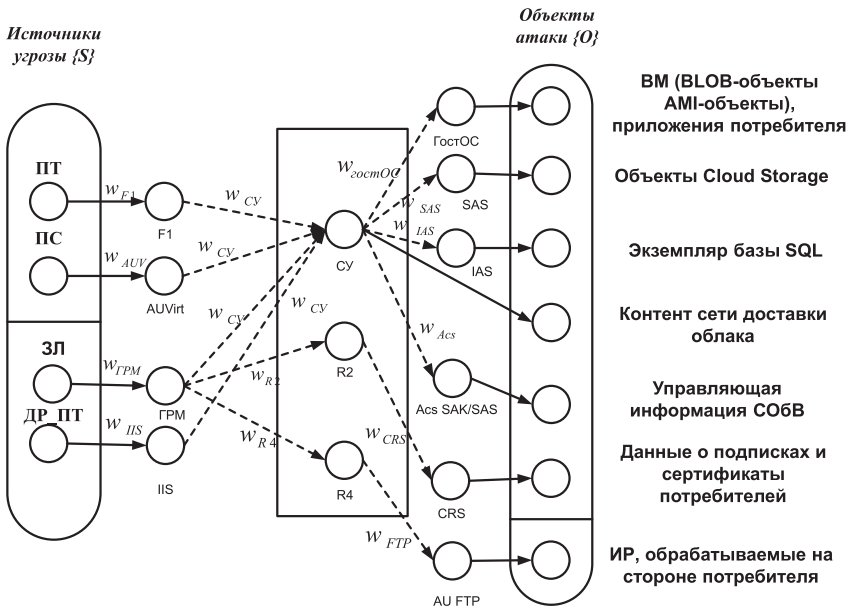

Рис. 4. Обобщенная модель угроз в виде НКК

На рис. 4 представлена обобщенная модель угроз в СОбВ в виде нечеткой когнитивной карты, в которой приведены начальные и конечные уязвимости компонентов инфраструктуры системы облачных вычислений на пути распространения атак.

На рис. 4 использованы следующие обозначения: ПТ — субъект доступа — сотрудник-нарушитель политики управления доступом компании потребителя облачных услуг; ПС — субъект доступа — сотрудник службы поставщика облачных услуг; ДР_ПТ — субъект доступа — сторонний нарушитель — субъект, являющийся другим потребителем облачных услуг облака сообщества (или запущенные им процессы); ЗЛ — субъект доступа — злоумышленник — субъект, не являющийся потребителем облачных услуг (или запущенные им процессы); w — уровни уязвимостей компонентов инфраструктуры СОбВ (веса промежуточных концептов); R — маршрутизатор; IIS — пограничный сервер; AUVirt, SAK, SAS, IAS — серверы аутентификации облака; FTP — файловый сервер; ГостОС — гостевая операционная система; СУ — сервер управления. Оценки уровней уязвимостей получены с использованием методики CVSS и международной базы данных уязвимостей (NVD) [6].

Использование нечетких когнитивных карт позволяет выполнить моделирование процессов распространения угроз в СОбВ через используемые уязвимости ее компонентов. При этом полученная модель обладает свойством *наглядности* и простотой *понимания и перевода* содержательного знания эксперта на математический язык.

Использование НКК для моделирования угроз позволяет провести численную оценку уровня риска по методу работы [7], т. е. оценить уровень защищенности.

Анализ визуализированных путей реализации угроз служит основой для обоснования выбора средств защиты — барьеров на путях реализации угроз (в том числе в виртуальной среде), снижающих значение риска нарушения ИБ до приемлемого уровня, что позволит обеспечить требуемый уровень защищенности СОбВ.

Полученные результаты

Сформированные в виде матрицы правила разграничения доступа 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.

Модель угроз, построенная на основе нечетких когнитивных карт, позволяет выполнить моделирование процессов распространения угроз информационной системе через используемые уязвимости ее компонентов. При этом полученная модель обладает свойством *наглядности* и простотой *понимания*. Анализ визуализированных путей реализации угроз служит основой для обоснования выбора средств защиты — барьеров на пути реализации угроз, снижающих значение риска нарушения ИБ до приемлемого уровня.

Заключение

При разработке частной политики управления доступом в СОбВ предлагается ввести в иерархию две максимальные роли: одну со стороны поставщика потребителя облачных услуг (роль технического директора поставщика облачных услуг), другую со стороны потребителя облачных услуг (роль технического директора потребителя облачных услуг), которые имели бы одновременно и *максимально необходимую роль* в собственном подразделении облака сообщества. *Достоинством* предложенного в работе подхода к разработке частной политики информационной безопасности в системе облачных вычислений на основе модели ролевого разграничения доступа является возможность *исключения* прав *суперпользователя*, который может напрямую обращаться к результирующим потокам данных потребителя облачных услуг и управлять всеми конфигурационными файлами системы облачных вычислений.

Соблюдение требований частной политики безопасности СОбВ позволит существенно снизить риски использования облачных вычислений потребителем облачных услуг и, как следствие, увеличить доверие потенциальных потребителей к ИСОТ.

Разработанная с учетом частной политики безопасности модель преднамеренных (целенаправленных) угроз нарушения информационной безопасности в системе облачных вычислений, основанная на построении нечетких когнитивных карт, позволяет учесть угрозы и уязвимости, связанные с динамической масштабируемостью, консолидацией вычислительных ресурсов, возможностью самообслуживания потребителя облачных услуг, а также учесть такой источник угроз, как другой потребитель облачных услуг.

Список литературы

1. **Барский А.Б, Желенков Б. В.** Средства оптимизации информационного взаимодействия ресурсных процессоров для минимизации времени "облачных" вычислений // Информационные технологии. 2016. Т. 22, № 1. С. 14—21.

2. **NIST.** Официальный сайт. URL: http://www.nist.gov/itl/cloud/ (дата обращения: 28.03.2016).

3. **Авраменко А.** Облачные вычисления. Взгляд из IBM // Jet Info. 2010. № 10. С. 63—75.

4. **Защита** информации. Требования по защите информации, обрабатываемой с использованием технологий "Облачных вычислений" ГОСТ РХХХХХ-20ХХ (проект, первая редакция). URL: http://docs.cntd.ru/document/1200102839 (дата обращения 23.03.2016).

5. **Глушенко С. А., Долженко А. И.** Система поддержки принятия решений нечеткого моделирования рисков информационной безопасности организации // Информационные технологии. 2015. Т. 21, № 1. С. 68—74.

6. **Международная** база данных уязвимостей. Официальный сайт. URL: https://nvd.nist.gov/ (дата обращения: 28.03.2016).

7. **Гузаиров М. Б., Машкина И. В., Степанова Е. С.** Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности // Безопасность информационных технологий. 2011. № 2. С. 37—49.

8. **Шаньгин В. Ф.** Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2012. 592 с.

9. **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.

10. **ГОСТ Р 50922—2006.** Защита информации. Основные термины и определения М.: Стандартинформ, 2007. 12 с.

11. **Варлатая С. К., Шахинова М. В.** Анализ методов описания политики безопасности при разработке информационно-безопасных технологий. // Доклады ТУСУР, Ч. 1. Аудит безопасности. Июнь 2010. № 1 (21). С. 10—13.

12. **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.

13. **Методология** организации технической поддержки. URL: http://msbro.ru/index.php/archives/2717 (дата обращения 28.03.2016).

I. V. Mashkina, DSc, Professor, mashkina.vtzi@gmail.com
A. Yu. Sentsova, Postgraduate Student, sentsova.alina@yandex.ru
Ufa State Aviation Technical University (UGATU), Ufa, Russia

Information Security of Cloud Computing System

The development model of threats and private information security policy cloud computing systems are discussed The threat model on the based of fuzzy cognitive map is developed, which allows modeling the propagation of threats to the information system, built using cloud computing technologies, through the exploited vulnerability of the components of its infrastructure. The formation of the private security policy based on the use of the model RBAC.

Keywords: *cloud computing, community cloud, the cloud computing system, cloud provider, cloud service consumer, the threat model, fuzzy cognitive map, private security policy, a role hierarchy*

References

1. **Barskij A. B., Zhelenkov B. V.** Sredstva optimizacii informacionnogo vzaimodejstvija resursnyh processorov dlja minimizacii vremeni "oblachnyh" vychislenij (Means of optimization of informational interaction of resource processors to minimize the time of "cloud" computing), *Informacionnye tehnologii*, 2016, no. 1, vol. 22, pp. 14—21.

2. **NIST.** Oficial'nyj sajt (The official NIST website), URL: http://www.nist.gov/itl/cloud/ (data of access: 28.03.2016).

3. **Avramenko A.** Oblachnye vychislenija. Vzgljad iz IBM (Cloud computing. A view from IBM), *Jet Info*, 2010, no. 10, pp. 63—75.

4. **Zashhita** *informacii. Trebovanija po zashhite informacii, obrabatyvaemoj s ispol'zovaniem tehnologij Oblachnyh vychislenij* GOST RHHHHH-20HH (proekt. pervaja redakcija) (The protection of information. Requirements for protection of information processed using technologies of Cloud computing), URL: http://docs.cntd.ru/document/1200102839 (data obrashhenija 28.03.2016).

5. **Glushenko S. A., Dolzhenko A. I.** Sistema podderzhki prinjatija reshenij nechetkogo modelirovanija riskov informacionnoj bezopasnosti organizacii (Support system decision making fuzzy modeling information security risk organization), *Informacionnye tehnologii*, 2015, vol. 21, no. 1, pp. 68—74.

6. **Mezhdunarodnaja** baza dannyh ujazvimostej Oficial'nyj sajt (The official website of the national vulnerabilities database), URL: https://nvd.nist.gov/ (data of access: 28.03.2016).

7. **Guzairov M. B., Mashkina I. V., Stepanova E. S.** Postroenie modeli ugroz s pomoshh'ju nechetkih kognitivnyh kart na osnove setevoj politiki bezopasnosti (The building threat models using fuzzy cognitive maps based on network security policy), *Bezopasnost' informacionnyh tehnologij*, 2011, no. 2, pp. 37—49.

8. **Shan'gin V. F.** *Zashhita informacii v komp'juternyh sistemah i setjah* (Information security in computer systems and networks), Moscow: DMK Press, 2012, 592 p.

9. **Demurchev N. G., Ishhenko S. O.** Problemy obespechenija informacionnoj bezopasnosti pri perehode na oblachnye vychislenija (Problems of information security in the transition to cloud computing), *Materialy XI Mezhdunarodnoj nauchno-prakticheskoj konferencii "Informacionnaja bezopasnost'"*, Ch. 1. Taganrog: Izd-vo TTI JuFU, 2010, pp. 147—151.

10. **GOST R 50922—2006.** *Zashhita informacii. Osnovnye terminy i opredelenija* (The protection of information. Key terms and definitions). M.: Standartinform, 2007, 12 p.

11. **Varlataja S. K., Shahinova M. V.** Analiz metodov opisanija politiki bezopasnosti pri razrabotke informacionno-bezopasnyh tehnologij. (The analysis of methods of the description of the security policy by working out of information-safe tehnologies), *Doklady TUSUR, Ch. 1 "Audit bezopasnosti"*, ijun' 2010, no. 1 (21), pp. 10—13.

12. **PC BR IBBS-2.0—2007.** *Rekomendacii v oblasti standartizacii Banka Rossii.* Obespechenie informacionnoj bezopasnosti organizacij bankovskoj sistemy Rossijskoj Federacii. Metodicheskie rekomendacii po dokumentacii v oblasti obespechenija informacionnoj bezopasnosti v sootvetstvii s trebovanijami STO BR IBBS-1.0. (Recommendations standardization of the Bank of Russia. Ensuring the information security of organizations of Bank system of the Russian Federation. Guidelines for documentation in the field of information security in accordance with the requirements of STO BR IBBS-1.0.), Moscow, Standartinform, 2007. 15 p.

13. **Metodologija** *organizacii tehnicheskoj podderzhki* (Methodology technical support). URL: http://msbro.ru/index.php/archives/2717 (data of access: 28.03.2016).