

ПОСТРОЕНИЕ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ В ОБЛАЧНЫХ ТЕХНОЛОГИЯХ НА ОСНОВЕ МНОГОАГЕНТНОГО ПОДХОДА С ИСПОЛЬЗОВАНИЕМ АВТОМАТНОЙ МОДЕЛИ

Боровский А. С.¹, Ряполова Е. И.²

В данной статье предлагается использование многоагентного подхода при построении модели системы защиты облачных вычислений, модель строится на основе эталонной архитектуры облачных вычислений NIST разработанной Национальным институтом стандартов и технологий США с выделением значимого агента безопасности, ему уделяется особая роль в системе защиты облачных вычислений. Он отвечает за формирование запросов от пользователей системы, мониторинг запросов пользователей и взаимодействие акторов в системе облачных вычислений. Система мониторинга поведения пользователей и акторов в системе облачных вычислений предлагается построить с использованием автоматной модели. Выделение агента безопасности необходимо с одной стороны в связи с увеличением количества коммерческих предприятий переходящих на платформу облачных вычислений, с другой стороны необходимостью данные ресурсы и данные защищать.

В статье так же представлены ряд сценариев взаимодействия акторов с учетом выделенного агента безопасности. Агент безопасности в данном случае выполняет контролирующую и связующую роль между всеми акторами модели, проводя мониторинг и распознавание несанкционированных действий как со стороны облачных пользователей, так и со стороны акторов системы.

Модель контроля поведения облачного пользователя и взаимодействия акторов в облачной системе представляет собой сигнатурную модель поиска запрещенных действий в системе облачных вычислений.

Для определения угроз безопасности системы облачных вычислений построена модель потоков данных.

Ключевые слова: модель системы защиты облачных технологий, многоагентный подход, защита облачных вычислений, автоматная модель, облачные вычисления, облачные технологии.

DOI: 10.21681/2311-3456-2017-4-10-20

Введение

Многоагентный подход широко используется при создании программных средств информационных систем, отвечающих за решение ряда задач начиная с задач поиска информации и заканчивая задачами управления и распознавания образов. Исследовательские работы в области использования многоагентного подхода проводятся давно, но задача построения универсальной модели многоагентной системы облачных вычислений до сих пор не решена из-за сложности и разнообразия использования аппаратных и программных платформ.

Учеными Национального института стандартов и технологий США разработана эталонная архи-

тектура облачных вычислений состоящая из 5 акторов (NIST)³.

Основным недостатком данной модели является отсутствие агента безопасности отвечающего за безопасное взаимодействие всех акторов системы. В данной модели не осуществляется мониторинг действий облачного пользователя, так же не представлен актор отвечающий за безопасность облачной системы в целом. Отсутствие данного актора может привести к утечке информации, несанкционированному доступу и искажению информации, использованием злоумышленника информации в своих целях. Данный недостаток является существенным, а система требует доработки.

- 1 Боровский Александр Сергеевич, доктор технических наук, доцент, заведующий кафедрой «Управления и информатики в технических системах» ФГБОУ ВО «Оренбургский государственный университет» г. Оренбург, Россия, borovski@mail.ru
- 2 Ряполова Елена Ивановна, кандидат педагогических наук, доцент кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Оренбургский государственный университет», г. Оренбург, Россия, ananeva_ei@mail.ru
- 3 NIST Референтная (эталонная) архитектура облачных вычислений (Cloud Computing Reference Architecture) Версия 1.0. [Электронный ресурс] // О Cloud Computing [сайт]. URL: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (дата обращения: 22.07.2017)

В статье О.Ю. Песковой, К.Е. Степовой рассмотрена референтная архитектура облачных вычислений с выделением 5 акторов и представлен ряд требований по обеспечению безопасности облачных сервисов. Авторы акцентируют внимание на ряде организационных и технических требований, но не раскрывают технологию обеспечения безопасности в системе облачных вычислений [1-3].

Авторами ряда статей определены требования к системе защиты информации для виртуальной инфраструктуры, построены модели нарушителя и модели угроз, но в модели виртуальной инфраструктуры отсутствует подсистема, отвечающая за безопасность функционирования системы в целом [4-9].

Опираясь на результаты исследований отечественных и зарубежных ученых в области защиты информации и информационной безопасности систем, таких как Зегжда П.Д., Зегжда Д.П., Заборовский В.С., Будзко В.И., Курбатов, В.А., Ли Р.Б., Воля Себастьян предложена обобщенная структура модели многоагентной системы облачных вычислений, предназначенная для информационной поддержки управленческих решений и защиты системы облачных вычислений, обеспечивающая выполнение ряда функциональных возможностей:

- получения достоверной и объективной информации о поведении пользователя и акторов в системе облачных вычислений для дальнейшего построения стратегии защиты системы;

- сохранение шаблонов пользовательских запросов и действий в системе, необходимых для получения часто используемых данных и выявления нерегламентированных действий и попыток воздействия на систему облачных вычислений;

- использование агента безопасности для мониторинга действий облачного пользователя и акторов в системе;

- расширение функциональных возможностей системы облачных вычислений путем увеличения способов анализа и интерпретации данных о поведении пользователей полученных из системы, то есть возможность дополнения определенных параметров системы и их взаимосвязей, а также увеличения их количества в процессе использования ресурсов системы облачных вычислений;

- проведение автоматизированных исследований статистических данных о поведении пользователей и акторов в системе,

а также минимизации числа ошибок системы, обусловленных человеческим фактором.

В данной статье предлагается модель системы облачных вычислений с выделенным агентом безопасности, он необходим для мониторинга действий облачного пользователя и акторов системы, так же для обеспечения безопасности системы в целом. Агент безопасности строиться с использованием автоматной модели.

Основная часть

В соответствии с концепцией (NIST) предложены базовые модели обслуживания (SaaS, PaaS, IaaS).

В концепции предлагается три базовых модели обслуживания:

1 SaaS – Software as a Service, программное обеспечение как услуга, подписчикам предоставляется готовое прикладное программное обеспечение, полностью обслуживаемое провайдером услуги.

2 PaaS – Platform as a Service, подписчикам предоставляется доступ к использованию информационно-технологических платформ: операционных систем, систем управления базами данных, средствам разработки и тестирования и другому подобному ПО, размещаемому у провайдера.

3 IaaS – Infrastructure as a Service, подписчику предоставляется возможность использования облачной инфраструктуры для самостоятельного управления ресурсами обработки, хранения, сетями и другими фундаментальными вычислительными ресурсами [3].

При построении модели системы облачных вычислений необходимо учесть ряд особенностей системы:

- клиенты облачных систем обслуживают себя сами, то есть предоставляется возможность самостоятельного получения доступа к информационным сервисам;

- универсальность доступа клиента к облачной системе с использованием информационно-телекоммуникационных сетей;

- возможность клиента получить доступ к информационным сервисам с использованием тонких или толстых клиентов по информационно-телекоммуникационному каналу связи;

- высокая консолидация вычислительных ресурсов – объединение вычислительных ресурсов в одной или нескольких точках для обслуживания клиентов с возможностью динамического распределения физических и виртуальных ресурсов в соответствии с запросами клиента;

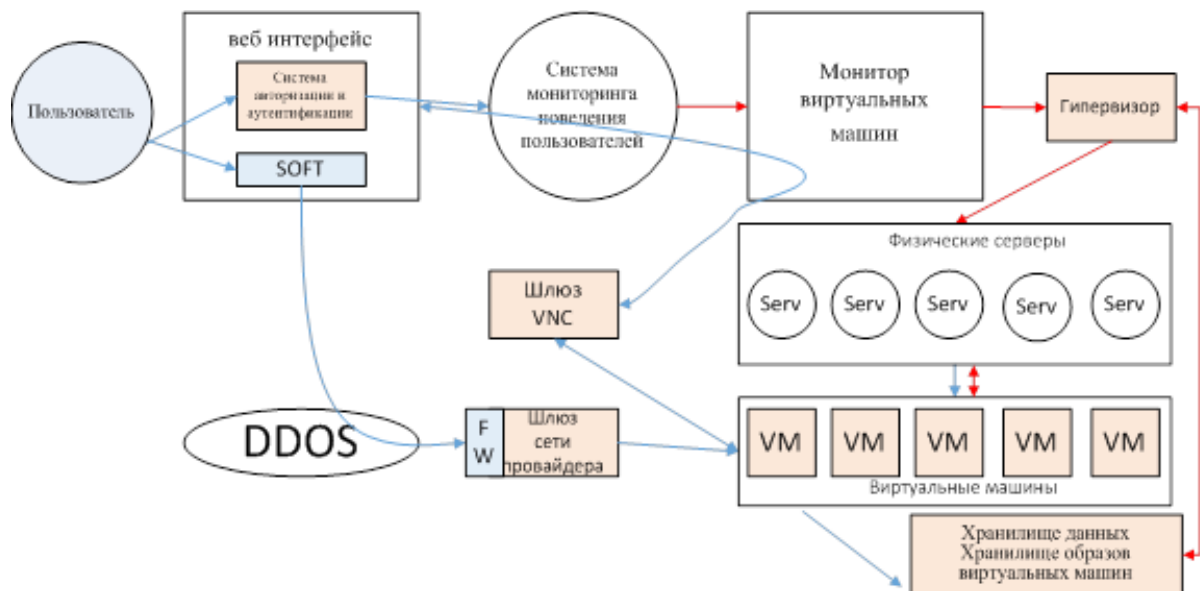


Рис. 1. Обобщенная модель системы облачных вычислений

– динамическая масштабируемость – возможность оперативного автоматического изменения производительности в зависимости от запроса клиента [10].

Обобщенная модель системы облачных вычислений представлена на рис.1.

На обобщённой модели можно видеть семь субъектов: система виртуализации (гипервизор), система управления вычислительными ресурсами (монитор виртуальных машин), хранилище данных, хранилище образов виртуальных машин, система авторизации и аутентификации, веб интерфейс, система мониторинга поведения пользователя.

Система виртуализации (гипервизоры) – представляет собой платформу полной виртуализации с возможностью использования аппаратных возможностей процессора, чаще всего гипервизоры.

Система управления вычислительными ресурсами (монитор виртуальных машин) – это система отвечает за предоставление пользователям виртуальных машин по средством управления виртуальным монитором, а так же выделение различного рода ресурсов необходимых пользователю, в частности виртуальные сети, виртуальные хранилища данных.

Хранилище данных – предоставляется пользователю для хранения разного рода данных и постоянной репликацией этих данных с использованием удаленного веб сервиса.

Хранилище образов виртуальных машин – система хранения образов виртуальных машин в различных форматах, отслеживания доступным образом виртуальных машин для пользователя.

Система авторизации и аутентификации – система используется всеми субъектами для авторизации и аутентификации акторов системы.

Веб интерфейс – объект, предоставляющий пользовательский интерфейс.

Система мониторинга поведения пользователя – система, построенная на ограничении и контроле запросов пользователей, а также рекомендаций по выполнению запросов пользователей в системе облачных вычислений, с возможностью предотвращения несанкционированного доступа к элементам системы облачных вычислений в частности виртуальной машине, гипервизору, хранилищу данных и др.

Модель взаимодействия субъектов отображена на рис.2.

Из рисунка видно, что взаимосвязь в модели организована каждый с каждым.

Нами предложена модернизированная архитектура облачных вычислений, она предполагает использование 6 главных действующих акторов (табл.1).

В данном случае модель акторов нами используется в качестве основы для моделирования системы защиты облачных вычислений. Идея композиции систем акторов является важным аспектом модульности.

На основе обобщённой модели системы облачных вычислений с использованием многоагентного подхода построим модель взаимодействия действующих акторов в системе облачных вычислений.

Модель взаимодействия акторов представлена на рис.3.

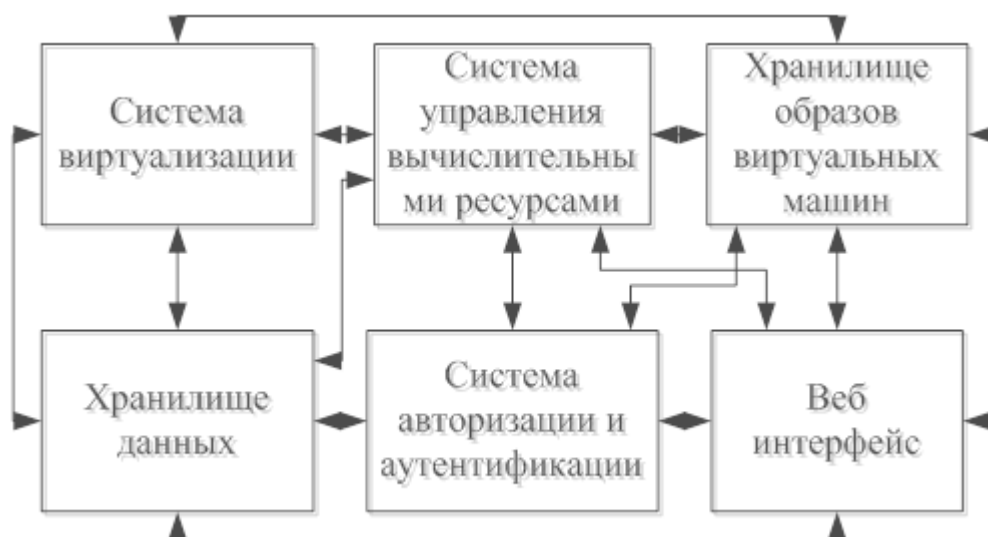


Рис. 2. Модель взаимодействия субъектов

Таблица 1.
Акторы системы облачных вычислений

Актор	Определение
Пользователь	Лицо или организация использующие ресурсы системы облачных вычислений
Ресурс	Сущность, отвечающая за доступность облачного ресурса либо услуги для пользователя
Аудитор	Лицо либо организация, выполняющая независимую оценку предоставляемых ресурсов, услуг, обслуживания информационной системы, производительность и безопасность реализация облака.
Брокер	Сущность, управляющая использованием и предоставлением ресурсов и услуг пользователю. Также устанавливающая взаимосвязь между ресурсом и пользователем
Оператор связи	Посредник, предоставляющий услуги подключения между ресурсом и пользователем (канал связи)
Агент безопасности	Сущность, формирующая запрос от пользователя к ресурсу, определяющая процессы необходимые для предоставления услуги или ресурса пользователю, отвечающий за безопасное взаимодействие акторов всей системы в целом

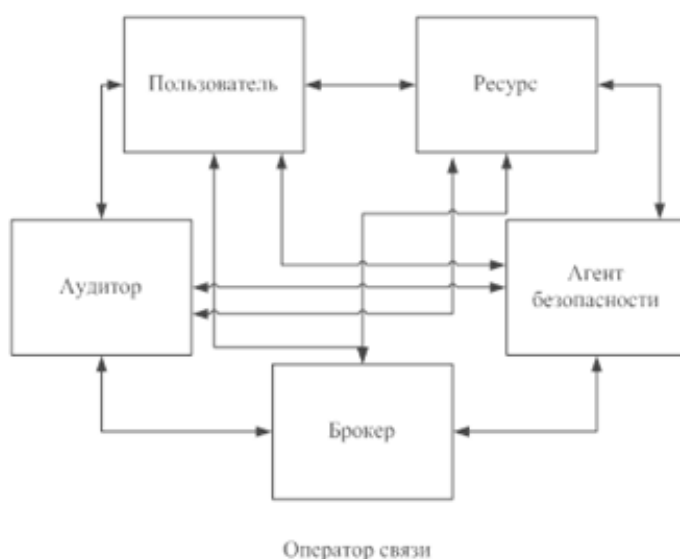


Рис. 3. Модель взаимодействия акторов

Опишем возможные варианты сценариев взаимодействия акторов, введенный нами дополнительный агент безопасности отвечает за целостность, конфиденциальность и доступность предоставления ресурсов и сервисов, а также проводит мониторинг запросов пользователей системы и взаимодействия акторов системы.

Сценарий 1: Облачный пользователь запрашивает услугу или сервис у облачного брокера вместо прямого запроса с облачным ресурсом. Запрос пользователя формируется в агенте безопасности и направляется к облачному брокеру, тот в свою очередь создает новый сервис, комбинируя набор сервисов, услуг и ресурсов. В данной

модели облачный ресурс не видим пользователю напрямую, обращение происходит через облачного брокера (рис. 4).

Сценарий 2: Облачный оператор связи предоставляет услуги подключения облачных услуг от облачного ресурса к пользователю (рис. 5).

Сценарий 3: Облачный аудитор проводит независимую оценку обслуживания и безопасности реализации облачных услуг и сервисов (рис.6).

Опишем функции и роли акторов в системе облачных вычислений.

Облачные пользователи разделяются по трем группам в зависимости от требуемых им приложений (табл.2).

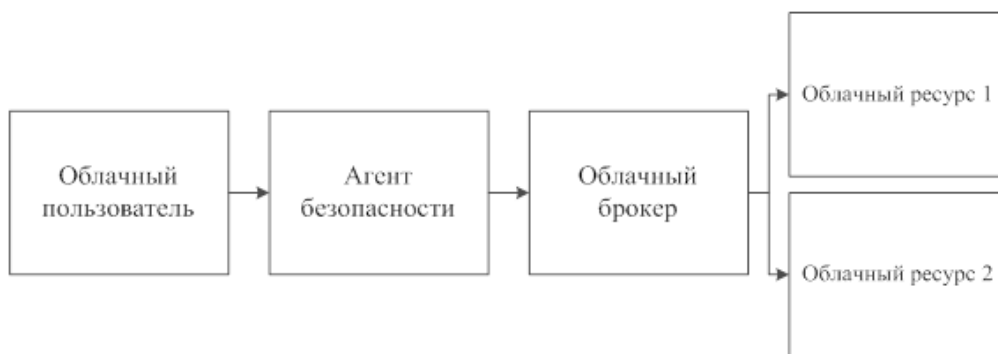


Рис. 4. Участие облачного брокера во взаимодействии пользователя и ресурса



Рис. 5. Участие облачного оператора связи в предоставлении ресурсов и услуг



Рис. 6. Участие облачного аудитора в оценке предоставляемых сервисов

Таблица 2.

Примеры и активность пользователей системы облачных вычислений

Тип пользователя	Активность пользователя	Примеры пользователей
SaaS	Лицо или организация используют приложения либо сервисы для автоматизации бизнес - процессов	Бизнес пользователи
PaaS	Использует приложения для разработки, тестирования и управления собственными проектами развернутыми в облаке	Администраторы системы, разработчики проектов и приложений, лица тестирующие приложения
IaaS	Мониторит и создает сервисы и услуги для управления IT инфраструктурой	Администраторы систем, системные разработчики и администраторы, IT менеджеры

Облачный ресурс отвечает за доступность облачной услуги или сервиса для облачных пользователей, решая задачи в различных сервисных моделях (табл. 3).

Облачный ресурс или сервис рассматривается как развертывание сервисов, согласование сервисов, облачный сервис менеджмент, безопасность и приватность (NIST) (рис. 7).

Облачный аудитор – лицо или организация, выполняющая независимую оценку предоставляемых облачных услуг и сервисов, он может давать оценку не только сервисам, но и безопасности предоставления услуг, а также соблюдение приватности.

Облачный брокер – сущность отвечающая за управление и использование предоставляемых облачных услуг пользователю. Основными предоставляемыми услугами являются: расширение облачного сервиса, комбинирование и обеспечение интеграции облачных сервисов, подборка сервисов для пользователя.

Облачный оператор связи является посредником, предоставляющим услуги подключения и доступ через сетевые и телекоммуникационные устройства связи, также обеспечивает доставку услуг и сервисов.

Агент безопасности – отмеченный выделением на рисунке 8, сущность, отвечающая за формиро-

Таблица 3.

Активность ресурса

Тип ресурса	Активность ресурса
SaaS	Управляет, устанавливает и поддерживает прикладное программное обеспечение на облачной инфраструктуре
PaaS	Предоставляет доступ к информационно-технологическим платформам и инструментам для разработки и администрирования программного обеспечения
IaaS	Управляет и предоставляет вычислительные ресурсы и физические мощности системы и сетей, а также управляет облачной инфраструктурой



Рис. 7. Блоки облачного ресурса



Рис. 8. Концептуальная структура взаимодействия акторов системы облачных вычислений

вание запроса от пользователя к ресурсу, так же отвечающая за мониторинг и адекватность запросов пользователей в системе облачных вычислений, предоставляет возможные варианты запросов в случае неверно выбранных действий или попытки несанкционированного доступа к ресурсам системы облачных вычислений, так же отвечает за взаимодействие акторов в системе. Данный актор более подробно будет описан ниже.

Концептуальная структура взаимодействия акторов системы облачных вычислений представлена на рис.8.

Опишем реализацию актора с подмножеством ментальных свойств. Ментальные свойства включают в себя: места, агенты, миграция, соединения, полномочия и разрешения (permits). Опишем перечисленные понятия:

Места – подразумевают компьютерную распределенную сеть как множество мест. Место — стационарный процесс на сервере, гипервизоре или в сети, предлагающий услуги входящему актору.

Агенты. Агенты это коммуникационное приложение занимающее определенное место. Иногда агенты могут мигрировать с места на место. Агент-

ские процедуры выполняются параллельно.

Миграция. Агенту предоставляется возможность мигрировать с места на место. Миграция это не заметный для пользователя процесс не влияющий на производительность системы. Отличительной особенностью миграции является удаленный доступ к услуге или ресурсу.

Соединения. Соединения позволяют агентам обмениваться информацией с разных мест.

Полномочия. Данное свойство позволяют агенту или месту распознавать полномочия другого агента/места, причем агент или место не могут ни скрывать, ни фальсифицировать свои полномочия. Свойство предусматривает проверку полномочий при перемещении агента между регионами сети, что позволяет защитить агентов и места от проникновения вирусов.

Разрешения. Данное свойство позволяет управлять назначением полномочий.

Агент безопасности является сущность отвечающей за мониторинг и адекватность запросов пользователей, за корректное отправление запроса к другим акторам системы и взаимодействие акторов.

Чтобы понять работу данного актора необходимо проанализировать поведение пользователя в системе облачных вычислений.

Модель мониторинга поведения пользователя и взаимодействия акторов в облачной системе представляет сигнатурную модель поиска запрещенных действий в системе. Предложенный нами алгоритм анализа поведения пользователя в системе облачных вычислений предназначен для разработки агента безопасности.

Предлагаемый подход повысит защищенность системы за счет повышения достоверности распознавания несанкционированных запросов и действий пользователей, а также взаимодействия акторов в системе облачных вычислений.

Обобщенная модель поведения пользователя и взаимодействия акторов в облачной системе как цифрового автомата A представлена в выражении функцией (1).

$$A = \{S, S_0, X, Y, \delta, \lambda\} \quad (1)$$

где S – текущее технологическое состояние системы облачных вычислений, обусловленное действиями пользователя, S_0 – начальное состояние системы облачных вычислений, X – входной алфавит действий пользователя, Y – выходной алфавит реакций системы облачных вычислений на действия пользователя, $\delta(s,x)$ – функция перехода

системы облачных вычислений, $\lambda(s,x)$ – функция выходов системы облачных вычислений.

Для выполнения определенной операции в системе пользователь выполняет некоторый алгоритм действий (совершение операций, ввод данных, выполнение условий, вывод данных, запрос ресурсов и сервисов),

Представленная математическая модель системы облачных вычислений описывает все входные и выходные значения и состояния системы и поведения пользователя в системе.

Так на рисунке представлена структурная схема взаимодействия системы облачных вычислений и подсистемы мониторинга поведения пользователей и взаимодействия акторов, согласно которой она контролирует все входные и выходные значения пользователя, акторов и системы в целом, ведет отчет по их работе, оказывает воздействие на компьютерную подсистему для осуществления разрешенных переходов согласно таблице выходов и переходов (рис.9). Пользователь выполняет действие над компьютерной подсистемой под влиянием предыдущих действий выполненных над ней. Компьютерная подсистема выполняет действия пользователя только в случае разрешения подсистемы мониторинга. Контроль осуществляется по предварительно составленной таблице выходов и переходов.



Рис. 9. Структурная схема взаимодействия облачного пользователя и системы облачных вычислений

где $X_{упр}$ – управляющее воздействие на пользователя или актор, $X_в$ – воздействие облачной системы на пользователя или актор, $Y_д$ – действие пользователя или актора на системы облачных вычислений, $Y_р$ – реакция подсистемы поведения пользователя или актора на действия пользователя, $Y_рс$ – реакция системы облачных вычислений на действие пользователя или актора (результат работы системы облачных вычислений).

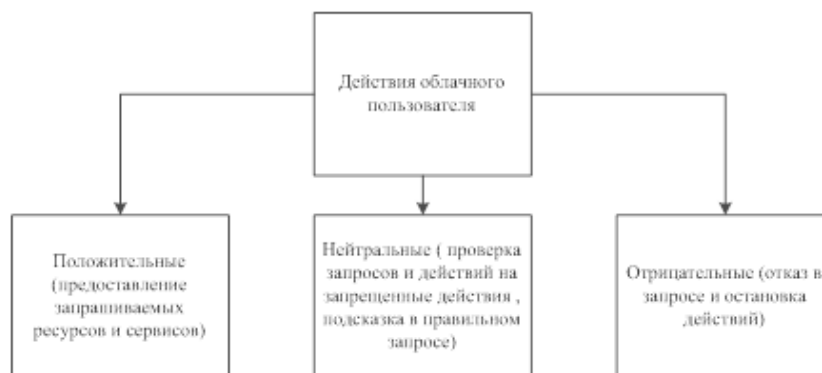


Рис. 10. Классификация действий пользователя в сигнатурном подходе

Классификация действий пользователя в сигнатурном подходе представлена на рис.10.

В зависимости от типа поведения пользователя и его действий, система облачных вычислений адекватно реагирует либо подсказывает, что необходимо сделать либо блокирует действия пользователя. Если пользователь делает запрос на ресурсы без каких-либо отклонений – система облачных вычислений не вмешивается (значение 0); в случае когда пользователь намерено либо не намеренно совершает запрещенное действие – система облачных вычислений заблокирует действия пользователя и уведомит администратора об инциденте (значение 1); в случае когда пользователь не совершает запрещенных запросов, но и не может выполнить соответствующее действие – система облачных вычислений подсказывает пользователю последующие запросы которые можно выполнить в системе облачных вычислений для получения пользователем необходимого результата (значение 0,5).

Для того, чтобы определить возможные каналы утечки информации в системе облачных вычислений необходимо определить потоки информации в системе облачных вычислений.

Воспользуемся специальным инструментом структурного анализа потока данных, который поможет выстраивать иерархию данных и выявлять их взаимосвязи – DFD (диаграмма потоков данных).

В результате анализа системы облачных вычислений, выявлены следующие информационные потоки:

- Log-действий облачного аудитора;
- Log-действий облачного брокера;
- Log-действий пользователей системы облачных вычислений;
- данные о запросах и действия пользователей облачных вычислений
- сведения о состоянии объектов управления.

Графический язык описания, моделирования систем составляет основу подхода и методологии IDEF0.

На рисунке представлена модель потоков информации в системе анализа поведения пользователя (рис.11).

Функциональная модель анализа поведения пользователя в системе облачных вычислений представлена в нотации методологии IDEF0 и представлена на рис.12.

Для разрабатываемого средства основной функцией является «Анализ аномального поведения пользователя на основе автоматной модели». Это будет главным блоком диаграммы.

Далее необходимо определить входные и выходные потоки. Входными потоками являются:

- Log-действий облачного аудитора;
- Log-действий облачного брокера;
- Log-действий пользователей системы облачных вычислений;
- алгоритм анализа запросов и действий облачного актора;
- шаблоны нормальных и аномальных запросов и действий.

Выходными потоками являются:

- отчеты запросов и действий акторов;
- формирование шаблонов запросов и действий акторов.

Данный подход анализа аномального поведения пользователей и акторов в системе облачных вычислений на основе автоматной модели должен являться элементом данной системы облачных вычислений, функционирующих на базе виртуальной платформы и будет способствовать повышению уровня защищенности системы облачных вычислений.

Основной задачей системы анализа аномальных запросов и действий акторов в системе облачных вычислений на основе автоматной модели является обеспечение обнаружения и блокирование основных угроз безопасности информации в системе облачных вычислений.

Данный подход должен быть универсален и

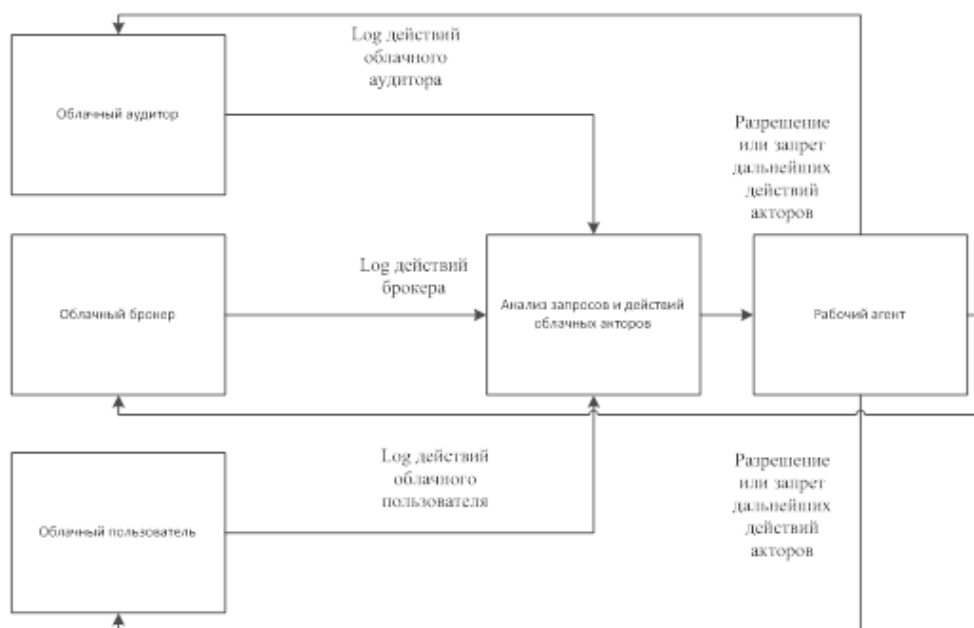


Рис. 11. Модель потоков информации

предназначен для защиты системы облачных вычислений как от внешних, так и от внутренних нарушителей; а так же для принятия решения о разрешении или запрещении запросов и действий акторов системы, для этого необходим анализ предыдущих действий и запросов акторов. В процессе функционирования системы пополняется база сигнатур с разрешающими и запрещающими запросами и действиями, так же происходит анализ и фиксация запросов и действий в системе облачных вычислений.

Выводы

Таким образом, в статье:

- предложена модернизированная модель облачных вычислений с использованием много-агентного подхода, выделен актер безопасности как один из основных, отвечающих за защиту системы облачных вычислений от внешних и вну-

тренних нарушителей;

- предложена модель и сценарии взаимодействия акторов с учетом выделенного агента безопасности;

- построена концептуальная структура взаимодействия акторов системы облачных вычислений;

- определены ментальные свойства для акторов системы облачных вычислений;

- построена модель мониторинга поведения облачного пользователя и взаимодействия акторов в данной системе, представляющая собой сигнатурный поиск запрещенных действий в системе;

- предложена обобщенная модель поведения пользователя и взаимодействия акторов в облачной системе на основе цифрового автомата;

- выделены потоки информации в системе облачных вычислений и построена модель потоков информации, контекстная диаграмма IDEF0.

Рецензент: Соловьев Николай Алексеевич, доктор технических наук, профессор Оренбургского государственного университета, г. Оренбург, Россия, E-mail: povt@unpk.osu.ru

Литература:

1. Пескова О.Ю., Степовая К.Е. Обобщенные требования по обеспечению безопасности облачных сервисов // Информационное противодействие угрозам терроризма. 2014. №23. С.120-130.
2. Пескова О.Ю., Степовая К.Е. Безопасность контроля доступа к облачным системам // Информационное противодействие угрозам терроризма. 2014. №23. С.110-120.
3. Селифанов В.В., Курносоев К.В. Требования к системе защиты информации для виртуальной инфраструктуры // Информационное противодействие угрозам терроризма. 2014. №23. С.188-194.
4. Машкина И.В., Тулиганова Л.Р., Павлова И.А. Разработка структурной вербальной модели угроз в системе облачных вычислений // Информационное противодействие угрозам терроризма. 2014. №23. С.196-200.
5. Пескова О.Ю. Подходы к обеспечению безопасности облачных сервисов // Информационное противодействие угрозам терроризма. 2013. №20. С.186-194.
6. Богданов В.В., Новоселова Ю.С. Актуальность обеспечения информационной безопасности в системах облачных вычислений, анализ источников угроз // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. № 1-2. С. 78-82.

7. Демурчев Н.Г., Ищенко С.О. Проблемы обеспечения информационной безопасности при переходе на облачные вычисления // Информационное противодействие угрозам терроризма. 2009. № 13. С. 147-151.
8. Зорин Е.Л., Чичварин Н.В. Информационная безопасность САПР/PLM, применяющих облачные технологии // Вопросы кибербезопасности. 2014. № 4(7). С. 23-29
9. Зубарев И.В., Радин П.К. Основные угрозы безопасности информации в виртуальных средах и облачных платформах // Вопросы кибербезопасности. 2014. № 2(3). С. 40-45
10. Влацкая И.В., Полежаев П.Н. Облачные вычисления в информационной безопасности // Информационное противодействие угрозам терроризма. 2015. №25. С.109-116.

THE BUILDING OF MODEL OF THE PROTECTION SYSTEM IN CLOUD TECHNOLOGIES BASED ON MULTI-AGENT APPROACH USING THE AUTOMATIC MODEL

Borovki A. S.⁴, Ryapolova E. I.⁵

This article propose to use multi-agent approach in the building of system's model of protection cloud computing and based on the reference architecture of cloud computing NIST developed by the National Institute of standards and technology of USA, with separation of the significant agent of safety, which have a special role in the protection of cloud computing. It is responsible for the formation of queries by users of the system, monitoring of the user's queries and interaction of actors in the system of cloud computing. Monitoring system of user's behavior and actors in the system of cloud computing is offered to construct using the automata model. Agent's separation of safety is necessary on the one hand in connection with increase of number of the commercial enterprises which transfer to the platform of cloud computing, on the other hand the need to protect resources and data.

In article provide a row of scenarios of actor's interaction taking into account of the selected agent of safety. The agent of safety in this case executes controlling and binding roles between all actors of model, using monitoring and recognition of unauthorized actions both from cloudy users, and from actors of the system.

The model of control for the behavior's of the cloudy users and interaction of actors in cloudy system represents signature model for the searching of the forbidden actions in the system of cloud computing.

For defining security risks of the system of cloud computing the threading model of data was developed.

Keywords: *model of system for the protection of cloud technology multi-agent approach, protection of cloud computing, automata model, cloud computing, cloud technology.*

References:

1. Peskova O.Yu., Stepovaya K.E. Obobshchennye trebovaniya po obespecheniyu bezopasnosti oblachnykh servisov // Informatsionnoye protivodeystviye ugrozam terrorizma. 2014. №23. pp.120-130.
2. Peskova O.Yu. Stepovaya K.E. Bezopasnost kontrolya dostupa k oblachnym sistemam // Informatsionnoye protivodeystviye ugrozam terrorizma. 2014. №23. pp.110-120.
3. Selifanov V.V., Kurnosov K.V. Trebovaniya k sisteme zashchity informatsii dlya virtualnoy infrastruktury // Informatsionnoye protivodeystviye ugrozam terrorizma. 2014. №23. pp.188-194.
4. Mashkin I.V., Tuliganova L.R., Pavlova I.A. Razrabotka strukturnoy verbalnoy modeli ugroz v sisteme oblachnykh vychisleniy // Informatsionnoye protivodeystviye ugrozam terrorizma. 2014. №23. pp.196-200.
5. Peskova O.Yu. Podchody k obespecheniyu bezopasnosti oblachnykh servisov // Informatsionnoye protivodeystviye ugrozam terrorizma. 2013. №20. pp.186-194.
6. Bogdanov V.V., Novoselova Yu.S. Aktualnost obespecheniya informatsionnoy bezopasnosti v sistemakh oblachnykh vychisleniy, analiz istochnikov ugroz // Doklady Tomskogo gosudarstvennogo universiteta system upravleniya i radioelektroniki. 2012. № 1-2. pp. 78-82.
7. Demurchev N.G., Ishchenko S.O. Problemy obespecheniya informatsionnoy bezopasnosti pri perekhode na oblachnye vychisleniya // Informatsionnoye protivodeystviye ugrozam terrorizma. 2009. № 13. pp. 147-151.
8. Zorin E.L., Chichvarin N.V. Informatsionnaya bezopasnost SAPR/PLM, primenyaushchikh oblachnye tekhnologii // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2014. № 4(7). pp 23-29
9. Zubarev I.V., Radin P.K. Osnovy ugroz bezopasnosti informatsii v virtualnykh sredakh i oblachnykh platformakh // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2014. № 2(3). pp 40-45
10. Vlatzkaya I.V., P.N. Polezhaev Oblachnye vychisleniya v informatsionnoy bezopasnosti // Informatsionnoye protivodeystviye ugrozam terrorizma. 2015. №25. pp.109-116.

4 Alexander Borovki, Doctor of Technical Sciences, the head of the department « Management and Informatics in technical systems» Federal State-Funded Educational Institution of Higher Education «Orenburg State University», Orenburg, borovski@mail.ru

5 Elena Ryapolova, Candidate of Pedagogic Sciences, Docent at the Department of «Computing Technique and Protection of Informa-tion» Federal State-Funded Educational Institution of Higher Education «Orenburg State University», Orenburg, ananeva_ei@mail.ru