DOI: 10.7256/2073–8560.2013.5.9587

ТЕХНОЛОГИИ И МЕТОДОЛОГИЯ В СИСТЕМАХ БЕЗОПАСНОСТИ

А.В. Царегородцев

ПОСТРОЕНИЕ ДЕРЕВЬЕВ ЦЕЛЕЙ ДЛЯ ИДЕНТИФИКАЦИИ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ СРЕДЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Аннотация: *необходимость совершенствования и повышения эффективности кардинальных принципов управления информационной безопасностью среды облачных вычислений приводит к многоаспектной области обеспечения свойств «системности». Применение технологии и методов формализованного структурного синтеза систем управления информационной безопасностью (СУИБ) в облачной среде, соединяющих различную структуру иерархий требований, позволило бы с большей эффективностью воспользоваться уже разработанными в каждом из локальных обеспечений технологиями и средствами автоматизации свойств и проявлений системности. Отличную возможность предоставляет эмпирически присущее моделям типа дерева целей свойство системности их структуры.Особое внимание в данной статье уделено вопросам построения деревьев целей для идентификации требований безопасности среды облачных вычислений и формирования базиса формализованного синтеза платформ безопасности информационно-телекоммуникационных систем, функционирующих на основе технологии облачных вычислений, в соответствии с определяемыми критериями системности и с учётом фактора развития системы.Учитывая, что в большинстве предлагаемых облачных сервисов отсутствует прозрачность в области:- соглашения об уровне обслуживания,— реальных возможностей поставщиков,— управления и обеспечения безопасности, созданы предпосылки к разработке нового метода построения гибридной среды облачных вычислений по требованиям информационной безопасности.*

Ключевые слова: *информационная безопасность, облачные вычисления, облачные сервисы, угрозы информационной безопасности, анализ информационных рисков, методы управления, требования информационной безопасности, бизнес активы, дерево целей, гибридная среда.*

Review: *The need for the improvement and higher efficiency of the cardinal principles of information security management in the sphere of cloud computing requires a multi-aspect sphere of guarantees for the systemic quality. Application of the formalized structural synthesis methods and technologies for the systems of information security management in the cloud computing, providing for various levels of requirements hierarchy, could allow for the more efficient use of local technologies and automation qualities, as well as systemic manifestations. The empiric quality of tree models systemic*

DOI: 10.7256/2073–8560.2013.5.9587

structure provides a good opportunity. Special attention is paid to formation of the trees of objectives for the identification of security requirements in the cloud computing and formation of the basis for the formalized synthesis of security platforms in information and telecommunications systems, functioning based upon the cloud computing technologies in accordance with the established systemic criteria and the system development factor. Considering the lack of transparency in such spheres as service level agreements, and realistic supplier capabilities, existing in most cloud computing services, the prerequisites are formed for the formation of a novel method for the formation of the hybrid sphere of information security requirements for cloud computing.
Keywords: *information security, cloud computing, cloud services, information security threats, analysis of information risks, management methods, information security requirements, business assets, tree of objectives, hybrid environment.*

Введение

Облачные вычисления являются одной из самых привлекательных современных информационных технологий, предоставляющих многочисленные преимущества, среди которых в первую очередь можно выделить хорошую масштабируемость и доступность по запросу. Несомненно, миграция на облачную архитектуру позволит организациям снизить общие затраты на внедрение и поддержку инфраструктуры и сократит время разработки новых бизнес приложений. При этом, наиболее острым и актуальным вопросом при миграции данных в облако встанет вопрос обеспечения информационной безопасности.

С использованием общедоступных облачных сервисов большая часть сети, систем, приложений и данных организации будет перенесена на контроль сторонней организации — облачного провайдера. Различные модели предоставления облачных сервисов выстраивают виртуальное пространство для клиента, в котором необходимо чётко разделить обязанности между клиентом и провайдером. Эта модель общей ответственности создает новое направление для формирования требований безопасности всей облачной среды.

Первый вопрос, на который необходимо дать ответ, это соответствует ли уровень прозрачности облачных сервисов уровню управления (распределению ответственности), а так же соответствует ли требованиям безопасности процессы для предоставления гарантий бизнесу, что информация на облаках соответствующе защищена.

Для ответа на данный вопрос, необходимо определить какие требования безопасности должен учитывать провайдер со своей стороны, и как должны быть применены традиционные элементы и процессы управления безопасностью организации в новой облачной среде. Оба ответа должны быть основаны на постоянной оценке критичности и значимости данных и сервисов, а так же на изменении уровня обслуживания с течением времени.

Клиент должен понимать границы доверия для обработки своих данных на всех уровнях облачной архитектуры: сеть, хост, приложение, база данных, хранилище данных и веб-сервисы, включая услуги проверки подлинности. Рассмотрим более детально функции безопасности и построим для них соответствующие деревья целей.

1. Управление доступностью

Облачные технологии не защищены от риска отключений и отказа в обслуживании, а тяжесть и масштаб воздействия на клиентов

DOI: 10.7256/2073–8560.2013.5.9587

может меняться в зависимости от конкретной ситуации. Аналогично любым внутренним ИТ-приложениям, влияние недоступности сервисов на бизнес зависит от критичности рассматриваемых облачных приложений и их связи с бизнес процессами организации. В случае критически важных приложений, где работа полагается на непрерывную доступность услуг, даже несколько минут простоя сервиса могут иметь серьезные отрицательные последствия для репутации организации, получения доходов, ожиданий конечных пользователей и установленного уровня обслуживания.

Принимая во внимание базу данных инцидентов облачных вычислений (CCID http://cloutage.org/), в которой отражается информация о сбоях облачных сервисов, наибольшее время простоя провайдера составляло от нескольких минут до нескольких часов. Во время нарушения работы облачных сервисов пострадавшие клиенты не имеют доступа к облачным услугам и, в некоторых случаях может случиться понижение эффективности работы пользователей с последующим снижением совокупной производительности организации.

На основе проведенного анализа можно сформулировать основные факторы, влияющие на гибкость и доступность облачных вычислений:

1. Архитектура и избыточность SaaS и PaaS приложений.
2. Архитектура центра данных облачных технологий, сетей, систем, включая географическое положение и отказоустойчивость при возникновении ошибок.
3. Надежность и избыточность Интернет соединения, используемого клиентом и провайдером.
4. Способность клиента быстро реагировать и опираться на собственные приложения и другие процессы, включая ручное управление бизнес-процессами.
5. Наглядность вины клиентов. В некоторых простоях, если событие касается небольшого числа пользователей достаточно затруднительно получить полную картину бедствия.
6. Надежность аппаратного и программного обеспечения компонентов, предоставляющих облачные вычисления.
7. Эффективность инфраструктуры безопасности и сети при распределенных атаках типа «отказ в обслуживании».
8. Эффективность контроля безопасностью и процессами, которые уменьшают вероятность человеческой ошибки и защищают инфраструктуру от злонамеренных внешних и внутренних угроз, например, злоупотребление привилегиями пользователей.

Управление доступностью SaaS. Провайдеры сервиса SaaS берут на себя полную ответственность за обеспечение непрерывности бизнеса, приложений клиента и инфраструктуры управления безопасностью процессами организации. Это означает полную передачу всех задач организации на сторону провайдера. Некоторым организациям, которые применяют лучше практики и стандарты, например ITIL, придется столкнуться с новыми проблемами управления в сервисах SaaS, поскольку они пытаются передать все внутренние службы на провайдера. В некоторых случаях вендоры SaaS могут и не включить в контракт соглашение об уровне сервиса и обозначать условия обслуживания в случае возникновения инцидента.

Мониторинг состояния SaaS инфраструктуры. Приведём список опций, доступный заказчикам для информирования о работоспособности их услуг.

Службы информационной панели, представленные провайдером. Обычно SaaS провайдеры, такие как Salesforce.com, публи-

DOI: 10.7256/2073–8560.2013.5.9587

куют текущее состояние сервисов, текущих сбоев которые могут повлиять на заказчиков и предстоящее запланированное техническое обслуживание на веб-портале.

База данных инцидентов облачных вычислений (CCID).

Список адресов заказчика, по которому происходит уведомление о происходящих или ранее происходивших сбоях.

Внутренние или сторонние сервисы мониторинга элементов, которые периодически проверяются поставщиками работоспособности SaaS и предупреждают заказчиков, когда сервис становится недоступным (например, элемент мониторинга Nagios).

Ленты RSS, размещенные на сервисе поставщика SaaS.

Управление доступностью PaaS. Для типичного PaaS сервиса, разработчики разворачивают клиентские приложения на PaaS платформе. Обычно платформы PaaS строятся на сети, серверах, операционных системах, инфраструктуре хранения и приложений компонентов (веб-сервисов) управляемых со стороны провайдера. В таких смешанных архитектурах программное обеспечение разворачивается посредством разделения обязанностей между клиентом и CSP. Заказчик ответственен за управление доступностью специально разработанного приложения и сторонних сервисов, и PaaS провайдер за платформу и другие внутренние сервисы. Например, Forct.com несет ответственность за управление платформой AppExchange, а клиент ответственен за управление приложений разработанных и внедренных на данную платформу. PaaS провайдеры могут также предоставлять набор веб-услуг, включая сервисы очередей сообщений, сервисы идентификации и аутентификации, а так же сервисы баз данных чтобы приложение могло использовать любые компоненты этих сервисов, как, например, Google BigTable. Следовательно, доступность PaaS приложений зависит от надежности разработанных клиентских приложений, PaaS платформы и компонентов веб-сервисов сторонних ресурсов.

Мониторинг состояния PaaS инфраструктуры. В общем случае, приложения PaaS это web-приложения, размещенные на платформе провайдера (например, Java или Python приложения, размещенные на Google App Engine). Следовательно, большинство процессов, используемых для мониторинга SaaS приложений так же применимы и к PaaS приложениям.

Управление доступностью IaaS. Доступность для IaaS инфраструктуры должно учитывать, как вычислительную инфраструктуру, так и системы хранения данных (постоянных и однодневных). IaaS провайдеры могут предлагать дополнительные услуги, такие как: управление аккаунтами пользователей, служба рассылки сообщений, услуги идентификации и аутентификации, сервисы баз данных, платежные сервис и сервисы мониторинга. Таким образом, следует учитывать, что управление доступом включает в себя все услуги, в которых нуждается IT организации. Клиенты несут ответственность по всем аспектам управления доступности: предоставление и управление жизненным циклом виртуальных серверов.

Таким образом, управление виртуальной инфраструктурой облачных вычислений зависит от пяти факторов:

1. Доступность сети провайдера, конечных устройств, накопителей и инфраструктуры поддержки приложений. Этот фактор включает в себя следующие компоненты.
   - Архитектура центра обработки данных провайдера, включая его географическое положение и устойчивость к ошибкам.

DOI: 10.7256/2073–8560.2013.5.9587

- Надежность, разнообразие и избыточность Интернет соединения, используемого клиентом и провайдером.
- Надежность и избыточность архитектура программных и аппаратных компонентов, используемых для доставки вычислительных услуг и сервисов хранения.
- Процессы и процедуры управления доступностью, включая непрерывную работу.
- Доступность веб-консоли и сервисов API, позволяющими управлять жизненным циклом работы виртуальных серверов. Когда эти услуги становятся недоступны, заказчики становятся не в состоянии предоставлять, запускать, останавливать и обеспечивать виртуальные серверы.
- Соглашение о сервисном обслуживании. Потому что этот фактор варьируется в зависимости от CSP. SLA следует проверять со всеми исключениями.

2. Доступность виртуальных серверов и устройств хранения для вычислительных услуг (например, Amazon Web Services'S3 и Amazon Elastic Block Store).
3. Доступность виртуальных средств хранения, от которых зависят пользователи и виртуальные серверы, включая синхронные и асинхронные варианты доступа к хранилищу. Примером синхронного доступа к хранилищу является транзакции базы данных, видео потоки и аутентификацию пользователей. Несоответствие или нарушения в таком режиме серьезно повлияют на общую доступность серверов и приложений.
4. Доступность сетевого подключения к Интернет или подключения виртуальной сети к сервисам IaaS. Иногда, это может затрагивать частную виртуальную сеть

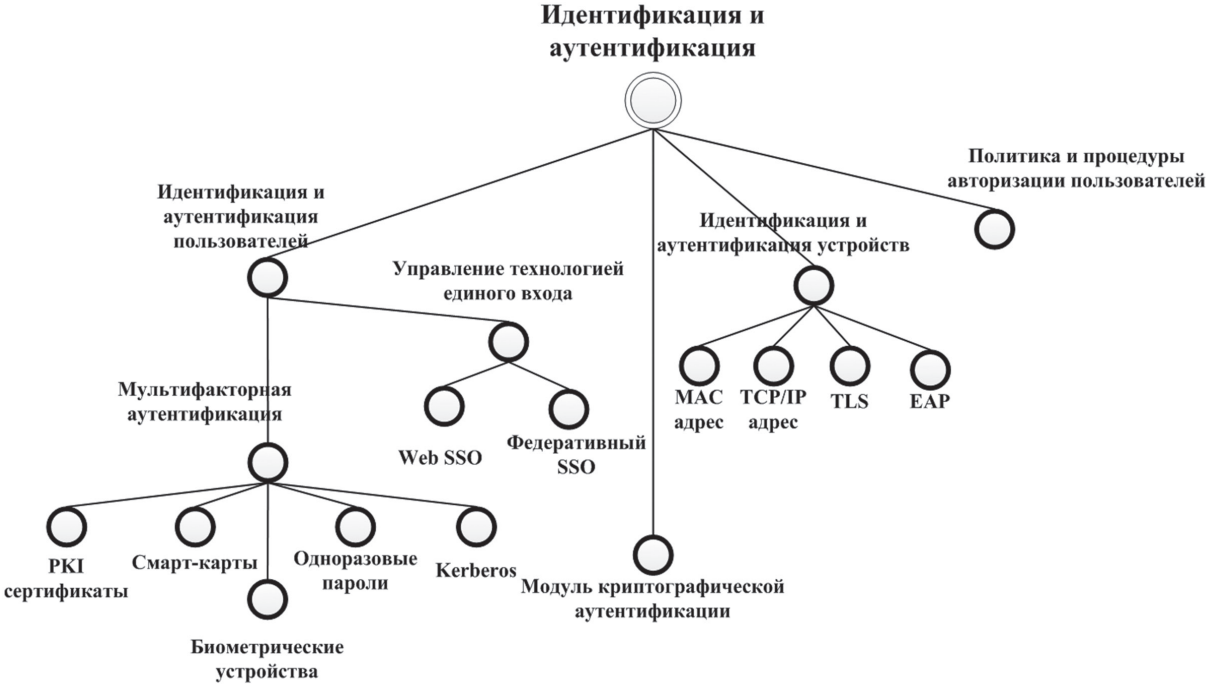

Рис. 1. Дерево целей управления идентификации и аутентификации среды облачных вычислений

DOI: 10.7256/2073–8560.2013.5.9587

(VPN), соединенную между внутренним центром обработки данных и общедоступным IaaS облаком (в случае рассмотрения гибридного облака).

5. Доступность сетевых услуг, включая DNS, услуг маршрутизации и аутентификации сервисов, требующих соединения с сервисами IaaS. Для примера на рисунке 1 представлено дерево целей управления идентификации и аутентификации среды облачных вычислений.

Мониторинг состояния IaaS инфраструктуры. Опции, доступные для клиентов IaaS для управления работоспособностью их сервисов, совпадают со средствами мониторинга PaaS и SaaS инфраструктур и могут быть расширены за счёт следующих сервисов.

Внутренних или сторонних услуг мониторинга, которые периодически проверяют работоспособность виртуальных серверов IaaS. Например, Amazon Web Services (AWS) предлагает облачную услугу мониторинга, называемую Cloud Watch. Этот веб сервис предоставляет мониторинг для облачных AWS ресурсов, включая Amazon's Elastic Compute Cloud (EC2). Это так же предоставляет клиентам прозрачность использования ресурсов, выполнения операций, видимость общих закономерностей запросов, включая метрики, такие как утилизацию CPU, чтение и запись дисков, сетевой трафик.

Веб консоль или API, которые публикуют текущий статус работоспособности виртуальных серверов и сетей.

2. Контроль доступа

Управление доступом является одной из самых сложных функций безопасности, которая включает требования для предостав-

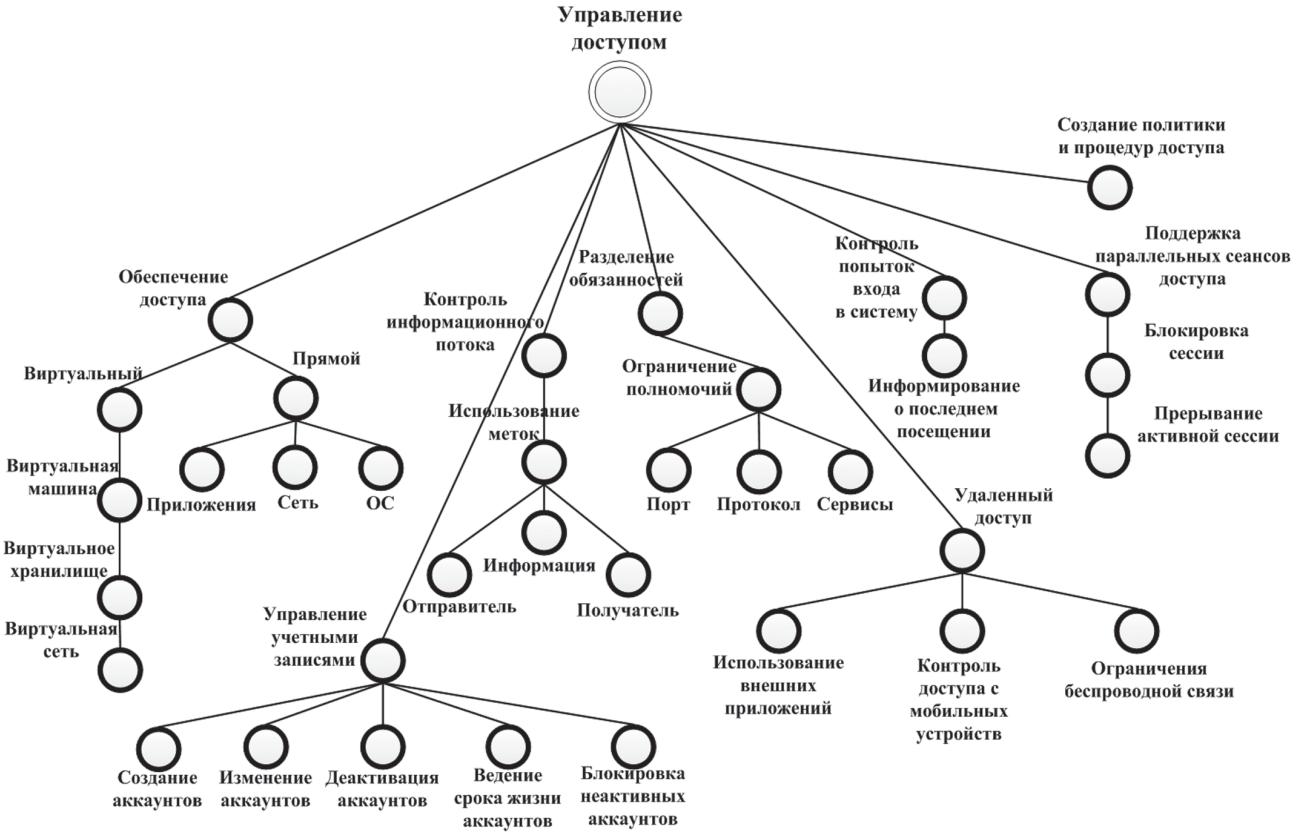

Рис. 2. Дерево целей управления доступом среды облачных вычислений

DOI: 10.7256/2073–8560.2013.5.9587

ления доступа для пользователей и системных администраторов (привилегированных пользователей), которые работают с сетью, системой или приложениями. Для идентификации требований по управлению доступом рекомендуется рассматривать следующие аспекты (рисунок 2).

1. Определение ответственных пользователей и назначение им соответствующих прав.
2. Определение процедуры доступа к облачным ресурсам. Выбор метода аутентификации для обеспечения защищенности предоставляемого ресурса.
3. Обоснование предоставления доступа к ресурсу и рассмотрение особенностей работы с ним.
4. Проведение аудита и ведение отчетности для контроля назначения прав.

Контроль доступа к ресурсам среды облачных вычислений. При рассмотрении модели использования облачных сервисов, в рамках которой пользователи имеют доступ с любого конечного устройства, имеющего доступ в Интернет, роль сетевого контроля доступа значительно уменьшается. Причина в том, что стандартный контроль доступа сети фокусируется на защите ресурсов от несанкционированного доступа, основанного на характеристиках конечных устройств, которые в большинстве случаев неполноценны, неуникальны для различных пользователей и могут привести к неточной оценке. В среде облачных вычислений, сетевой контроль доступа проявляется в виде политики построения облачных брандмауэров, обеспечивающих конечные устройства контролями доступа на входах и выходах точек распределения облачных сред. Обычно это достигается путем настройки правил, основанных на стандарте параметров TCP/IP.

В отличие от сетевого управления доступом, пользовательскому контролю доступа должно уделяться большее внимание в среде облачных вычислениях, так как это серьезно влияет на идентификацию пользователя для получения доступа. Пользовательское управление доступом, включает в себя строгую авторизацию, технологию единого входа (SSO), управление привилегиями, запись и мониторинг ресурсов облачных вычислений, играющих значительную роль в защите конфиденциальности и целостности вашей информации в облачных вычислениях.

Стандарт ISO/IEC 27002 определяет шесть объектов контроля доступа, которые включают: уровень безопасности обычного и привилегированного пользователя (администратора), сети, приложений и контроля доступа к информации. Приведём актуальные выдержки из ISO 27002 об управлении контроля доступа пользователей для облачных вычислений.

Формальные процедуры предоставления доступа по стандарту ISO 27002 должны охватывать все этапы жизненного цикла доступа пользователя, от первоначальной регистрации новых пользователей до завершения процесса и снятия с регистрации тех пользователей, которым больше не требуется доступ к системной информации и сервисам. Особое внимание следует обратить, когда это требуется, на необходимость контроля распределения привилегированных прав доступа, которые позволяют пользователям переопределить систему управления. Выделяют шесть операторов управления:

1. Контроль доступа к информации;
2. Управление правами доступа пользователей;
3. Поддержание передовой практики доступа;
4. Контроль доступа сетевых услуг;
5. Контроль доступа операционных систем;
6. Контроль доступа приложений и систем.

Процессы управления доступом как таковые являются ничем иным как отдельной политикой в управлении безопасностью ИТ.

DOI: 10.7256/2073–8560.2013.5.9587

Контроль доступа SaaS. SaaS провайдер отвечает за управление всеми аспектами инфраструктуры сети, сервера и приложений. В такой модели, когда приложение поставляется как услуга для конечных пользователей, обычно через web-браузер, сетевой контроль становится неэффективным и заменяется контролем доступа пользователя, например, при авторизации используются одноразовые генерируемые пароли. Таким образом, клиенту следует обратить внимание на контроль доступа пользователей (авторизация, объединение, управление привилегиями, удаление полномочий) для защиты информации, хранящейся в SaaS. Некоторые сервисы SaaS, такие как Saleforce.com, усиливают контроль за счёт сетевого контроля (например, контроль по IP-адресу пользователя или его подсети).

Контроль доступа PaaS. В модели поставки PaaS, провайдер отвечает за управление контролем доступа к инфраструктуре сети, серверов и платформенных приложений, в то время как заказчик отвечает за контроль доступа к приложениям, развернутым на платформе. Контроль доступа приложений проявляется как управление доступом конечного пользователя, что включает резервирование и его аутентификацию.

Контроль доступа IaaS. Клиенты IaaS полностью несут ответственность за управление всеми аспектами контроля доступа к их ресурсам на облаке. Клиент обязан организовать безопасный доступ к виртуальным серверам, виртуальной сети, виртуальному хранилищу и приложениям, размещенным на IaaS платформе.

В модели IaaS управление контролем доступа подразделяется на 2 категории.

1. Контроль доступа к инфраструктуре со стороны провайдера.

Управление контролем доступа к сети, хосту и приложениями, которые принадлежат и контролируются провайдером. Провайдер ответственен за управление контролем доступа к административной сети, которая используется для выполнения функций администратора, включающих в себя контроль доступа к административным процессам, таким как: резервное копирование, управление хостом, обслуживание сети, системный мониторинг. Доступ к функциям администратора должен быть защищен при помощи строгой аутентификации и соответствующим разграничением доступа. Периодические проверки контроля доступа и сертификатов пользователей должны проводиться для согласования привилегий и разграничения обязанностей. Например, политика информационной безопасности Amazon.com основана на принципе ограничения привилегий. Принцип минимальных привилегий позволяет защитить основные информационные активы клиента, требуя чтобы ни одному человеку, программе или системе не предоставлялся привилегированный доступ, превышающий необходимый для решения конкретной задачи.

2. Виртуальный контроль доступа со стороны клиента.

Управление контролем доступа к виртуальному серверу (виртуальной машине или VMs), виртуальному хранилищу, виртуальным сетям и другим приложениям, размещенным на виртуальных серверах.

Стандартной практикой для IaaS провайдеров является предоставление API функций (REST, SOAP или HTTP с XML/JavaScript Object Natation (JSON)) для создания большинства процедур управления, в том числе контроль удаленного доступа. Организациям, использующим услуги IaaS провайдеров, следует самостоятельно осуществлять контроль доступа: запрос, подтверждение и обслуживание каталога привилегированных пользователей, имеющих доступ к ресурсам IaaS.

DOI: 10.7256/2073–8560.2013.5.9587

Примем во внимание ключевые аспекты управления контролем доступа среды облачных вычислений.

- Сетевой контроль доступа.

Со стороны клиента необходимо проверить стандартную конфигурацию сетевого доступа, применяемую у провайдера. Запрещение полного доступа к виртуальным серверам клиента является распространенной практикой провайдера, при этом блокируется входящий интернет-трафик для виртуальных серверов. Эти действия могут заставить более детально разрабатывать новые правила для разрешения доступа к виртуальным серверам.

- Виртуальный контроль доступа к серверу.

Виртуальные сервера, работающие на выбранной ОС (Linux, Solaris, Windows), должны быть защищены механизмами строгой аутентификации. Стандартной практикой для настройки Unix серверов является применение основанных на SSH логинов со строгой аутентификацией. Строгая аутентификация предотвращает некоторые угрозы информационной безопасности (например, имитация IP соединения, вымышленные маршруты, MitM-атака, имитация DNS соединения). Методы аутентификации включают в себя криптографический алгоритмы с открытым ключом (RSA), алгоритм создания открытого и секретного ключей и сетевой протокол аутентификации, позволяющий безопасно передавать данные через незащищённые сети для безопасной идентификации. При использовании RSA ключей рекомендуется, чтобы ключи хранились в безопасной форме и для доступа к ним необходимо было ввести фразу-пароль. Эти меры помогают защитить ключи доступа от неавторизированных пользователей.

- Управление облачной инстанцией.

Управление виртуальными ресурсами в облаке осуществляется клиентом при помощи приложений, используя API функции (REST, SOAP или HTTP с XML/JSON). Клиентский инструментарий, поддерживаемый провайдером и установленный на инстанции управления, взаимодействует с сервисом управления провайдера по API интерфейсу. Принимая во внимание, что инстанция содержит конфиденциальную информацию, включая в себя хост и пользовательские ключи, брандмауэр, управление облачной инстанцией следует рассматривать как центр управления всей облачной инфраструктурой. Следовательно, доступ к управлению инстанцией должен быть защищен с помощью механизмов строгой аутентификации.

- Веб-клиент удаленного доступа.

Провайдер может обеспечить специально разработанные веб-клиенты удаленного доступа, с помощью которых будет осуществляться управление облачной инстанцией. Веб-клиент предлагает альтернативные способы управления облачной инфраструктурой и предоставляет удалённый доступ к конфиденциальной информации, включая доступ к хост ключам и брандмауэру. В связи с этим необходимо в достаточной мере обеспечить защиту доступа к консоли. Например, доступ к консоли должен осуществляться только по HTTPS протоколу.

Принимая во внимание детальный анализ основных функций контроля доступа, можно сделать вывод, что это важнейшая функция управления безопасностью среды облачных вычислений, независимо от модели предоставления сервисов (SaaS, PaaS, IaaS) и типа развертывания (публичный, частный, гибридный). Управление доступом является важным аспектом для защиты информации и может быть основным средством управления безопасностью при отсутствии шифрования и других средств управления данными.

На данный период возможности управления доступом, предлагаемые со стороны

DOI: 10.7256/2073–8560.2013.5.9587

провайдера, не являются достаточными для корпоративных клиентов по ряду причин.

Механизмы контроля доступа, нормы и процессы, применяемые провайдером, не стандартизированы. Для эффективного управления доступом к облачной инфраструктуре клиентам необходимо предпринимать дополнительные процедуры и усилия для понимания параметров контроля и настроек со стороны провайдера.

Отсутствие единой стандартизации для API функций делает затруднительным управление доступом для нескольких облаков. Например, SAML не поддерживается даже ключевыми облачными провайдерами, включая Amazon Web Services (AWS).

Контроль доступа пользователей к ресурсам облака осуществляется на достаточно низком уровне. Провайдер осуществляет контроль на сетевом уровне, но не всегда уделяет внимание управлению доступом пользователей.

Для решения поставленной задачи требуется разработать гибкий инструмент контроля доступа к облачным ресурсам, основанным на принципах наименьших привилегий и разделения обязанностей.

С точки зрения корпоративных клиентов управление доступом — это основной процесс обеспечения безопасности для защиты конфиденциальности, целостности и доступности информации, расположенной на облаке. Надежная программа управления доступом должна включать в себя процедуры резервного копирования, периодического удаления привилегий, гибкой аутентификации, управление полномочиями, учет использования ресурсов, аудит и поддержка оперативного управления.

3. Управление уязвимостями, обновлением и конфигурацией

Возможность использования различных уязвимостей компонентов инфраструктуры, сетевых сервисов и приложений остается главной угрозой для облачных сервисов. Данный аспект представляет серьёзную опасность для публичных PaaS и IaaS моделей, в которых управление уязвимостями,

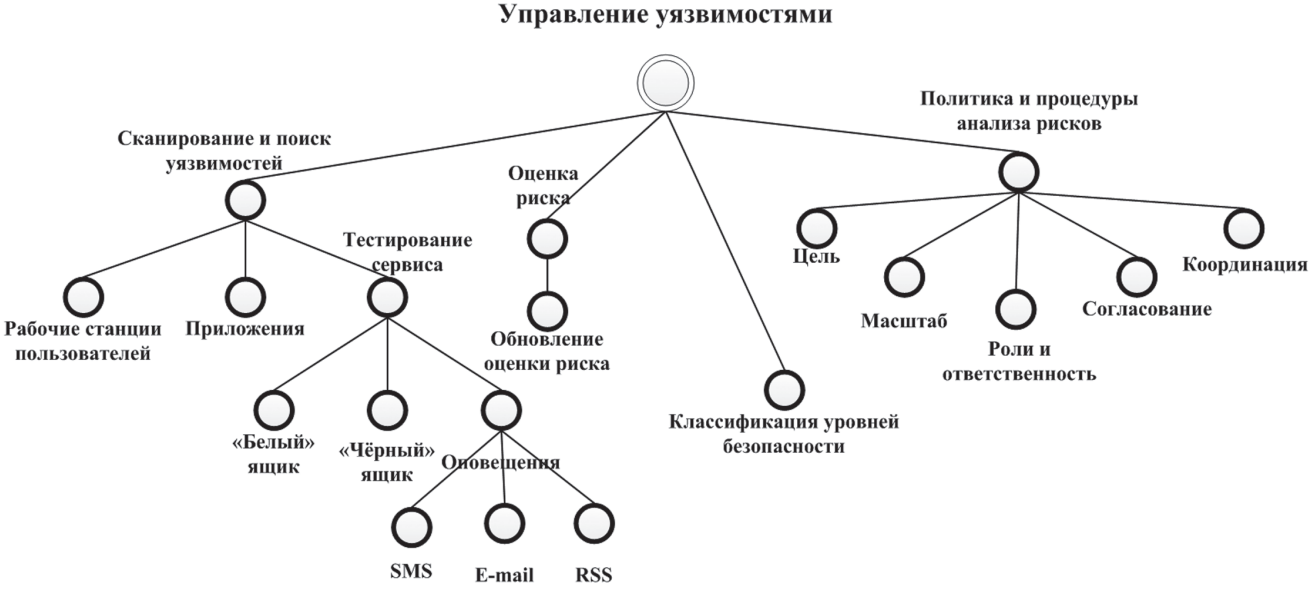

Рис. 3. Дерево целей управления уязвимостями среды облачных вычислений

DOI: 10.7256/2073–8560.2013.5.9587

конфигурацией и обновлением находится в обязанностях клиента. В общедоступной облачной среде общий уровень защищенности распределен между участниками всей многопользовательской виртуальной среды. Следовательно, для клиентов становится критически важным понять границы и разделить обязанности по обеспечению комплексной безопасности.

Подходя к проблеме с одной стороны, ответственность за уязвимости, обновление и конфигурацию (VPC) инфраструктуры (сети, хосты, приложения и память) лежит на стороне провайдера. В то же время клиенты облачной среды должны понимать именно те аспекты VPC, за которые они ответственны. VPC менеджмент должен обеспечивать межабонентскую безопасность и включать в себя процедуры конфигурируемых настроек.

Для формирования требований по управлению уязвимостями, конфигурацией и обновлениями необходимо рассмотреть следующие открытые вопросы.

- Распределение обязанностей и ответственностей за управление уязвимостями в облаке.
- Определение необходимости исправления работы облачного сервиса и обновления.
- Определение ответственности за исправление и конфигурацию безопасности в облачной инфраструктуре.
- Определение альтернативных вариантов для расширения существующих процессов управления безопасностью облачных сервисов.

Управление уязвимостями. Управление уязвимостями — важный элемент сдерживания возможных угроз с целью защиты хоста, сетевых устройств, и приложения от атак (рисунок 3). Зрелые организации ввели процедуры управления уязвимостями, которые включают в себя стандартное сканирование систем, подключенных к сети, анализ рисков возникновения уязвимостей и модификацию процесса для устранения рисков. Организации, использующие стандарт ISO/IEC 27002, используют технические возможности по управлению уязвимостями, которые основывается на принципе достижения снижения риска, возникающего при эксплуатации, используя известные на данный момент времени технические уязвимости. Управление уязвимостями должно быть реализовано эффективной, систематической и повторимой процедурой с возможностью измерить её эффективность. Клиент и провайдер несут ответственность за управление уязвимостью в облачной инфраструктуре в зависимости от модели предоставления сервисов.

Управление обновлениями и исправлениями. Аналогично управлению уязвимостями, управление обновлениями и исправлениями является важным элементом сдерживания возможных угроз на уровне хоста, сетевых устройств и приложений, где действия неавторизованных пользователей направлены на использование известных им уязвимостей. Управление обновлениями и исправлениями снижает риск возникновения внешних и внутренних угроз.

SaaS провайдеры должны оценивать новые уязвимости и исправлять аппаратное и программное обеспечение на всех системах, которые включены в поставку клиентам. Ответственность за управление обновлениями для клиента будет варьироваться от низкой до высокой: в зависимости от модели предоставления сервисов (SaaS, PaaS, IaaS). Клиенты полностью освобождены от процедур обновления в среде SaaS, в то время как они ответственны за управление патчами для целого стека программного обеспечения (ОС, приложения, базы данных), установленного

DOI: 10.7256/2073–8560.2013.5.9587

и управляемого на платформе IaaS. Клиенты также несут полную ответственность за исправление приложений, развернутых на платформе PaaS.

Управление конфигурацией. Управление конфигурацией безопасности (УКБ) является еще одним важным аспектом в управлении угрозами для сетевых устройств и узлов от неавторизированных пользователей, использующих любые слабости в конфигурации. Кроме того, УКБ связано с программой управления уязвимостями и является подмножеством IT управления конфигурациями (рисунок 4). Защита конфигурации сети, узла и приложения влечет за собой контроль и управление доступом к критической системе и базе данных конфигурационных файлов, в том числе конфигурации ОС, политики брандмауэра, сетевым настройкам зоны локального и удаленного хранения данных и управление базами данных.

Провайдеры сервисов SaaS и PaaS несут полную ответственность за управление конфигурацией их платформ, в то время как клиенты IaaS несут ответственность за управление конфигурацией ОС, приложений и баз данных, развернутых на платформе aaS.

Управление VPC в рамках модели SaaS. Модель предоставления SaaS работает по принципу, который позволяет использовать облачный сервис по Интернет соединению с помощью веб-браузера, работающему на любом устройстве (персональный компьютер, виртуальный рабочий стол, мобильные устройства). Таким образом, основное внимание должно быть обращено на защиту конечных устройств, с помощью которых можно получить доступ к облачному сервису. Модуль управления VPC должен включать в себя требования по управлению конечными устройствами и быть адаптирован к корпоративной среде.

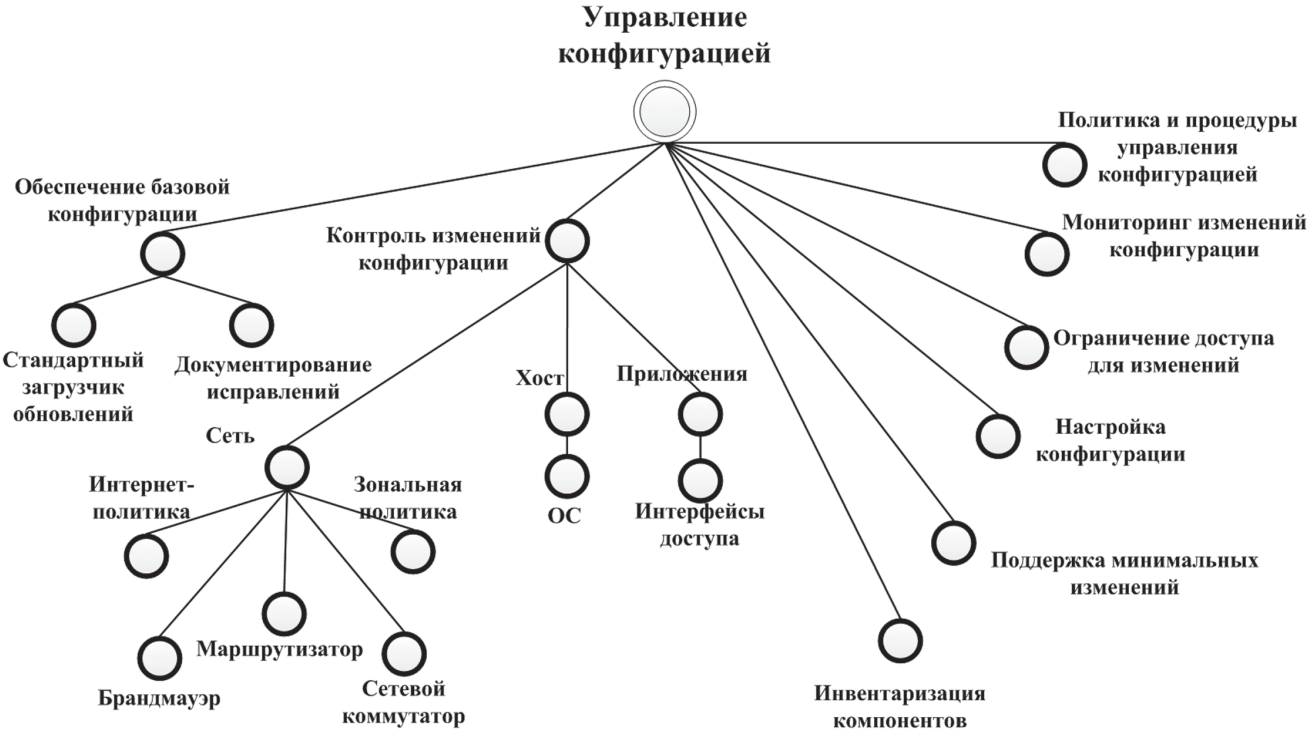

Рис. 4. Дерево целей управления конфигурацией среды облачных вычислений

DOI: 10.7256/2073–8560.2013.5.9587

Определим ключевые требования безопасности, которые определяют области действия VPC SaaS провайдера.

- Системы, сети, узлы, приложения и хранилище, принадлежащие и управляемые провайдером или третьей стороной.
- Персональные компьютеры и мобильные устройства, принадлежащие работникам SaaS провайдера.

Поскольку SaaS сервисы предоставляются через XML интерфейс, клиент имеет ограниченные обязанности по управлению VPC инфраструктурой в облаке.

Однако, клиенты SaaS ответственны за VPC управление, которые взаимодействуют со службой SaaS. Определим ключевые требования безопасности, которые определяют области действия VPC SaaS клиента:

- персональные компьютеры пользователя SaaS;
- приложения и услуги, взаимодействующие с сервисом SaaS;
- тестирование безопасности сервиса SaaS.

Хотя поставщики SaaS ответственны за управление уязвимостями, некоторые клиенты могут выбрать независимое тестирование состояния безопасности приложений, получив соответствующее согласие провайдера.

Тестирование приложений обычно выполняется сторонней организацией и может включать в себя активный анализ приложения и моделирование реальных сценариев атаки с целью обнаружения уязвимостей в приложении. Этот качественный метод также как и объем тестирования может меняться в зависимости от выявленных уязвимостей.

Зоны обеспечения VPC управления должны включать в себя безопасность браузера, систем и приложений (как в доверенной, так и не в доверенной зоне), взаимодействующие с SaaS сервисами.

Управление VPC в рамках модели PaaS. В данном случае управление относится не только к инфраструктуре провайдера, но и к инфраструктуре клиента, связанной с обслуживанием PaaS.

Определим ключевые требования безопасности, которые определяют области действия VPC SaaS провайдера. Подобно модели SaaS, PaaS провайдер ответственен не только за управление VPC инфраструктурой, находящейся под его управлением, а так же за сторонние службы.

В дополнении к обязанностям клиента SaaS клиенты PaaS несут ответственность за VPC управление приложениями, развернутыми и выполняемыми на PaaS платформе. Уязвимости или слабости в конфигурации приложений, находящихся на PaaS платформе, должны быть переданы в цент управления данными. Уязвимости программного обеспечения могут возникать из-за ошибок кодирования или плохого проектного решения. Недостаток конфигурации может возникнуть при использовании неподходящей конфигурации приложений для управления привилегиями и средствами аутентификации. Клиенты PaaS должны руководствоваться общепринятыми действиями Жизненного цикла Разработки Программного Обеспечения (ЖЦРПО), позволяющими уменьшить уязвимости приложения.

PaaS клиенты несут ответственность за VPC управлением следующих областей:

- ПК PaaS пользователей;
- программы для доступа к PaaS сервисам;
- приложения, расположенные на рабочих станциях клиентов и связанные с PaaS сервисами.

Управление VPC в рамках модели IaaS. Управление IaaS VPC отличается от SaaS и PaaS тем фактом, что отсутствует четкое разграничение инфраструктуры, сетевых границ между клиентами и провайдером. Для каждого уровня инфраструктуры (сеть, узел, хранение) у клиента и провайдера есть обя-

DOI: 10.7256/2073–8560.2013.5.9587

занности, заключающиеся в управлении VPC на соответствующих уровнях. Например, в случае общедоступного облака провайдер несет ответственность за доступность общей инфраструктуры, а клиент за доступность своей виртуальной инстанции.

Сфера управления VPC со стороны IaaS провайдера должна включать в себя:

- системы, хост (гипервизор), хранилище и приложения, относящиеся к провайдеру и третьим организациям.
- веб-клиент или станция управления, используемая клиентами для управления их виртуальной инфраструктурой;
- ПК, принадлежащие работникам IaaS и поставщикам.

Клиенты IaaS обязаны осуществлять VPC управление своей виртуальной инфраструктурой, размещенной на общей инфраструктуре IaaS провайдера, включая следующие компоненты.

- Виртуальные серверы.

Включая виртуальные машины (ВМ), которые могут быть либо активными, либо находиться в состоянии бездействия. Управленческий процесс VPC ВМ должен учитывать ОС виртуальных серверов (Fedora Linux, Solaris 10, Windows 2003). Приведём рекомендации, которым должны следовать клиенты в области управления ВМ.

1. Использование образов с подходом стандартной безопасности по умолчанию.
2. Применение стандартов конфигурации.

ОС, сервер приложений, сервер базы данных и веб-сервер должны быть установлены и настроены в соответствии с минимальными правами доступа и принципами усиления безопасности для сокращения площади атаки.

3. Управление конфигурацией.

Необходимо ведение централизованного управления конфигурацией, где находится информация о конфигурации, необходимой для управления большим числом узлов и зон в публичном облаке IaaS. Многочисленные средства управления конфигурацией и сервисные программы коммерческих производителей, таких как: BMC, Configuresoft, HP, Microsoft, IBM, являются общедоступными, включая их открытый исходный код.

- Применение политики сетевого доступа

Необходимо предусмотреть использование межсетевого экрана для создания зон безопасности приложений, размещенных в облаке IaaS, при этом сетевые зонирования играют большую роль в общей архитектуре безопасности. Конфигурацией сетевых политик, позволяющей управлять входящим и исходящим трафиками, необходимо тщательно управлять для снижения угрозы возникновения рисков из-за неправильно подобранной конфигурации. Неправильная конфигурация политики сетевого доступа может предоставить взломщикам возможность для нахождения уязвимостей.

Политики сетевого доступа группируется по следующим категориям:

1. Интернет-политика

В данном случае разрешается трафик между клиентскими виртуальными серверами и хостами по Интернет соединению только в рамках заранее обозначенных портов, при этом вводится запрет на исходящий трафик, инициированный от клиентских виртуальных серверов.

2. Зональная политика

Заключается в разрешении трафика между виртуальными серверами в пределах облака (например, разрешение использования порта 3306 из сервера зоны A в сервер зоны B).

IaaS администраторы несут ответственность за VPC управление системами, которые взаимодействуют с IaaS сервисами и включают в себя:

DOI: 10.7256/2073–8560.2013.5.9587

- облачные инстанции управления, выступающие в роли хоста, в рамках которого клиенты управляют своей виртуальной инфраструктурой.
- ПК администраторов IaaS;
- программы, используемые для доступа к IaaS сервисам.

IaaS клиент может использовать услуги третьих лиц, таких как: RightScale, Enomaly, Elastra и 3tera для управления процедурами развертывания своих публичных и частных облаков в IaaS инфраструктуре.

4. Обнаружение вторжений и реагирование на инциденты

Многоарендная архитектура среды облачных вычислений, предоставляющая различные модели предоставления сервисов (SaaS, PaaS, IaaS) создаёт серьёзные проблемы для клиента и провайдера, так как поверхность нападения такой архитектуры становится очень большой. Управление вторжениями и инцидентами — ключевая функция информационной безопасности корпоративного домена, которые смягчает такие риски, как потеря интеллектуальной собственности, несоблюдение нормативных актов, снижение репутации бренда и мошенничество (рисунок 5). Эти важнейшие функции поддерживают управление безопасностью и позволяют организациям реагировать на указания данных нарушений.

Принимая во внимание многоарендную архитектуру общедоступного облака, которая используется несколькими клиентами, необходимо разделить ответственность за управление вторжениями и инцидентами между клиентом и провайдером.

Традиционно, клиенты среднего и крупного предприятий управляют процессами мониторинга инцидентов, используя либо центр операций внутренней безопасности (SOC), либо через стороннюю управляемую службу. Современный SOC отслеживает события

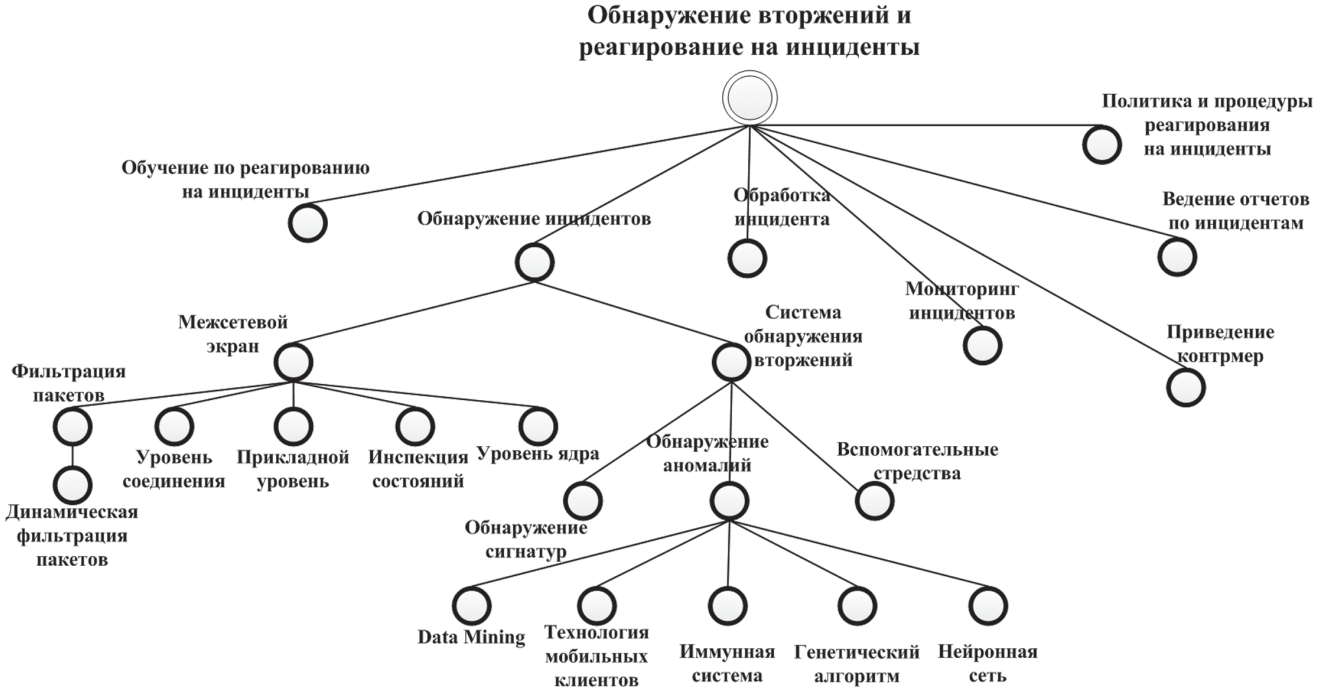

Рис. 5. Дерево целей обнаружения вторжений и реагирования на инциденты среды облачных вычислений

DOI: 10.7256/2073–8560.2013.5.9587

от межсетевых экранов и платформ обнаружения вторжений и реагирует на инциденты, используя группы реагирования на компьютерные происшествия (CERT). Развертывания облачного приложения бросает серьёзный вызов традиционной сетевой модели контроля безопасности, потому что эти приложения больше не будут защищены контролируемыми брандмауэрами и традиционными системами обнаружения вторжений.

Ответственность за контроль вторжений и инцидентов будет зависеть от модели SPI поставки (SaaS, PaaS, IaaS), сервисного соглашения об обслуживании (SLA), инцидентной политики раскрытия информации и модели управления данными. Принимая во внимание тот факт, что провайдеры могут создавать сотни тысяч виртуальных серверов (IaaS), экземпляров приложений (PaaS) и множество сервисов (SaaS), то объем производимых операций может значительно увеличиться и достичь критического значения, которое невозможно будет обработать. Уведомление об инциденте в облаке является не таким простым событием, как текущий процесс управления инцидентами, сопровождаемый командами CERT или SOC. В традиционной модели, эти процессы принадлежат к одной модели управления и реагирования на инциденты, где одна внутренняя группа обрабатывает уведомления и исправления для всех приложений, которыми управляет ИТ-отдел организации. В случае облачной среды, где размещаются тысячи приложений, процесс уведомления более сложен и не будет соответствовать традиционным методам. Новые инструменты реагирования на инциденты, возможно, могут нуждаться в формировании такого направления, как управление сложностями — например, реестр приложения, реализованный CSP›s, с контактной информацией владельцев приложений и автоматизированной системы уведомления для обработки большого количества клиентов (арендаторов).

Обеспечение конфиденциальности данных диктует необходимость изоляции приложений и данных между клиентами. В традиционной архитектуре процесс управления нарушениями сосредоточивается на одном объекте, но в облачной среде, разделение данных размоется достаточно быстро, и инцидентная процедура должна будет выявить зависимости таким образом, чтобы уведомление об инциденте могло быть доставлено всем заинтересованным сторонам.

Учитывая общую инфраструктуру и общий принцип разделения обязанностей, заказчик и провайдер должны иметь оперативный план по преодолению любых нарушения безопасности.

В случае IaaS или PaaS среды, доверительные границы системы и приложений переплетаются между провайдером и клиентом. В результате, обе стороны несут совместную ответственность за мониторинг безопасности и реагировании на инциденты.

Провайдер должен защитить огромное количество связанных с безопасностью данных. Например, на сетевом уровне, провайдер должен контролировать и защищать брандмауэр, систему предотвращения проникновений (IPS), управление инцидентами безопасности и событиями (SIEM) и собирать данные потока маршрутизатора.

На уровне узла провайдер должен собирать системные файлы журнала, на прикладном уровне провайдеры SaaS должны собирать данные журнала приложений, включая информацию об аутентификации и авторизации. То, какие данные собирает провайдер и какие процедуры использует для контроля, является важным аспектом для провайдера для его собственных целей. Кроме того, эта информация важна как для провайдеров, так и для клиентов в случае, если она необходима для реагирования на инциденты и для любой цифровой судебной экспертизы, требуемой для анализа инцидента. Таблица 1 обобщает данные анали-

DOI: 10.7256/2073–8560.2013.5.9587

за стандартов, подходов и моделей, связанных с разграничением полномочий между клиентом и провайдером в области обнаружения вторжений и реагирования на инциденты.

ТАБЛИЦА 1.
РАЗГРАНИЧЕНИЕ ПОЛНОМОЧИЙ МЕЖДУ КЛИЕНТОМ И ПРОВАЙДЕРОМ

Контроль действий		IaaS	PaaS	SaaS
Обнаружение вторжений	Клиент ответственен за:	• контроль виртуальных копий сетевых интерфейсов; • контроль безопасности от вторжений таких систем как OSSEC; • контроль безопасности вычислительных машин, приложений, системы баз данных, хранящейся в системных журналах. • контроль сторонних сервисов, например шифрование данных.	• контроль возможного проникновения в приложения, развернутые на платформе PaaS.	• контроль вторжений в сеть, систему, приложения и базу данных.
	Провайдер ответственен за:	• контроль возможного проникновения в совместно используемую инфраструктуру сети/системы/приложения, включая гипервизоры, например DOS-атаки на сеть.	• контроль совместно используемой инфраструктуры сети/системы/приложений, включая механизм исполнения платформы PaaS и поддерживаемой служба, например атака механизма исполнения PaaS.	
Реагирование на инциденты	Клиент ответственен за:	• реагирование на инциденты и утечку данных с их виртуальных серверов; • информирование пострадавших пользователей системы и приложений, расположенных на дискредитированных виртуальных серверах.	• информирование пострадавших пользователей; • своевременную реакцию на происшествие, выполнение экспертизы и восстановление приложений.	• информирование пострадавших пользователей; • работа с CSP при ликвидации последствий
	Провайдер ответственен за:		• уведомление клиента о вторжениях в их приложения и данные, о существовании угрозы для пользователей.	• уведомление клиента о вторжениях и о существовании угрозы для пользователей.

Заключение

В статье сформулированы практические рекомендации по разграничении полномочий по управлению безопасностью для клиентов публичных облачных сервисов, что позволяет на их основе разработать комплексную модель разграничения полномочий по обеспечению информационной безопасности среды облачных вычислений.

Учитывая, что в большинстве предлагаемых облачных сервисов отсутствует прозрачность в области:

- соглашения об уровне обслуживания,
- реальных возможностей поставщиков,
- управления и обеспечения безопасности,
- созданы предпосылки к разработке нового метода построения гибридной среды облачных вычислений по требованиям информационной безопасности.

DOI: 10.7256/2073–8560.2013.5.9587

Библиография

1. Царегородцев А. В., Качко А. К. Обеспечение информационной безопасности на облачной архитектуре организации // Национальная безопасность.— М.: Изд-во «НБ Медиа», 2011.—№ 5.— С. 25–34.
2. Царегородцев А. В., Качко А. К. Один из подходов к управлению информационной безопасностью при разработке информационной инфраструктуры организации // Национальная безопасность.— М.: Изд-во «НБ Медиа», 2012.—№ 1 (18).— С. 46–59.
3. Чен И. Пэксон И., Пэксон В., (2010) Новые проблемы информационной безопасности облаков. Технический отчёт UCB/EECS-2010–5, Департамент EECS, Университет Калифорнии, Беркли.

References (transliterated)

1. Tsaregorodtsev A. V., Kachko A. K. Obespechenie informatsionnoi bezopasnosti na oblachnoi arkhitekture organizatsii // Natsional'naya bezopasnost'.— M.: Izd-vo «NB Media», 2011.—№ 5.— S. 25–34.
2. Tsaregorodtsev A. V., Kachko A. K. Odin iz podkhodov k upravleniyu informatsionnoi bezopasnost'yu pri razrabotke informatsionnoi infrastruktury organizatsii // Natsional'naya bezopasnost'.— M.: Izd-vo «NB Media», 2012.—№ 1 (18).— S. 46–59.
3. Chen I. Pekson I., Pekson V., (2010) Novye problemy informatsionnoi bezopasnosti oblakov. Tekhnicheskii otchet UCB/EECS-2010–5, Departament EECS, Universitet Kalifornii, Berkli.