Математическая биология и биоинформатика
2015. Т. 10. № 2. С. 567–579. doi: 10.17537/2015.10.567

==========ИНФОРМАЦИОННЫЕ И ВЫЧИСЛИТЕЛЬНЫЕ ==========
==========ТЕХНОЛОГИИ В БИОЛОГИИ И МЕДИЦИНЕ==========

УДК 004.56, 004.75

Обеспечение информационной безопасности облачных вычислений

Исаев Е.А.[1,3], Думский Д.В.[1,3], Самодуров В.А.[1,3], Корнилов В.В.[1,2]

[1]*Национальный исследовательский университет «Высшая школа экономики», Москва, 101000, Россия*
[2]*Институт математических проблем биологии, Российская академия наук, Пущино, Московская область, 142290, Россия*
[3]*Пущинская Радиоастрономическая обсерватория Астрокосмического центра ФИАН, Пущино, Московская область, 142290, Россия*

Аннотация. Стремительное развитие информационных технологий в современном обществе диктует новые требования к технологиям обеспечения информационной безопасности данных, методам удалённого доступа и обработки информации, комплексному снижению финансовых затрат на работу с информацией. В последние годы в качестве идеального решения всех этих задач активно предлагается концепция облачных вычислений. Данная методика действительно даёт ряд несомненных преимуществ при работе с информацией и уже достаточно широко используется в целом ряде направлений научной и деловой деятельности, однако многие аспекты информационной безопасности, характерные для облачных вычислений, всё ещё далеки от удовлетворительного решения. В статье рассматривается основные проблемы обеспечения информационной безопасности облачных вычислений. Представлен обзор методов обеспечения безопасности обработки данных, обсуждается выбор наиболее безопасной модели облачных вычислений, предлагаются способы повышения безопасности облачных вычислений.

Ключевые слова: облачные вычисления, информационная безопасность.

ВВЕДЕНИЕ

На смену парадигме построения на предприятиях и в научных центрах собственных информационно-вычислительного комплексов [1], в последнее время всё большее распространение получает технология облачных вычислений, подразумевающая удалённый (в том числе через Интернет) доступ пользователей к хранилищам данных, вычислительным ресурсам и программным приложениям [2]. Облачные технологии способны представить пользователям необходимые вычислительные мощности за счёт динамического выделения необходимых ресурсов, при этом нагрузка между компьютерами, входящими в вычислительное облако, распределяется автоматически. Клиенты провайдеров облачных услуг получают возможность, посредством любых, в том числе мобильных, устройств доступа в сеть, использовать требующиеся вычислительные ресурсы и объёмы памяти, необходимое программное обеспечение. Хотя назначение облачных вычислений состоит вовсе не в достижении пиковой производительности при решении единственной вычислительной задачи, что является типичным для суперкомпьютеров и вычислительных кластеров [3], но для большинства организаций, в том числе и научных, именно облачные сервисы сегодня являются

наиболее привлекательной моделью доступа к вычислительным ресурсам. Их основные преимущества – удобство доступа, масштабируемость предоставляемых услуг, относительно невысокая (по сравнению с приобретением суперкомпьютера, созданием вычислительного кластера или даже прямой аренды вычислительных ресурсов в центрах обработки данных (ЦОД)) стоимость.

Клиенты облачных сервисов могут существенно уменьшить стоимость как хранения данных, так и использования вычислительных мощностей, используя общедоступные сетевые хранилища и вычислительные ресурсы, в том числе за счёт предоставляемой провайдерами этих услуг возможности изменения используемых ресурсов по требованию клиента и оплаты им только того объёма, который ему в данный момент нужен. Поставщик услуг объединяет ресурсы для обслуживания большого числа потребителей в единый пул для динамического перераспределения мощностей между потребителями в условиях постоянного изменения спроса на мощности. Аппаратные ресурсы, которые больше не нужны для какого-то сервиса или приложения можно быстро переназначить, и дополнительная вычислительная мощность начнёт потребляться другими сервисами для увеличения их эффективности.

Таким образом, одним из основных принципов облачных технологий является возможность использования одних и тех же вычислительных ресурсов различными пользователями (одновременно или в разные моменты времени). Но при этом возникают новые проблемы. С одной стороны, предоставление в аренду пользователям одних и тех же ресурсов, и программного обеспечения является экономически обоснованным решением. С другой стороны, подобный подход требует повышенного внимания к безопасности, разграничению прав, изолированию данных и программных продуктов, а также к балансировке нагрузки на аппаратную часть, что является весьма непростой задачей [4].

Действительно, разнообразие устройств, используемых в облачных вычислениях, радикальным образом снижают стоимость использования вычислительных ресурсов [5]. Уменьшающаяся стоимость распределенных вычислений, общей памяти и систем хранения данных фундаментально меняют экономику обработки данных, делая облачные вычисления весьма привлекательными для многих клиентов. При этом часто упускается из вида тот факт, что как только данные клиента оказываются в облаке, всё управление ими, и, в том числе, забота об их безопасности становится зоной ответственности провайдера облачных вычислений. Однако провайдеры не спешат брать на себя ответственность за безопасность данных[6]. При передаче данных в облако владелец практически лишается возможности контролировать их безопасность [7].

ТЕХНОЛОГИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Одним из основных подходов к реализации облачной инфраструктуры является технология виртуализации – предоставление вычислительных ресурсов, абстрагированное от их реальной аппаратной реализации, например, одновременное выполнение нескольких, изолированных друг от друга, операционных систем (ОС) и приложений на одном компьютере. Совокупность компьютерных ресурсов, эмулирующую работу отдельных компонентов аппаратного или программного обеспечения (ПО), или даже целого компьютера, принято называть виртуальной машиной (ВМ). Наличие нескольких ВМ на одном реальном компьютере обеспечивает возможность независимой работы на одном физическом сервере (узле) нескольких операционных систем и приложений.

Виртуализация может улучшить адаптивность, гибкость и масштабируемость ИТ-среды и существенно снизить расходы. Виртуализация позволяет более эффективно использовать вычислительные мощности и совместно использовать ресурсы различных

аппаратных устройств при обслуживании многопользовательских клиентов. Кроме того, виртуализация ускоряет развертывание рабочих нагрузок, повышает их производительность и доступность, а также дает возможность автоматизировать многие процессы.

В настоящее время существует две основных технологии создания систем облачных вычислений, основанные на виртуализации серверов (рис. 1).

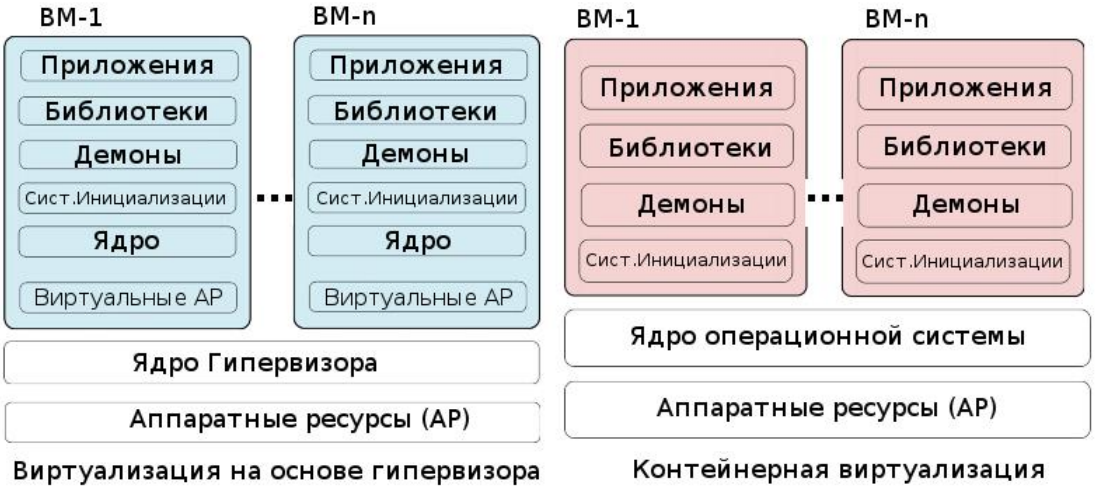

Рис. 1. Сравнение двух технологий виртуализации.

В первом подходе виртуализация осуществляется с помощью гипервизора – программной надстройки над основной ОС, которая отделяет виртуальные машины от сервера и по мере необходимости динамически выделяет вычислительные ресурсы каждой ВМ (Amazon, Azure, VMWare) [8]. Согласно определению облачных технологий, данному NIST (Национальный институт стандартов и технологий США) [9], использование данного подхода не является строгим требованием и существует второй способ, использующий изолированные контейнеры (OpenVZ, LXC (Linux Containers), Docker) [10–13]. В каждом из этих подходов есть как свои преимущества, так и недостатки. Подход с использованием виртуализации позволяет запускать в облаке ОС любых производителей, но теряя при этом в производительности от 8 до 12 процентов по сравнению с использованием физического сервера. Второй подход выгоднее с точки зрения вычислительной производительности системы и экономии дисковых ресурсов, так как контейнеры используют ядро основной системы. При этом пользователи ограничены в выборе ОС только дистрибутивами семейства GNU/Linux, что в большинстве случаев рассматривается как существенный недостаток контейнерной виртуализации. В тоже время, существенный выигрыш в производительности позволяет в этом случае использовать ресурсы облака даже для высокопроизводительных вычислений [10]. В последние годы и такие крупные игроки на рынке облачных услуг, как Amazone и Azure, помимо традиционной виртуализации на основе гипервизоров стали предоставлять услуги на основе контейнерных технологий [14]. Google использовали данную технологию изначально как основную [15].

Вторым недостатком до недавнего времени были серьёзные проблемы в безопасности: так как каждый контейнер имеет доступ к ядру основной системы, то потенциальный злоумышленник мог получить привилегированные права в основной системе взломав один из контейнеров в облаке. Однако ИТ-технологии не стоят на месте и, например, в последних разработках системы виртуализации LXC появилась возможность запускать непривилегированные контейнеры, взломав которые,

злоумышленник получит только ограниченные права пользователя в основной системе [16].

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Хотя облачные вычисления сегодня уже не являются относительно новой технологией, вопросы обеспечения их информационной безопасности продолжают оставаться слабым местом. В связи с технологическими особенностями, используемыми для построения структуры облачных вычислений, к стандартным типам угроз, являющихся следствием размещения ресурсов на физических серверах, добавились сложности, связанные с контролем облачной среды виртуализации, трафика между гостевыми машинами и разграничением прав доступа. Более того, распределенная и открытая структура облачных вычислений с мультидоменной и многопользовательской структурой стала очень привлекательной мишенью для потенциальных злоумышленников.

Архитектура облачных сервисов состоит из трёх взаимозависимых уровней: инфраструктура, платформа и приложения. Каждый из этих уровней может быть уязвим к программным и конфигурационным ошибкам, допущенным пользователями или провайдерами сервиса. Система облачных вычислений может подвергаться нескольким видам угроз безопасности – включая угрозы целостности, конфиденциальности и доступности её ресурсов, данных и виртуальной инфраструктуры, которые могут быть использованы нецелевым образом, например, в качестве площадки для распространения новых атак [17].

Хранение данных в облаке означает, что эти данные содержатся на общедоступных серверах. Если компания перейдёт в облако без учёта непредвиденных последствий, критические корпоративные данные, такие, как, например, информация о клиентах или интеллектуальная собственность, подвергнутся повышенному риску. При этом юридическая ответственность за сохранность информации по-прежнему лежит на организации, разместившей эти данные в облаке, а не на провайдере облачных услуг. Рассмотрим, например, компанию медицинского страхования. Если клиент предоставляет персональную информацию страховой компании, он ожидает, что компания её защитит. И для клиента не важно, что страховая компания доверила хранение этих данных облачному провайдеру, слабо контролирующему свою информационную безопасность. Важна их сохранность и защита от неправомерного распространения.

Другая серьёзная проблема с защитой данных в облаке – это неспособность для клиента облачных услуг самому проводить аудит и контролировать события службы безопасности, например, посредством проверки лог-файлов, что может серьёзно ограничить возможности по поиску происшествий, повлёкших к нарушению безопасности системы.

В облачных вычислениях важную роль выполняет технология виртуализации. Однако принципы виртуализации содержат потенциальные угрозы информационной безопасности облачных вычислений, например, связанные с использованием общих хранилищ данных разными ВМ. Каждая ВМ хранится в виде образа, который представляет собой отдельный файл. Размеры этих файлов могут быть изменены в зависимости от текущих нужд пользователя сервиса. Уменьшение размера раздела одной из ВМ облака и увеличение раздела другой, могут привести к тому, что физические сектора, содержащие информацию об удалённых файлах, переместятся с одной ВМ на другую. В результате пользователь второй ВМ может получить доступ и восстановить данные, которые ранее принадлежали другой организации. Одним из возможных решений является шифрование всей информации. В этом случае

зашифрованная информация не сможет быть восстановлена без подходящих ключей [18], однако следует учитывать, что шифрование может потребовать дополнительных вычислительных ресурсов и значительно замедлять процесс чтения и записи данных.

В противоположность физическому серверу ВМ с такой же ОС и приложениями с идентичными настройками подвержена гораздо большему риску. Если провайдер облака резервирует, управляет или манипулирует виртуальными машинами для клиентов на основе своих собственных конфигурационных шаблонов, то контроль доступа и базовые конфигурации не будут соответствовать таковым в собственном дата-центре организации. Даже в рамках одного провайдера облака, может возникать ситуация, когда настройки экземпляра виртуальной машины в одном размещении будут отличаться от настроек в другом размещении [19].

Виртуальные машины динамичны. Они клонируются и могут перемещаться между физическими серверами. Данная изменчивость влияет на разработку целостности системы безопасности. Однако уязвимости ОС или приложений в виртуальной среде распространяются бесконтрольно и часто проявляются после произвольного промежутка времени (например, при восстановлении из резервной копии). В среде облачных вычислений важно надёжно зафиксировать состояние защиты системы, независимо от её местоположения.

Уязвимости внутри виртуальной среды. Серверы облачных вычислений и локальные серверы используют одни и те же ОС и приложения. Для облачных систем угроза удалённого взлома или заражения вредоносным ПО высока. Система обнаружения и предотвращения вторжений должна быть способна обнаруживать вредоносную активность на уровне виртуальных машин, вне зависимости от их расположения в облачной среде.

Защита бездействующих виртуальных машин. Даже когда виртуальная машина выключена, она также подвергается опасности заражения. Доступа к хранилищу образов виртуальных машин через сеть для этого вполне достаточно, при этом на выключенной виртуальной машине невозможно запустить защитное программное обеспечение. В данном случае должна быть реализована защита не только внутри каждой виртуальной машины, но и на уровне гипервизора.

Защита периметра и разграничение сети. При использовании облачных вычислений периметр сети размывается или исчезает. Это приводит к тому, что менее защищённая часть сети определяет общий уровень защищенности. Для разграничения сегментов с разными уровнями доверия в облаке виртуальные машины должны сами обеспечивать себя защитой, перемещая сетевой периметр к самой виртуальной машине. Корпоративный firewall (межсетевой экран) – основной компонент для внедрения политики ИТ-безопасности и разграничения сегментов сети – не в состоянии повлиять на серверы, размещённые в облачных средах [20].

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Стандартно выделяют три основные задачи информационной безопасности: конфиденциальность, целостность и доступность [21]. Конфиденциальность – это скрытие информации и ресурсов. Целостность – это достоверность данных или ресурсов, обычно связана с предотвращением любых некорректных или неавторизованных изменений. Доступность определяется способностью использовать информацию или ресурсы [22]. Принципиально ожидается, что доступ к данным могут получить только люди, прошедшие аутентификацию в качестве клиента сервиса и владельца именно этих данных.

Один из основных моментов, который необходимо учитывать применительно к безопасности в облаке, состоит в том, что ответственность за использование ресурсов разделяется между клиентом и поставщиком облачного сервиса. И необходимо понимать, где кончается ответственность провайдера облачных вычислений и начинается ответственность клиента.

При построении сложных систем (одной из разновидностей которых являются облака) применяют архитектурную концепцию многоуровневой безопасности (Defense-in-Depth) – механизм, который использует несколько уровней защиты (рис. 2), чтобы увеличить время атакующего, затрачиваемое на попытки взломать систему; а также вести подсчёт количества попыток взлома для принятия решения о блокировке атакующего [23].

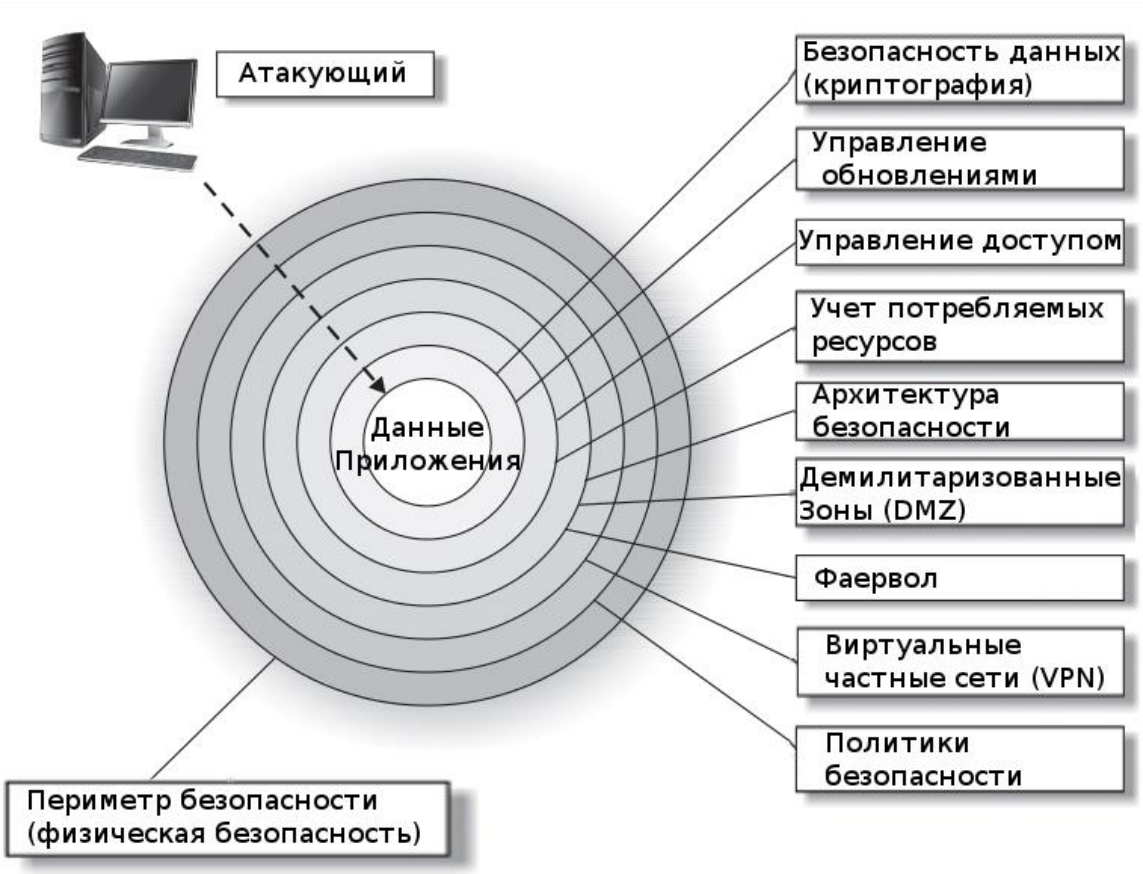

Рис. 2. Многоуровневый подход к безопасности компьютерных систем [24].

Соответственно, при построении системы безопасности среды облаков также можно выделить свои слои контроля и доступа. Облако комбинирует возможности пользователя и поставщика, брандмауэры и разновидности способов изоляции. При этом отдельные элементы безопасности могут контролироваться пользователем независимо от провайдера (рис. 3).

NIST в своей специальной публикации [7] выделяет три модели облачных вычислений: инфраструктура как сервис (IaaS), платформа как сервис (PaaS) и программное обеспечение как сервис (SaaS); при этом для каждого типа управление данными меняется.

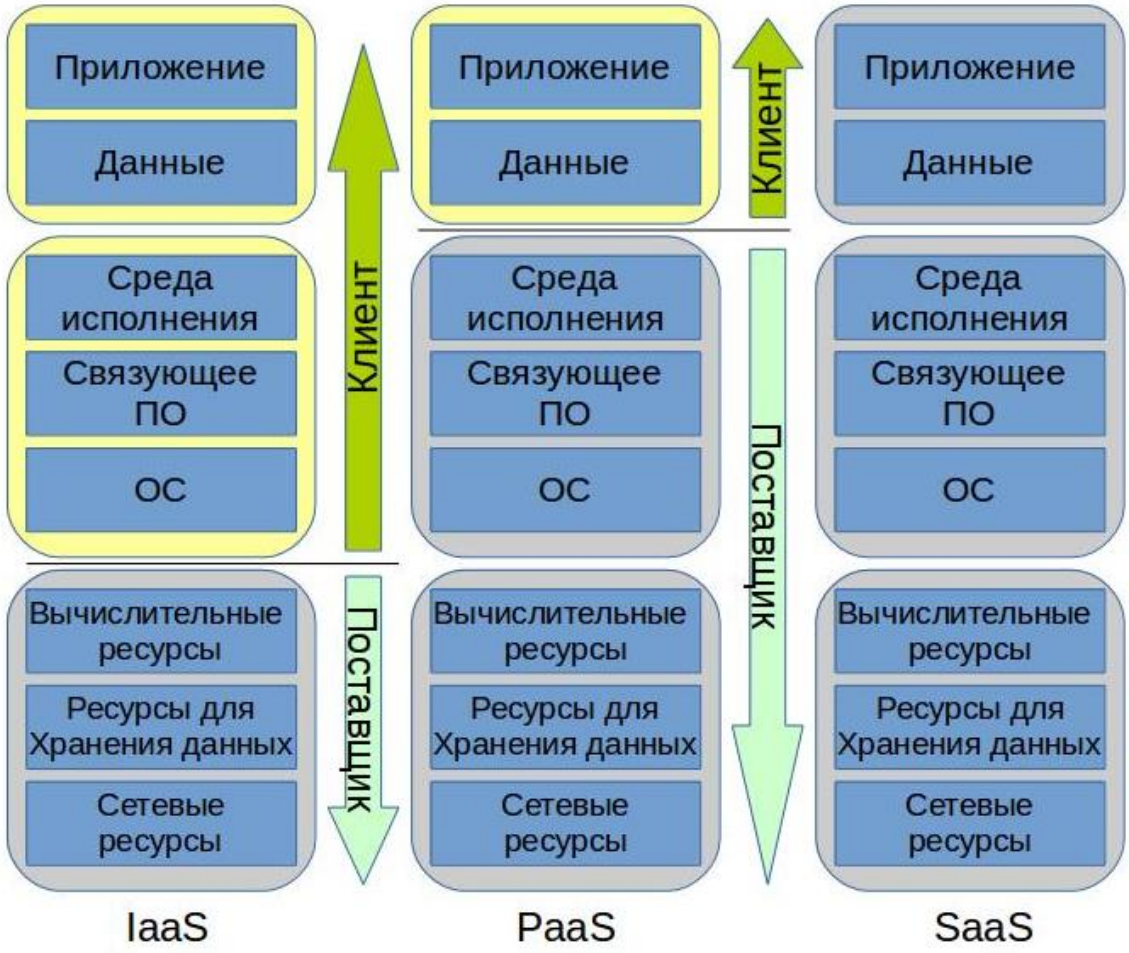

Рис. 3. Многоуровневая система безопасности облаков на примере трёх моделей облачных сервисов. В разных сервисах клиентом контролируются различные слои безопасности независимо от провайдера [25].

Как можно увидеть из рисунка 3, возможности пользователя по управлению системой безопасности зависят от выбора сервисной модели. В модели IaaS (например, IBM SoftLayer или Amazon Web Services) на стороне заказчика можно построить свои собственные технические средства обеспечения безопасности. Клиент может иметь полный контроль над реальной конфигурацией сервера, что гарантирует ему больший контроль рисков безопасности окружения и данных.

В PaaS (IBM Bluemix, Microsoft Windows Azure) поставщик управляет лишь аппаратной платформой и операционной системой, что ограничивает способности предприятия заказчика в управлении рисками на этих уровнях.

В модели SaaS (Salesforce.com, Google) как платформа, так и инфраструктура полностью управляется провайдером облачных услуг. Это означает, что, если операционная система или сервис не настроены должным образом, то данные на более высоком прикладном уровне могут быть в опасности. Пользователям в этом случае не обязательно знать, как предоставляются эти услуги (которые включают в себя сеть, серверы, операционные системы, хранилища и даже отдельные функции приложений). Пользователю важно, чтобы сервис был достаточно дёшев и доступен в любое время, когда он необходим. Поэтому многие детали функционирования сервиса и его инфраструктура оказываются скрытыми для пользователя. В возможностях управления клиент оказывается ограниченным только минимальным набором настроек конфигурации приложения под свои нужды.

Ответственность поставщика облачного сервиса начинается с физической безопасности и безопасности среды. Этот уровень безопасности – высокоуровневый, так как он связан с управляемостью облаком как единой информационной системой. Именно поставщик облачного сервиса осуществляет эксплуатацию физических серверов центров обработки данных, поэтому клиент так же, как и в случае с обычным ЦОД, должен рассмотреть следующие ключевые моменты: физический доступ персонала к серверам и сетевой инфраструктуре, средства пожарной сигнализации и пожаротушения, климатический и температурный контроль над серверами и другими аппаратными средствами, уничтожение выводимых из эксплуатации устройств хранения данных.

В отличие от физической безопасности, сетевая безопасность в первую очередь представляет собой построение надёжной модели угроз, включающей в себя защиту от вторжений и межсетевой экран. Использование межсетевого экрана подразумевает работу фильтра с целью разграничить внутренние сети ЦОД на подсети с разным уровнем доверия. Это могут быть отдельно серверы, доступные из Интернета, или серверы из внутренних сетей.

Доступ через Интернет к управлению вычислительной мощностью облака – одна из ключевых характеристик облачных вычислений. В большинстве традиционных ЦОД доступ инженеров к серверам контролируется на физическом уровне, в облачных средах они работают через Интернет. Разграничение контроля доступа и обеспечение прозрачности изменений на системном уровне являются одними из главных критериев защиты.

Аналогичным образом на общий уровень безопасности влияет выбор модели развёртывания облачной среды: частное облако, инфраструктура, подготовленная для эксклюзивного использования единой организацией; публичное облако, инфраструктура, предназначенная для свободного использования широким кругом пользователей; общественное облако, вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи; и гибридное облако, комбинация из двух или более различных облачных инфраструктур.

Ключевые особенности частных облаков в структуре обеспечения информационной безопасности:

- ответственность клиента за инфраструктуру;
- возможность детальной настройки управления безопасности;
- хорошая видимость внутридневных операций;
- лёгкий доступ к системным логам и политикам;
- приложения и данные остаются внутри сетевого экрана.

Принято считать, что частные облака являются наиболее безопасными, поскольку они позволяют внедрить собственные средства шифрования и защиты ещё на этапе их создания, а также из-за того, что данные остаются в существующей инфраструктуре компании. Однако, если данные не защищены должным образом в облаке они могут быть потеряны или повреждены независимо от того частное это облако или публичное. В частности, недобросовестные лица внутри компании, имеющие доверенный доступ к системе могут просматривать, повреждать и похищать незащищённые данные. Внутренние угрозы не являются какими-то новыми типами угроз, но при переходе корпоративных дата-центров в виртуальные, традиционные механизмы контроля доступа становятся менее эффективными, не будучи приспособленными к виртуальному пространству. Например, когда требуется установить экземпляр базы данных на новый физический сервер, применяются процедуры управления изменениями. Управление изменениями представляет собой процесс прогнозирования и планирования будущих изменений, регистрации всех потенциальных изменений для детального изучения, оценки последствий, одобрения или отклонения, а также

организации мониторинга и координации исполнителей, реализующих изменения в проекте. В виртуальном частном облаке новый экземпляр базы данных может быть создан простым клонированием уже существующего виртуального сервера. Если данные с защищаемого сервера передаются на незащищённый, то эти данные смогут просмотреть пользователи, имеющие меньшие права доступа в этом частном облаке.

Интересно наличие неконтролируемой системами безопасности слепой зоны – трафика между виртуальными серверами в облаке. Традиционные средства мониторинга работают с использованием зеркалирования трафика с портов сетевых устройств и сенсоров, которые способные захватывать и анализировать этот трафик. Однако каналы передачи данных между ВМ создаются в гипервизоре. Вредоносный трафик и данные могут перемещаться между ВМ без выхода в реальную сеть, что означает, что атака будет не замечена традиционными инструментами.

Данные, хранящиеся на выключенных ВМ, также являются уязвимыми, в случаях, когда в основной ОС, на которой они размещаются, контроль доступа не настроен должным образом, или не установлены обновления, исправляющие критические уязвимости.

На другом полюсе (в сторону уменьшения безопасности) принято располагать публичные облака. Можно отметить следующие особенности публичных облаков:

- за инфраструктуру отвечает провайдер;
- меньшая настраиваемость управления безопасностью;
- нет видимости внутридневных операций;
- трудный доступ к логам и политикам;
- приложения и данные используются публично.

Используя публичное облако, организации могут воспользоваться инфраструктурой провайдера в облаке (IaaS), платформой (PaaS) и программным обеспечением (SaaS). Данные сохраняются в среде облачного провайдера, с использованием арендуемой инфраструктуры коммерческих ЦОД. В большинстве случаев экономия средств в публичном облаке достигается за счёт более эффективного использования общих физических ресурсов. Это может означать как предоставление клиентам разных ВМ, размещённых на одном и том же физическом сервере, так и организация доступа клиентов к одному и тому же сервису или приложению под разными учётными записями. Например, популярное облачное CRM-приложение salesforce.com является примером предоставления одного и того же сервиса разным клиентам с использованием уникальных логинов для предотвращения неавторизованного доступа, хотя при этом данные разных пользователей оказываются перемешанными на одном хранилище. В любом случае при использовании виртуализации приходится принимать во внимание весь комплекс проблем информационной безопасности, связанный с этой технологией.

Конечно, в рамках публичного облака возможно и предоставление клиенту целиком отдельного, выделенного компьютерного ресурса, что, в частности, даёт возможность более качественного мониторинга и аудита. Однако такой дополнительный уровень комфорта в обеспечении безопасности часто сопровождается существенным увеличением цены использования облачных ресурсов, что может в целом снизить преимущества таковых перед собственным дата-центром [19].

Классические угрозы информационной безопасности в публичном облаке становятся особенно актуальными. Так, например, администратор крупного облачного ресурса имеет доступ к данным множества клиентов. Он легко может осуществить несанкционированные действия над этими данным, при этом такие события в принципе могут быть никогда не обнаружены. Существуют и внешние угрозы безопасности, такие как, например, удалённые хакерские атаки. В публичных облаках размещается огромное количество корпоративных данных, что делает их привлекательными для злоумышленников. Обнаруживать уязвимости в веб-приложении ресурса, содержащего

данные 100 компаний гораздо интереснее, чем взламывать веб-приложение одиночной компании. Аналогично атака на сетевое хранилище резервных копий множества крупных компаний может дать больше данных, чем взлом хранилища, принадлежащего только одной организации.

И даже когда хранилище данных достаточно хорошо защищено от внешних атак, а контроль и разграничение доступа предоставляет только минимальные полномочия особенно доверенным лицам, все ещё остаются открытыми вопросы безопасности при передаче данных между клиентом и облачной инфраструктурой. Сегодня существует множество стандартов и технологий передачи данных по информационным сетям, и задача обеспечения безопасности информации в них является абсолютно нетривиальной, особенно в случае использования беспроводных сетей. Злоумышленники могут перехватить данные множеством способов, например, с помощью поддельных серверов доменных имён, перехвата маршрутов и трафика при использовании сотрудниками компании не доверенных облаков [26] и общественных Wi-Fi точек доступа и др.

Организации могут повысить уровень безопасности при использовании гибридного подхода к облачным вычислениям, который сочетает в себе публичные и частные облака. Часть данных, которые классифицируются организацией как наиболее критические остаются в частном облаке, тогда как все остальные данные хранятся в публичном облаке.

Хотя этот подход может гарантировать большую безопасность, чем стандартная модель публичного облака, гибридные облака несут в себе те же риски, как частные и публичные облака в случаях неправильного их использования. Сохранение критически важных данных внутри предприятия требует вовлечения механизмов и процедур, гарантирующих, что эти данные не попадут наружу, в публичное облако.

Таким образом, для облачных технологий наблюдается обратная зависимость: при увеличении степени открытости технологии, гибкости работы с ней и универсальности доступа, уменьшается защищенность системы и усложняется методика обеспечения её безопасности.

Для того, чтобы создать более безопасную среду облачных вычислений, организации могут начать с простых шагов, например, с разработки политики и процедуры безопасности, повышения прозрачности в использовании облачных приложений, платформ и инфраструктуры, и защиты данных с шифрованием и усилением процедуры доступа к элементам управления, таких как многофакторная аутентификация [27].

ИТ-организации должны сделать больший акцент на усиление контроля доступа пользователей методом многофакторной аутентификации. Это ещё более важно для компаний, которые дают третьим сторонам и поставщикам доступ к своим данным в облаке. Многофакторные решения аутентификации, управляемые централизованно, обеспечат более безопасный доступ ко всем приложениям и данным – вне зависимости от того, находятся ли они в облаке или в локальной сети [27].

Технически хотя и сложно, но все же вполне реализуемо (в частном облаке – уже сейчас) настроить на всех промежуточных уровнях элементы шифрования, аутентификации, защиты данных. В последние несколько лет, например, переживают бурный рост различные облачные системы медицинской направленности (см., например, [28]), хотя ещё несколько лет назад из-за проблем обеспечения конфиденциальности и сохранности персональных данных облака не рекомендовались для употребления медициной. В данный момент медицинские облака строятся на основе частных облаков с эшелонированной многослойной защитой и управляемой обычно специальным сервером безопасности данных.

Существует несколько способов защитить данные в облаке. Часть из них уже упоминались – это контроль доступа и мониторинг. Однако наиболее эффективным и

при этом универсальным способом обеспечить защиту данных, их конфиденциальность и целостность – это использованием шифрования данных при их передаче по информационным сетям и при хранении внутри облака. Например, в руководстве по информационной безопасности [29], разработанном Альянсом безопасности облаков, утверждается, что шифрование предоставляет преимущества наименьшей зависимости как от провайдера облачного сервиса, так и от эксплуатационных ошибок.

Защита данных, основанная на шифровании, делает эти данные бесполезными для любого лица, не имеющего ключей для их дешифровки. И не важно, находятся эти данные в процессе передачи или хранения, они остаются защищёнными. Владелец ключей шифрования поддерживает безопасность данных, и принимает решения кому, и к каким данным предоставлять доступ. Процедура шифрования может быть встроена в существующий рабочий процесс облачных сервисов. Например, администратор может зашифровывать все данные резервного копирования перед отправкой их в облачное хранилище. Сотрудник организации может защитить корпоративную интеллектуальную собственность, прежде чем положить его в частное облако. Представитель компании может зашифровать личные контракты клиентов, прежде чем отправить их в совместное рабочее место в публичном облаке.

Итак, можно заключить, что в идеале нам, как минимум, необходимо:

- задействовать между облаком и потребителем облачных услуг функции шифрования;
- наладить адаптивный и динамический выбор ближайшего (по критериям времени отклика, загруженности и другим параметрам) облачного шлюза, при этом ограничивать подключение потребителя одним определенным шлюзом неразумно – сразу теряется большая часть преимуществ от перехода к модели облачных вычислений;
- настроить шифрованную передачу данных внутри облачной среды.

ЗАКЛЮЧЕНИЕ

Существует множество преимуществ использования облачных сервисов. Экономия средств от использования масштабируемых и разделяемых ресурсов, доступность в любое время с многочисленных мобильных устройств, высокая доступность больших хранилищ для резервного копирования, простота использования. Однако облака, как частные, так и публичные, вводят дополнительный слой абстракции между первоначальным владельцем данных и теми, кто в реальности управляет этими данными.

Одним из универсальных способов обеспечения защиты данных в облаке является выбор решения безопасности, основанного на шифровании данных на уровне файлов прежде чем они покинут доверенную зону. ИТ-администраторы и пользователи могут частично вернуть себе контроль над обеспечением безопасности своих данных, используя решения защиты, основанные на шифровании данных, так как эти решения переносимы на все вычислительные платформы и операционные системы и работают в любом компьютерном окружении. Использование подходящих методов шифрования предотвращает неавторизованный доступ к данным независимо от того, где они находятся (в процессе передачи или хранения в облаке), и это означает, что организации могут использовать преимущества облачных вычислений, не подвергая важные данные риску или сводя этот риск к минимуму.

СПИСОК ЛИТЕРАТУРЫ

1. Лахно В.Д., Исаев Е.А., Пугачев В.Д., Зайцев А.Ю., Фиалко Н.С., Рыкунов С.Д., Устинин М.Н. Развитие информационно-коммуникационных технологий в

Пущинском научном центре РАН. *Математическая биология и биоинформатика*. 2012. Т. 7. № 2. С. 529–544. doi: 10.17537/2012.7.529.

2. Antonopoulos N., Gillam L. *Cloud Computing: Principles, Systems and Applications.* London: Springer-Verlag, 2010. 379 p.
3. Корнилов В.В., Исаев Е.А., Исаев К.А. Перспективы использования центров обработки данных при решении задач математической биологии и биоинформатики. *Математическая биология и биоинформатика*. 2015. Т. 10. № 1. С. 60–71. doi: 10.17537/2015.10.60.
4. Оплачко Е.С., Устинин Д.М., Устинин М.Н. Облачные технологии и их применение в задачах вычислительной биологии. *Математическая биология и биоинформатика*. 2013. Т. 8. № 2. С. 449–466. doi: 10.17537/2013.8.449.
5. Исаев Е.А., Корнилов В.В. Проблема обработки и хранения больших объемов научных данных и подходы к ее решению. *Математическая биология и биоинформатика*. 2013. Т. 8. № 1. С. 49–65. doi: 10.17537/2013.8.49.
6. Amazon Web Services Customer Agreement. *Website of Amazon Web Services*. 2008. URL: http://aws-portal.amazon.com/gp/aws/developer/terms-and-conditions.html (дата обращения: 21.12.2015).
7. Jansen W, Grance T. *Guidelines on Security and Privacy in Public Cloud Computing*. 2011. 80 p. (NIST Special Publication 800-144). URL: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf (дата обращения: 09.10.2015).
8. White J.S., Pilbeam A.W. A survey of virtualization technologies with performance testing. *arXiv.org: Cornell University Library.* URL: http://arxiv.org/pdf/1010.3233.pdf (дата обращения: 22.10.2015).
9. Mell P., Grance T. *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*. 2011. 7 p. (NIST Special Publication 800-145). URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (дата обращения: 09.10.2015).
10. Xavier M.G., Neves M.V., Rossi F.D., Ferreto T.C., Lange T., De Rose C.A.F. Performance Evaluation of Container-Based Virtualization for High Performance Computing Environments. In: *21st Euro. Int. Conf. on Parallel, Distrib. & Network-based Processing.* IEEE, 2013. P. 233–240.
11. Bardac M., Deaconescu R., Florea A.M. Scaling Peer-to-Peer testing using Linux Containers. In: *Roedunet International Conference (RoEduNet).* IEEE, 2010. P. 287–292.
12. Yuhao Z., David M.N. A Virtual Time System for OpenVZ-Based Network Emulations. In: *Proceeding PADS '11 Proceedings of the 2011 IEEE Workshop on Principles of Advanced and Distributed Simulation.* 2011. P. 1–10.
13. Bui T., Analysis of Docker Security. *arXiv.org: Cornell University Library.* URL: http://arxiv.org/pdf/1501.02967.pdf (дата обращения: 21.12.2015).
14. Morabito R. Power Consumption of Virtualization Technologies: an Empirical Investigation. *arXiv.org: Cornell University Library.* URL: http://arxiv.org/pdf/1511.01232v1.pdf (дата обращения: 21.12.2015).
15. Cacciatore K., Czarkowski P., Dake S., Garbutt J., Hemphill B., Jainschigg J., Moruga A., Otto A., Peters C., Whitaker B.E. Exploring Opportunities: Containers and OpenStack. *OpenStack White Paper.* 2015. 19 p. URL: https://www.openstack.org/assets/pdf-downloads/Containers-and-OpenStack.pdf (дата обращения: 21.12.2015).
16. Reshetova E., Karhunen J., Nyman T., Asokan N. Security of OS-level virtualization technologies. *arXiv.org: Cornell University Library.* URL: http://arxiv.org/pdf/1407.4245v1.pdf (дата обращения: 21.12.2015).

17. Patel A., Taghavi M., Bakhtiyari K., Junior J.C. An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications*. 2013. V. 36. P. 25–41.
18. Brenton C. *The basics of virtualization security*. Cloud Security Alliance, 2011. 17 p. URL: https://cloudsecurityalliance.org/wp-content/uploads/2011/11/virtualization-security.pdf (дата обращения: 09.10.2015).
19. Kelley D. How Data-Centric Protection Increases Security in Cloud Computing and Virtualization Security Curve. *Website of Cloud Security Alliance.* 2011. P. 1–6. URL: https://cloudsecurityalliance.org/wp-content/uploads/2011/11/DataCentricProtection_intheCloud.pdf (дата обращения: 09.10.2015).
20. Бердник А.В. Проблемы безопасности облачных вычислений. Анализ методов защиты облаков от cloud security alliance. Альманах современной науки и образования. В: *Альманах современной науки и образования*. Тамбов: Грамота, 2013. № 10. С. 35–38.
21. Lubacz J., Mazurczyk W., Szczypiorski K. Principles and Overview of Network Steganography. *Communications Magazine*. IEEE, 2014. V. 52. № 5. P. 225–229. URL: http://arxiv.org/pdf/1207.0917.pdf (дата обращения: 09.10.2015).
22. Bishop M. *Introduction to Computer Security, 1st ed*. Boston: Pearson Education, 2004. 747 p.
23. Prescott E. Small. *Defense in Depth: An Impractical Strategy for a Cyber World*. SANS Institute, 2011. 24 p. URL: https://www.sans.org/reading-room/whitepapers/assurance/defense-depth-impractical-strategy-cyber-world-33896 (дата обращения: 21.12.2015).
24. Harris S. *CISSP All-in-One Exam Guide, 6th Edition.* Osborne: McGraw-Hill, 2012. 1456 p.
25. Ржаби В. *Избавьтесь от опасений относительно безопасности данных в облаке*. IBM developerWorks, 2015. 16 p. URL: https://www.ibm.com/developerworks/ru/library/dm-1408datasecuritycloud/dm-1408datasecuritycloud-pdf.pdf (дата обращения: 09.10.2015).
26. *Avoiding the hidden Costs of the Cloud*: report of Symantec Corporation. 2013. P. 1–11. URL: www.symantec.com/content/en/us/about/media/pdfs/b-state-of-cloud-global-results-2013.en-us.pdf (дата обращения: 21.12.2015).
27. *The Challenges of Cloud Information Governance: A Global Data Security Study*: Ponemon Institute Research Report. 2014. P. 1–30. URL: http://www2.safenet-inc.com/cloud-security-research/SafeNet-Cloud-Governance.pdf (дата обращения: 21.12.2015).
28. Sultan N. Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management.* 2014. V. 34. P. 177–184.
29. Hoff Ch. In: *Security guidance for critical areas of focus in cloud computing*. 2011. P. 12–20. URL: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf (дата обращения: 21.12.2015).

Материал поступил в редакцию 15.12.2015, опубликован 23.12.2015.