№ 1 (21), 2023

Издание Ассоциации
«Институт внутренних аудиторов»

Внутренний аудитор

Итоги X Национальной премии «Внутренний аудитор года» 2022

Внутренний аудит в быстро меняющемся мире. Переосмысление понятия устойчивой организации

Интервью с Людмилой Диордиевой

Ключевые индикаторы риска: факторы, влияющие на эффективность внедрения

Подходы к аудиту информационной безопасности систем облачных вычислений

Непрерывный аудит: практика запуска в компании

Институт внутренних аудиторов

Содержание

Подходы к аудиту информационной безопасности систем облачных вычислений (cloud security)

Алексей Алексеев, CIA, CISSP, CEH, CISA, CGEIT, CISM, MBA, CRMA, CRISC, CFE, CDPSE, PMP, PMI-ACP

Последние несколько лет мир постоянно меняется. Сначала пандемия приучала нас к удаленному режиму работы, и, тем самым, развеяла миф о небезопасности облачных технологий, так как компании, ранее не использовавшие облака, убедились на своем опыте в их надежности. Теперь зарубежные вендоры и провайдеры уходят с рынка, и российский бизнес ищет альтернативные способы решения задач, стараясь сохранить тот же результат. Российские компании, в большинстве своем, уже завершили миграцию из зарубежных ЦОДов* в отечественные облачные решения (собственные или арендуемые), инфраструктура которых усиленными темпами развивается, чтобы удовлетворить активно прогрессирующий спрос со стороны не только бизнеса, но и госсектора. С учетом данной тенденции вопрос обеспечения безопасности облачных систем как никогда актуален: в частности, в данной статье будут рассмотрены подходы к оценке рисков и внутреннему ИТ-аудиту со стороны корпоративного пользователя услуг облачных вычислений (частной компании или бюджетной организации).

Определение безопасности облачных вычислений в контексте Модели линий защиты

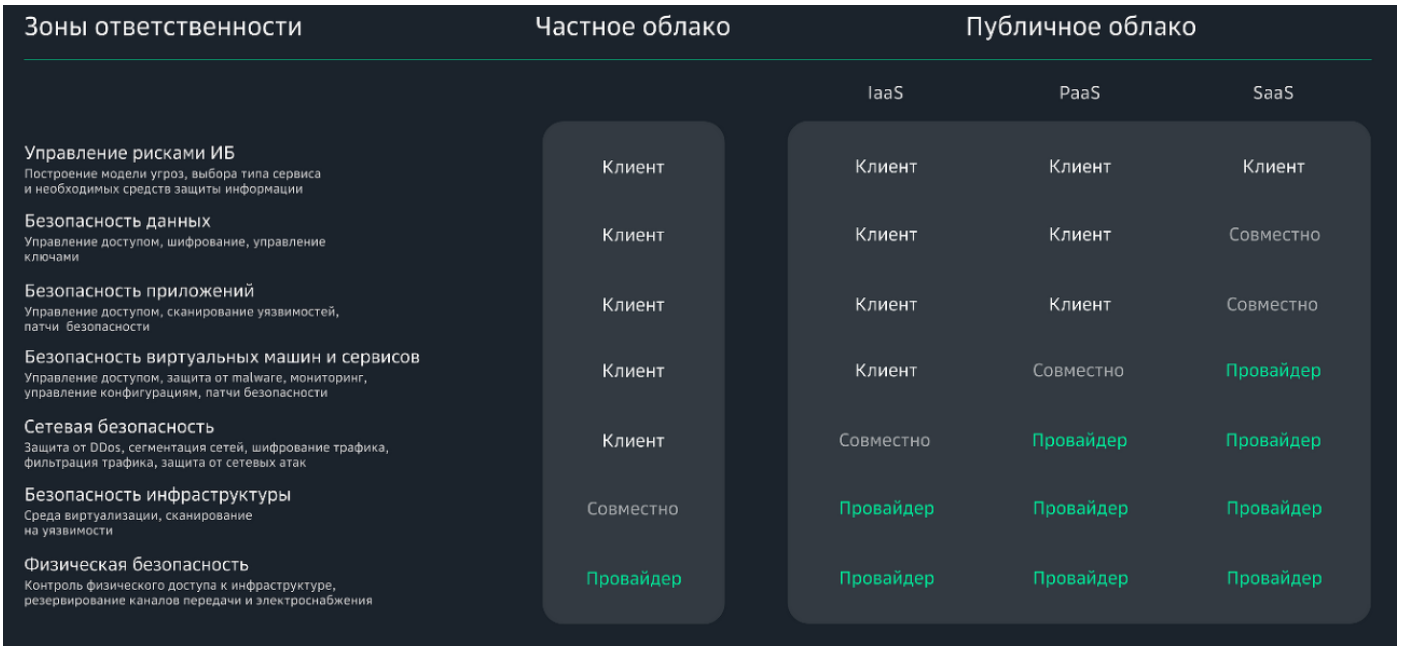
Безопасность облачных вычислений — это дисциплина кибер-безопасности, посвященная защите систем облачных вычислений. Это включает в себя обеспечение конфиденциальности и безопасности данных в онлайн-инфраструктуре, приложениях и платформах. Защита этих систем требует взаимных усилий облачных провайдеров и клиентов, которые их используют, независимо от того, использует ли их физическое лицо, малый и средний бизнес или предприятие. Соответственно, как провайдер облачных услуг (как 1-я линия защиты), так и непосредственно клиент-пользователь (как 1-я, 2-я и 3-я линии защиты) выступают субъектами контрольных мероприятий по обеспечению защиты данных клиента. Внешние организации, осуществляющие независимую оценку соответствия инфраструктуры облачных сервисов предъявляемым требованиям (напр., международные – Uptime Institute, PCI DSS, Cloud Security Alliance; национальные – ФСТЭК), могут выступать в качестве 4-й линии защиты элементов облачных вычислений.

Облачные провайдеры размещают вычислительные среды, предоставляющие услуги, на своих серверах через постоянное подключение к сети Интернет. Поскольку успешность и жизнеспособность их бизнеса напрямую зависит от доверия клиентов, для обеспечения конфиденциальности и безопасного хранения данных клиентов используется широкий спектр методов облачной безопасности. Однако облачная безопасность также частично находится в руках и самого клиента. Понимание особенностей распределения зон ответственности провайдера и клиента имеет решающее значение для надежного решения по обеспечению безопасности в облаке.

……

*Центр (хранения и) обработки данных (ЦОД / ЦХОД) (ср. англ. data center) — специализированное здание для размещения (хостинга) серверного и сетевого оборудования и подключения абонентов к каналам сети Интернет.

В качестве примера можно привести схему распределения обязанностей между провайдером и клиентом в зависимости от модели потребления облачных услуг в компании Cloud:



Зоны ответственности	Частное облако	Публичное облако		
		IaaS	PaaS	SaaS
Управление рисками ИБ Построение модели угроз, выбора типа сервиса и необходимых средств защиты информации	Клиент	Клиент	Клиент	Клиент
Безопасность данных Управление доступом, шифрование, управление ключами	Клиент	Клиент	Клиент	Совместно
Безопасность приложений Управление доступом, сканирование уязвимостей, патчи безопасности	Клиент	Клиент	Клиент	Совместно
Безопасность виртуальных машин и сервисов Управление доступом, защита от malware, мониторинг, управление конфигурациям, патчи безопасности	Клиент	Клиент	Совместно	Провайдер
Сетевая безопасность Защита от DDos, сегментация сетей, шифрование трафика, фильтрация трафика, защита от сетевых атак	Клиент	Совместно	Провайдер	Провайдер
Безопасность инфраструктуры Среда виртуализации, сканирование на уязвимости	Совместно	Провайдер	Провайдер	Провайдер
Физическая безопасность Контроль физического доступа к инфраструктуре, резервирование каналов передачи и электроснабжения	Провайдер	Провайдер	Провайдер	Провайдер

Источник: https://sbercloud.ru/ru/docs/overview/security-introduction/topics/responsibility-areas.html#responsibility-areas-responsibles

По своей сути облачная безопасность состоит из следующих категорий, представляющих систему внутреннего контроля (СВК):
• Безопасность данных (Data security)
• Управление идентификацией и доступом (Identity and access management)
• Организационное управление (политика предотвращения, обнаружения и смягчения угроз)
• Планирование долгосрочного хранения данных и непрерывности бизнеса (BC)
• Соблюдение правовых норм

Приведенные аспекты облачной безопасности могут казаться очень близкими традиционной безопасности ИТ-систем, но на самом деле подходы к их аудиту существенно отличаются.

Аспекты организации систем облачных вычислений при оценке рисков для целей аудита информационной безопасности

Безопасность облачных вычислений (cloud security) — это совокупность технологий, протоколов и лучших практик, которые защищают среды облачных вычислений, приложения, работающие в облаке, и данные, хранящиеся в облаке. Защита облачных сервисов начинается с понимания того, что именно защищается, а также системных аспектов, которыми необходимо управлять.

В целом, разработка серверной части для устранения уязвимостей безопасности в значительной степени находится в руках поставщиков облачных услуг. Помимо выбора поставщика, заботящегося о безопасности, клиенты должны сосредоточиться в основном на правильной конфигурации услуг и безопасных привычках использования. Кроме того, клиенты должны быть уверены, что любое оборудование и сети конечного пользователя должным образом защищены.

Обеспечение облачной безопасности как комплекс мероприятий направлено на защиту следующих элементов, независимо от конфигурации распределения обязанностей между провайдером и клиентом:

• Физические сети и инженерные системы — маршрутизаторы, электроэнергия, кабели, климат-контроль и т. д.
• Емкости для хранения данных — жесткие диски и т. д.
• Серверы данных — основное сетевое вычислительное оборудование и программное обеспечение.
• Среды компьютерной виртуализации — программное обеспечение виртуальных машин, хост-компьютер (host machine) и компьютеры, подключенные к нему (guest machines).
• Операционные системы (ОС) — ПО, обеспечивающее работу сервиса на инфраструктурном уровне.
• Межплатформенное ПО (middleware) — управление интерфейсом прикладного программирования (API).
• Среды выполнения (runtime environments) — выполнение и поддержка работающей программы.
• Данные — вся информация, которую возможно хранить, изменять и к которой можно обеспечивать доступ в пределах облачной среды
• Приложения — традиционные программные сервисы (например, электронная почта, ПО для бухгалтерского учета, пакеты для повышения производительности и т. д.)
• Аппаратное обеспечение конечного пользователя (end-user hardware) — компьютеры, мобильные устройства, устройства, работающие по технологии «Интернет вещей» (Internet of Things, IoT) и т. д.

В средах облачных вычислений распределение прав собственности между провайдером и клиентом на вышеуказанные компоненты может сильно различаться. Это может привести к неясности сферы ответственности клиента за безопасность. Поскольку защита облака может выглядеть по-разному в зависимости от того, кто имеет полномочия в отношении каждого компонента, ИТ-аудитору важно понимать сложившиеся подходы к распределению ответственности на рынках облачных решений.

Для упрощения компоненты облачных вычислений защищены с двух основных направлений: способов предоставления облачных сервисов и моделей развертывания облачных сред.

1. Типы облачных сервисов предлагаются сторонними поставщиками в виде модулей, используемых для создания облачной среды. Вы можете управлять различными компонентами внутри сервиса в зависимости от его типа:

• Ядром любой сторонней облачной услуги является поставщик, управляющий физической сетью, хранилищем данных, серверами данных и платформами виртуализации компьютеров. Услуга хранится на серверах провайдера и виртуализируется через их внутреннюю управляемую сеть для доставки клиентам для удаленного доступа. Это разгружает оборудование и другие затраты на инфраструктуру, чтобы предоставить клиентам доступ к своим вычислительным мощностям из любого места через подключение к Интернету.

• Облачные сервисы типа «Программное обеспечение как услуга» (Software-as-a-Service, SaaS) предоставляют клиентам доступ к приложениям,

которые размещаются исключительно на серверах провайдера. В данном случае провайдер управляет приложениями, данными, средой выполнения, межплатформенным ПО и операционной системой. Клиент, в свою очередь, отвечает только за пользование приложениями. В качестве примеров SaaS-сервисов можно выделить: Yandex Cloud, 1С в облаке, Google Drive, Slack, Salesforce, Microsoft 365, Cisco WebEx, Evernote.

• Облачные сервисы типа «Платформа как услуга» (Platform-as-a-Service, PaaS) предоставляют клиентам среду для разработки собственных приложений, которые запускаются в собственной виртуализированном пространстве («песочнице») клиента на серверах провайдера. Провайдеры управляют средой выполнения, межплатформенным ПО, операционной системой. Клиентам поручено управлять своими приложениями, данными, доступом пользователей, устройствами конечных пользователей и сетями конечных пользователей. В качестве примеров российских компаний, которые предоставляют PaaS-сервисы, можно выделить: Т1 Интеграция, VK Цифровые Технологии, Cloud, СофтЛайн и пр.

• Облачные сервисы типа «Инфраструктура как услуга» (Infrastructure-as-a-Service, IaaS) предлагают клиентам оборудование и платформы удаленного подключения для размещения основной части их вычислительных сред, вплоть до операционной системы. Провайдеры управляют только основными облачными сервисами. Перед клиентами стоит задача защитить все, что находится поверх ОС, включая приложения, данные, среды выполнения, межплатформенную ПО и непосредственно саму ОС. Кроме того, клиентам необходимо управлять доступом пользователей, устройствами конечных пользователей и сетями конечных пользователей. В качестве примеров российских провайдеров IaaS-сервисов можно выделить: Ростелеком-ЦОД, DataFort (Билайн), Yandex Cloud и пр.

2. Облачные среды — это модели развертывания, в которых один или несколько облачных сервисов создают систему для конечных пользователей и организаций. Эти сегменты управленческих обязанностей, включая безопасность, распределяются между клиентами и поставщиками.

К настоящему времени сформировались следующие модели облачных сред:

- Общедоступные облачные среды (Public cloud environments) состоят из облачных сервисов с несколькими арендаторами, в которых клиент совместно использует серверы поставщика с другими клиентами, например, офисное здание или коворкинг. Это сторонние службы, управляемые провайдером для предоставления клиентам доступа через сеть Интернет.
- Частные сторонние облачные среды (Private third-party cloud environments) основаны на использовании облачной службы, которая предоставляет клиенту эксклюзивное использование собственного облака. Эти среды с одним клиентом-арендатором обычно управляются внешним провайдером.
- Частные внутренние облачные среды (Private in-house cloud environments) также состоят из серверов облачных служб с одним клиентом-арендатором, но работают из собственного частного ЦОДа. В этом случае эта облачная среда управляется самим бизнесом, чтобы обеспечить надлежащую управляемость и наблюдаемость каждого элемента инфраструктуры.
- Мультиоблачные среды (Multi-cloud environments) environments) предполагают использование двух или более облачных служб от разных поставщиков. Это может быть любое сочетание общедоступных и/или частных облачных сервисов.
- Гибридные облачные среды (Hybrid cloud environments) представляют собой сочетание частного стороннего облака и/или локального частного облачного центра обработки данных с одним или несколькими общедоступными облаками.

Исходя из вышеизложенного ИТ-аудитору следует понимать различия в конфигурации обеспечения безопасности облачных вычислений в зависимости от типа облачного пространства, и, исходя из этого, осуществлять оценку присущих рисков и рисков контрольных процедур.

Задачи СВК в обеспечении безопасности облачных вычислений

Каждый элемент СВК работает для выполнения одного или нескольких из следующих действий:

• активация восстановления данных в случае их потери;
• защита хранилища и сетей от злонамеренной кражи данных;

• снижение до допустимого уровня риска человеческой ошибки или халатности, которые вызывают утечку данных;
• снижение ущерба в результате компрометации данных или системы.

Безопасность данных — это аспект облачной безопасности, который включает техническую сторону предотвращения угроз. Инструменты и технологии позволяют поставщикам и клиентам устанавливать барьеры между доступом и видимостью конфиденциальных данных, и аудитору необходимо оценить, насколько данные возможности используются. В частности, одним из самых распространенных инструментов защиты данных является шифрование (encryption). С помощью данного инструмента ваши данные кодируются по предопределенному алгоритму (протоколу шифрования), и их может прочитать только тот, у кого есть ключ-дешифратор. Если ваши данные потеряны или украдены, они будут практически нечитаемы и бессмысленны. Вместе с тем, внутреннему аудитору важно убедиться, что используемый протокол шифрования достаточно надежен и соответствует требованиям безопасности. Кроме этого, важно отметить организацию защиты передачи данных в рамках облачной инфраструктуры через виртуальные частные сети (VPN).

Управление доступом (Identity and access management, IAM) относится к организации дифференцированного уровня доступа, предлагаемого для учетных записей пользователей. Здесь также применяется управление аутентификацией и авторизацией учетных записей пользователей. Контроль доступа имеет решающее значение для ограничения пользователей — как законных, так и злонамеренных — от ввода и компрометации конфиденциальных данных и систем. Управление паролями, многофакторная аутентификация и другие методы входят в сферу управления процессом IAM.

Организационное управление (governance) сосредоточено на разработке, внедрении и контроле соблюдения политик предотвращения, обнаружения и митигации кибер-угроз в облачных средах. Для малого и среднего бизнеса, а также для крупных корпоративных игроков такие аспекты, как информация об угрозах, могут помочь в отслеживании и приоритизации угроз для обеспечения тщательной защиты основных систем.

Тем не менее, даже отдельные облачные клиенты могут извлечь выгоду из политики безопасного поведения пользователей и обучения.

Планирование хранения данных и обеспечения непрерывности облачных сервисов включает технические меры аварийного восстановления в случае потери данных. Центральное место в любом плане аварийного восстановления занимают методы обеспечения резервного копирования данных. Кроме технических систем, для обеспечения бесперебойной работы могут помочь платформы для проверки работоспособности резервных копий и подробные инструкции по восстановлению рабочего режима для сотрудников, которые также важны для BCM*-планов облачных сред.

Соблюдение законодательства сконцентрировано вокруг защиты конфиденциальности данных пользователей, как это установлено соответствующими международными или национальными нормативными документами (152-ФЗ, GDPR, HIPAA и др.). Государственные органы подчеркивают важность защиты частной информации пользователей от ее несанкционированного использования в целях получения прибыли. Таким образом, компании, в зависимости от своей юрисдикции и регионов операционного присутствия, должны следовать тем или иным правилам, чтобы соблюдать эти политики. Одним из подходов является использование маскирования данных, которое исключает возможность идентификации данных по отношению к конкретному физическому лицу с помощью методов шифрования.

Специфические аспекты безопасности облачных вычислений, которые важно понимать ИТ-аудитору

Традиционные средства обеспечения безопасности информационных систем претерпели огромные изменения из-за перехода к облачным вычислениям. В то время как облачные модели обеспечивают большее удобство, наличие постоянного онлайн-подключения требует новых соображений для обеспечения их безопасности. Облачная безопасность как мо
решени
от устар
.....
*BCM (Bus
непрерыв

Продолжение статьи читайте в полной версии журнала, доступной членам Ассоциации «Институт внутренних аудиторов»

Институт внутренних аудиторов

ИВА www.iia-ru.ru
Telegram https://t.me/iiarus
YouTube
ЦОК ИВА http://cok.iia-ru.ru/
Тренинги ИВА www.iva-edu.ru
Национальная конференция ИВА www.iva-conf.ru
Национальная Премия ИВА www.iva-ag.ru

Ассоциация «Институт внутренних аудиторов» (Ассоциация «ИВА»), зарегистрированная в 2000 году, является профессиональным объединением 4000 внутренних аудиторов, внутренних контролеров и работников других контрольных подразделений российских компаний и организаций.