Инженерный вестник Дона, №7 (2024)
ivdon.ru/ru/magazine/archive/n7y2024/9390

Особенности обеспечения безопасности облачных систем

М.В. Шатурный

Финансовый университет при Правительстве Российской Федерации, Москва

Аннотация: В статье проведен анализ особенностей защиты современных облачных систем и распределения ответственности между взаимодействующими сторонами, предложены рекомендации повышению безопасности облачных ресурсов. На основании проведенного анализа предложены комплексные меры защиты и рекомендации по повышению безопасности облачных ресурсов, которые могут быть полезны специалистам по информационной безопасности и ИТ-специалистам для понимания особенностей защиты облачных систем, а также в выборе облачного провайдера и для подготовки к переходу в облако.
Ключевые слова: облачные вычисления, облачный провайдер, модель совместной ответственности, безопасность облачных ресурсов.

Введение

Мировой рынок облачных технологий год от года демонстрирует стабильный рост [1]. Это связано с увеличением объема обрабатываемых данных, а также с простотой масштабируемости, гибкостью и экономической эффективностью облачных решений по сравнению с построением локальной инфраструктуры внутри организации. Облачные технологии дают возможность делегировать провайдеру облачных услуг задачи по поддержке и обслуживанию инфраструктуры, что тем самым позволяет организациям сконцентрироваться на решении собственных бизнес – задач [2].

На сегодняшний день существует следующие основные подходы по использованию облачной инфраструктуры в организации:

- использование инфраструктуры исключительно одной организацией (частное облако);

- использование стандартной модели облачных ресурсов для развертывания собственных приложений и работе с данными (публичное облако);

- использование организацией одновременно частной облачной инфраструктуры и публичного облака (гибридное облако) [3].

Среди плюсов использования облачных технологий можно выделить: получение необходимых вычислительных мощностей без закупки и настройки дополнительного оборудования, быстрый запуск своего приложения, масштабируемость;

Помимо вычислительных мощностей, облако предлагает расширенные возможности по обеспечению безопасности ресурсов, что может существенно повысить эффективность защиты и снизить расходы для организаций, использующих локальную среду, за счет экономии на средствах защиты и содержании большого количества специалистов по информационной безопасности. Это наиболее актуально для среднего и малого бизнеса, стремящегося оптимизировать бюджет и в тоже время обеспечить безопасность своих ресурсов, и соответствовать требованиям законодательства. Однако, воспользоваться данными преимуществами организация может только в случае понимания возможностей и обязанностей провайдера по обеспечению безопасности облачных услуг и корректировке собственной инфраструктуры и политик безопасности, а также элементов управления в соответствии с ними.

Цель исследования – анализ особенностей обеспечения безопасности облачных систем с учетом, разделяемой между клиентом и провайдером ответственности и формулировка рекомендаций для организаций, планирующих переход в облако.

Модель совместной ответственности

При миграции систем и данных в облачную инфраструктуру между клиентом в лице организации и поставщиком в лице провайдера возникают совместные обязательства по обеспечению безопасности облачного ресурса, что является одной из основных особенностей облачных систем [4].

Зона ответственности зависит от выбранной клиентом услуги: IaaS, PaaS, SaaS.

IaaS (infrastructure as a service) – услуга по предоставлению клиенту вычислительных мощностей (сервера, хранилища, каналы связи).

PaaS (platform as a service) – услуга по предоставлению клиенту готовой платформы с уже настроенным программным обеспечением (операционная система, система управления базой данных, среда машинного обучения, среда разработки) и включающая весь перечень услуг IaaS.

SaaS (software as a service) – услуга, предоставляющая клиенту готовый программный продукт, разработанный для решения определенных задач (CRM системы, почтовые сервисы, конструкторы сайтов).

Разделяемая ответственность между клиентом и провайдером является главной особенностью использования облачных ресурсов. Обязательства по обеспечению безопасности конкретизируются в модели совместной ответственности.

Многие ведущие в отрасли провайдеры (AWS, Azure, Google Cloud Platform) публикуют ее на своих ресурсах. Она позволяет клиентам выбрать подходящее для них решение в зависимости от специфики бизнеса, обрабатываемой информации, возможностей собственной системы информационной безопасности и ИТ – зрелости организации [5;6]. В таблице 1 приведены основные аспекты этих моделей совместной ответственности.

Таблица 1

<table>
<tr><td rowspan="2">Зона ответственности</td><td colspan="3">Модель облачной услуги</td></tr>
<tr><td>IaaS</td><td>PaaS</td><td>SaaS</td></tr>
<tr><td>Данные</td><td colspan="3" rowspan="2">клиент</td></tr>
<tr><td>Управление доступом</td></tr>
<tr><td>Приложение</td><td colspan="2">клиент</td><td>облачный провайдер</td></tr>
<tr><td>Операционная система</td><td rowspan="2">клиент</td><td colspan="2" rowspan="2">облачный провайдер</td></tr>
<tr><td>Виртуальные сети</td></tr>
<tr><td>Средства виртуализации</td><td colspan="3" rowspan="2">облачный провайдер</td></tr>
<tr><td>Физическая инфраструктура (сети, сервера, хранилища)</td></tr>
</table>

По сути разделение ответственности за безопасность определяется наличием контроля над компонентом облачной инфраструктуры. Клиент для защиты системы в своей зоне ответственности может использовать как собственные локальные средства, так и доступные сервисы провайдера за дополнительную плату. В любом случае, вне зависимости от выбранной модели облачной услуги и дополнительного сервиса, невозможно полностью переложить ответственность за обеспечение безопасности своей системы в облаке на провайдера, ввиду сложности и специфичности многих процессов, например, управление доступом пользователей и управление правами на ресурсы.

Особенности обеспечения безопасности

Для защиты облачных систем в большинстве случаев используются те же методы и подходы, что и для локальных систем, но есть и некоторые различия, связанные с изменением характера риска, ролей и обязанностей.

Для эффективного предотвращения и минимизации угроз безопасности облачных систем следует использовать комплексный подход к защите. Среди компонентов комплексной безопасности выделяются следующие:

- Физическая безопасность. Заключается в совокупности средств и мер по контролю доступа к оборудованию и помещениям дата – центров провайдера, обеспечение отказоустойчивости и катастрофоустойчивости инфраструктуры. В случае с услугами в публичном облаке, ответственность за обеспечение безопасности физической инфраструктуры полностью ложится на провайдера.

- Безопасность инфраструктуры. Включает в себя самые низкие уровни безопасности. Это фундамент, на котором строится безопасность облачной платформы, включая безопасность вычислений, сети и хранилища. В связи с отсутствием возможности прямого управления инфраструктурой у клиента,

ответственность за обеспечение безопасности на этом уровне несет провайдер.

- Безопасность на уровне виртуализации. Безопасность виртуальной инфраструктуры по сравнению физической охватывает два дополнительных компонента: безопасность технологии виртуализации (гипервизора), средства управления безопасностью виртуальных ресурсов. Несанкционированный доступ к гипервизору создает риски получения доступа к виртуальным машинам и перехвату трафика [7]. Безопасность уровня виртуализации связана с особенностями виртуальной инфраструктуры: использование таких абстракций, как контейнеры (виртуальная среда выполнения с изолированным пространством пользователя), возможность информационного обмена в виртуальных сетях без прохождения трафика через реальную сеть. Ответственность за обеспечение безопасности уровня виртуализации будет зависеть от выбранной клиентом платформы, но в любом случае, провайдер несет ответственность за безопасность физической инфраструктуры и платформы виртуализации. Пользователь отвечает за настройку средств безопасности виртуальной инфраструктуры (виртуальная сеть и межсетевой экран, выделенный хостинг и т.д.).

- Безопасность на уровне управления (API). В этом заключается основное отличие облачных систем от «традиционной инфраструктуры», размещенной локально [8].

- Безопасность приложений. Состоит из сложного и многочисленного набора мер: от проектирования и моделирования угроз до тестирования, обслуживания и защиты. Модель совместной ответственности зависит от используемого сервиса. Вне зависимости от выбранной услуги, обеспечение безопасности приложения для клиента означает определенную зависимость от провайдера. При использовании IaaS, это может заключатся в отсутствии видимости сетевых журналов, при использовании PaaS, в отсутствии

видимости журналов сервера и служб и отсутствии контроля над балансировщиком нагрузки. Все особенности платформы провайдера и модели совместной ответственности необходимо учитывать при моделировании угроз на этапе разработки.

- Управление доступом. Облачные технологии оказывают большое влияние на управление идентификацией, авторизацией и правами доступа пользователей [9]. Главной особенностью IAM в облачных вычислениях являются отношения между провайдером и клиентом. Управление контролем доступа требует взаимодействия провайдера и клиента облачных услуг по вопросам распределения обязанностей в обеспечении его функционирования. Проблема взаимодействия усугубляется при распространении своего IAM организацией на нескольких облачных провайдеров. В зависимости от выбранного клиентом сервиса, провайдер отвечает за управление контролем доступа к соответствующей инфраструктуре.

- Безопасность данных. Является ключевым аспектом обеспечения безопасности облачных ресурсов. В связи с использованием виртуализации, облачное хранилище имеет особенности в типах хранения данных. Примерами могут служить хранилище объектов, хранилище экземпляров виртуальных машин. Основными методами защиты данных являются контроль доступа и шифрование. Главными требованиями к безопасности данных являются: конфиденциальность, целостность и доступность [10]. Ответственность за безопасность данных вне зависимости от используемого облачного сервиса несет клиент.

- Реагирование на инциденты. Особенностями реагирования на инциденты информационной безопасности при использовании облачных ресурсов является необходимость активного взаимодействия между клиентом и провайдером, точное распределение ролей и обязанностей, а также заранее оговоренные меры по совместному реагированию на инцидент

[11]. Отличием от реагирования на инциденты в «традиционной инфраструктуре» являются источники данных (журналы), многие из которых находятся в ведении провайдера. Помимо системных и сетевых журналов облачные платформы используют журналы API (для протоколирования вызовов API). Ответственность и обязанность сторон устанавливаются в договоре об оказании услуг.

- Соответствие требованиям законодательства. Соблюдение законодательства при использовании облачных вычислений – это общая ответственность и обязанность клиента и провайдера. При решении о миграции в облако, клиент должен оценить уровень защиты информации у поставщика облачных услуг и проверить наличие соответствующих сертификатов, аттестатов и оценок соответствия требованиям нормативно – правовым актам и стандартам.

В ходе исследования предложены следующие меры обеспечения безопасности облачных систем с учетом ответственности каждой из сторон, приведенные в таблице 2.

Таблица 2

Компонент безопасности облачных систем	Меры обеспечения безопасности со стороны провайдера	Меры обеспечения безопасности со стороны клиента	Рекомендации по обеспечению безопасности для клиента
1	2	3	4
Физическая безопасность	- контроль доступа в помещение дата – центра и его сегментированные структуры; - резервирование источников электропитания; - использование системы видеонаблюдения; - противопожарная безопасность		

1	2	3	4
Безопасность инфраструктуры	- физическая и логическая изоляция пользовательских ресурсов; - защита периметра сети облака; - обнаружение и предотвращение атак; - использование межсетевых экранов: - фильтрация нежелательного трафика; - использование списка IP адресов; - отключение неиспользуемых портов и протоколов; - использование средств антивирусной защиты; - использование средств AntiDDoS; - тестирование на проникновение		
Безопасность виртуализации	- изоляция вычислительных процессов клиентов; -поддержание безопасной инфраструктуры виртуализации от внешних атак и внутреннего неправомерного использования; - обеспечение защиты процессов запуска виртуальной машины пользователя из образа; - защита энергозависимой памяти от несанкционированного мониторинга; - сегрегация и изоляция	- безопасная настройка виртуализации с учетом рекомендаций провайдера; - управление идентификационными данными для доступа к виртуальной машине; - мониторинг и ведение журнала (состояние виртуальной машины); - управление образами (контейнер, виртуальная машина); - развертывание безопасной конфигурации образа	- использование выделенного хостинга, если он доступен, в зависимости от условий безопасности ресурса; - изоляция контейнеров, с помощью виртуальных или физических машин

1	2	3	4
	пользовательского сетевого трафика; - исключение отслеживания пакетов, утечек метаданных сетевой инфраструктуры; - использование межсетевых экранов; - уточнение в договоре об оказании услуг модификации сети и перехвата сетевого трафика клиентов - шифрование физического хранилища для исключения утечек при смене накопителя; - изоляция функции шифрование от функций управления данными; - удаление потенциально конфиденциальной информации при передаче экземпляра клиента обратно в гипервизор	виртуальной машины; - безопасная настройка используемой виртуальной сети, в том числе настройка виртуального межсетевого экрана при необходимости; - сегментация сетей с помощью виртуализации; - развертывание безопасного и проверенного образа контейнера; - использование строгой аутентификации и контроля доступа для управления контейнерами и репозиториями	
Безопасность на уровне управления (API)	- защита периметра шлюзов API и веб-консолей, включая защиту от атак на уровнях L3/L4, L7; - предоставление безопасной аутентификации (OAuth, подпись HTTP запросов); - использование исключительно многофакторной аутентификации при управлении облачными ресурсами; - мониторинг и журналирование процессов, связанных с управлением	- контроль учетных данных; - настройка безопасности уровня управления сервисом	- использование многофакторной аутентификации; - отдельный аккаунт для root и обычного администратора; - использование принципа минимальных привилегий

1	2	3	4
	облачными ресурсами; - предоставление доступа клиенту к настройке безопасности уровня управления сервисом		
Безопасность приложений	- использование межсетевого экрана уровня приложения; - защита API и веб – сервисов; - мониторинг необычной активности API; - тестирование сервиса	- моделирование угроз с учетом модели угроз провайдера; - использование практик безопасной разработки с учетом особенностей использования в облачной инфраструктуре; - настройка динамического тестирования с учетом работы в облаке; - оценка уязвимостей; - тестирование на проникновение с учетом ограничений и разрешений провайдера; - автоматизированное отслеживание изменений в приложении	- проверка вызовов API к облачному сервису и сохраненных учетных данных API при проведении статического анализа; - разграничение прав доступа для каждой службы приложения - изменение политики безопасности организации с учетом использования облачных ресурсов
Управление доступом	- обеспечение безопасной аутентификации пользователей; - обеспечение авторизации и контроля доступа; - поддержка детализированных атрибутов для обеспечения ABAC (доступ на основе атрибутов)	- определение и корректная настройка прав; - сопоставление атрибутов, включая роли и группы при использовании федеративной идентификации; - определение идентификационных данных и атрибутов;	- использование многофакторной аутентификации; - использование системы единого входа; - использование групп доступа; - использование брокера идентификации; - использование принципа минимальных привилегий;

1	2	3	4
		- мониторинг; - учет в плане реагирования на инциденты сценария захвата учетных записей пользователей, в том числе и привилегированных	- разработка матрицы прав доступа
Безопасность данных	- применение политики запрета доступа по умолчанию; - провайдер может предлагать инструменты по предотвращению утечки данных, мониторинга активности(базы данных), управление ключами шифрования	- контроль доступа (для пользователей и приложений); мониторинг изменения прав хранимые данные; - локальное резервное копирование; - мониторинг активности базы данных; - мониторинг активности файлов; - использование систем для предотвращения утечек данных; - защита данных при перемещении в облачное хранилище; - шифрование и управление ключами	- создание матрицы прав для контроля доступа; - использование разных вариантов шифрования (хранилища, базы данных, при передаче данных, резервной копии) на основе модели угроз и бизнес-процессов; - использование CASB (брокер безопасности облачного доступа)
Реагирование на инциденты	- информирование клиентов о типах, полноте и возможности предоставления регистрируемых на платформе облачных услуг событий, а также их формате для подготовки клиентами планов по реагированию на инциденты и, возможно, настройки собственных средств для мониторинга и	- создание плана реагирования на инциденты безопасности в своей организации; - отражение в договоре об оказании услуг вопросов, связанных с реагированием на инциденты с учетом всех этапов (анализ, локализацию,	- автоматизация некоторых процессов при возникновении оповещения (снимок хранилища виртуальной машины, захват метаданных) для обеспечения более эффективного расследования инцидента

1	2	3	4
	оповещения на уровне виртуальной машины или приложения; - описание в договоре об оказании услуг порядка взаимодействия с клиентом в случае возникновения инцидента, распределение ролей, обмен данными; - предоставление клиенту в рамках договора об оказании услуг информации для реагирования на инциденты	ликвидацию и восстановление); - оценка достаточности предоставляемых провайдером данных; - при необходимости использование средств мониторинга и оповещения	
Соответствие требованиям законодательства или иным стандартам безопасности	- проведения аттестации и аудитов и предоставление заказчикам данных о наличии: - аттестата ФСТЭК о соответствии требованиям для работы с персональными данными; - оценке соответствия ГОСТ Р 57580.1-2017; - сертификата соответствия требованиям PCI DSS; - аттестатов, сертификатов, аудиторских отчетов на соответствие требованиям других стандартов обеспечения безопасности облачных вычислений	- оценка поставщика облачных услуг при выборе платформы как минимум по критерию наличия документов, подтверждающих соблюдение требований законодательства или соответствия иным стандартам безопасности; - приведение в соответствие внутренней документации и средств защиты для соблюдения требований законодательства;	- проведение аудита собственных информационных систем

Для помощи организациям и облачным провайдерам в выборе мер защиты существуют стандарты обеспечения информационной безопасности в облаке:

- Cloud Security Aliance «Security guidance for critical areas of focus in cloud computing v4.0».
- Cloud Security Aliance «Cloud controls matrtix».
- NIST «Cloud computing security reference architecture».
- ГОСТ Р ИСО/МЭК 27001-2021.
- ГОСТ Р ИСО/МЭК 27018-2020.
- ГОСТ Р ИСО/МЭК 27017-2021.

Заключение

В работе были проанализированы особенности обеспечения безопасности облачных систем, главными из которых являются:

- разделение ответственности между клиентом и провайдером за безопасность облака;
- доступность инфраструктуры облачного провайдера;
- безопасность API – программного интерфейса приложения;
- управление безопасностью виртуальных ресурсов;
- безопасность передаваемых в облако данных;
- отсутствие прозрачности облачной инфраструктуру и меньший контроль для клиента;
- небезопасная конфигурация облачной инфраструктуры клиентом.

Для повышения эффективности защиты ресурсов клиента можно предложить следующие рекомендации:

- При выборе провайдера облачных услуг производить его проверку и оценку (доступная документация и политики, аудиторский отчет, сертификаты и аттестаты, подтверждающие соблюдение требований законодательства).
- Разработать матрицу обязанностей.
- Включить в модель угроз организации частную модель угроз облачного провайдера;

- Разработать план реагирования на инциденты с учетом взаимодействия с облачным провайдером;

- Разработать матрицу прав доступа к облачным ресурсам.

Литература

1. Саиткамолов М. С. У., Карабаев Р. З. Рационализация потребления ресурсов компании с помощью облачных технологий //ЭФО: Экономика. Финансы. Общество. – 2024. – №. 1 (9). – С. 73-80.

2. Фомин А. А., Фомина М. А. Цифровизация и облачные технологии: деньги на ветер или конкурентное преимущество для малого бизнеса //Московский экономический журнал. – 2020. – №. 9. – С. 249-254.

3. Немировская-Дутчак О. Э., Морозова Т. А., Кузнецова Е. А., Пронина Е. В. Обеспечение информационной безопасности при применении облачных технологий в производственных информационных системах //Международный журнал прикладных наук и технологий «Integral». – 2022. – №. 5. – С. 1805-1818.

4. National Institute of Standards and Technology, Special Publication 500-299 «Cloud Computing Security Reference Architecture». – 2013. – P. 88.

5. Разделение ответственности в облаке // learn.microsoft.com: статья 18.10.2023. URL: learn.microsoft.com/ru-ru/azure/security/fundamentals/shared-responsibility (дата обращения 10.05.2024).

6. Shared responsibilities and shared fate on Google Cloud // cloud.google.com: Cloud Architecture Center 21.08.2023. URL: cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate (дата обращения 10.05.2024).

7. Шанцов А. В. Особенности построения комплексной системы защиты информации облачных ресурсов. – 2021. – С. 103-106.

8. Джалалов М. Э. Стратегии управления версионностью API в микросервисной архитектуре //Экономика и качество систем связи. – 2024. – №. 1 (31). – С. 136-143.

9. Санников А. В., Бобичев Р. Е. Аспекты защиты информации в облачных системах электронного документооборота //Измерение, контроль, информатизация. – 2023. – С. 244-249.

10. Huang C-T, Huan L, Qin Z, Yuan H, Zhou L, Varadharajan V, Jay Kuo C.-C. Survey on securing data storage in the cloud. APSIPA Transactions on Signal and Information Processing, V. 3, 2014. – P. 175.

11. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing – 2021. – P. 101-107.

References

1. Saitkamolov M. S. U., Karabaev R.Z. E`FO: E`konomika. Finansy`. Obshhestvo. 2024. №. 1 (9). pp. 73-80.

2. Fomin A. A, Fomina M. A. Moskovskij e`konomicheskij zhurnal. 2020. №. 9. pp. 249-254.

3. Nemirovskaya-Dutchak O. E., Morozova T. A., Kuznetsova E. Y., Pronina E. V. Mezhdunarodny`j zhurnal prikladny`x nauk i texnologij «Integral». 2022. №. 5. pp 1805-1818.

4. National Institute of Standards and Technology, Special Publication 500-299 «Cloud Computing Security Reference Architecture». 2013. P. 88.

5. Razdelenie otvetstvennosti v oblake [Sharing responsibilities in the cloud]. URL: learn.microsoft.com/ru-ru/azure/security/fundamentals/shared-responsibility (accessed 10.05.2024).

6. Shared responsibilities and shared fate on Google Cloud. URL: cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate (accessed 10.05.2024).

7. Shanczov A. V. Osobennosti postroeniya kompleksnoj sistemy` zashhity` informacii oblachny`x resursov. [Features of building a comprehensive information protection system for cloud resources]. 2021. pp. 103-106.

8. Jalalov M. E. E`konomika i kachestvo sistem svyazi. 2024. №. 1 (31). pp. 136-143.

9. Sannikov A. V., Bobichev R. E. Izmerenie, kontrol`, informatizaciya. 2023. P. 244-249.

10. Huang C-T, Huan L, Qin Z, Yuan H, Zhou L, Varadharajan V, Jay Kuo C.-C. Survey on securing data storage in the cloud. APSIPA Transactions on Signal and Information Processing, V. 3, 2014. P. 175.

11. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing. 2021. pp. 101-107.

Дата поступления: 20.05.2024

Дата публикации: 11.07.2024