aws partner network | competency

AWS Competency: розничная торговля
Контрольный список проверки партнера-технолога

Декабрь 2019 г.
Версия 1.0

Содержание

Введение

Задача программы AWS Competency заключается в выявлении партнеров партнерской сети AWS («Партнеры APN»), которые подтвердили свой технический профессионализм и успешную работу с клиентами в сфере специализированных решений. Контрольный список проверки партнера в рамках программы AWS Competency («Контрольный список») предназначен для партнеров APN, которые хотят подать заявку на участие в программе AWS Competency. В контрольном списке приведены критерии для получения соответствующего статуса в программе AWS Competency. После подачи заявки по конкретной специализации программы Competency партнерам APN необходимо пройти аудит. Для проведения аудита AWS привлекает как собственных экспертов, так и сторонние компании. AWS оставляет за собой право вносить изменения в настоящий документ в любое время.

Ожидания сторон

Предполагается, что партнеры APN даже при соответствии всем требованиям внимательно изучат настоящий документ перед подачей заявки на участие в программе AWS Competency. Если содержимое настоящего документа неясно и требуется дальнейшее пояснение, свяжитесь сначала с представителем AWS по развитию партнеров (PDR) или менеджером AWS по развитию партнеров (PDM). При необходимости дальнейшей помощи ваш PDR или PDM обратится в офис программы.

Когда заявка будет готова к подаче, партнеры APN должны заполнить колонку самооценки в контрольном списке, который приведен в продолжении настоящего документа.

Для отправки заявки выполните следующие действия.

1. Авторизуйтесь на портале партнеров APN (https://partnercentral.awspartner.com/) в качестве главного специалиста Alliance.
2. Выберите «View My APN Account» в левой части страницы.
3. Перейдите к разделу «Program Details».
4. Выберите «Update» рядом с программой AWS Competency, на которую подается заявка.
5. Заполните заявку и нажмите «Submit».
6. Отправьте заполненную самооценку по адресу competency-checklist@amazon.com.
    - Самооценка должна включать следующее.
        - Категория решения (привлечение клиентов, корпоративный мерчандайзинг и планирование, цепочка поставок и дистрибуция, физические, цифровые и виртуальные магазины, расширенный анализ данных и основные бизнес-приложения для розничной торговли)
        - Тип развертывания (SaaS-решение или решение с самостоятельным развертыванием на AWS)
        - Документацию для примеров использования AWS (см. определения ниже)

Если у вас есть вопросы по этим инструкциям, обратитесь к своему представителю по развитию партнеров (PDR) или менеджеру по развитию партнеров (PDM).
AWS рассмотрит заявку и ответит в течение пяти рабочих дней, чтобы начать подготовку к планированию аудита или запросить дополнительную информацию.

Партнеры APN должны подготовиться к аудиту: прочитать контрольный список, выполнить самооценку с помощью контрольного списка, а также собрать и систематизировать фактические данные, чтобы предоставить их аудитору в назначенное время аудита.

AWS рекомендует, чтобы партнеры APN выделили на время аудита сотрудников, обладающих глубокими знаниями по требованиям аудита. Партнеру APN рекомендуется обеспечить доступность следующих сотрудников в ходе аудита: одного или несколько инженеров или архитекторов с большим техническим опытом, прошедших обучение и получивших сертификаты AWS; операционного менеджера, который отвечает за операции и поддержку; менеджера по развитию бизнеса для проведения обзорного доклада. До назначения даты аудита партнеры APN должны дать согласие на предоставление аудитору (AWS или другой стороне) всей информации, представленной в виде фактических данных или демонстраций.

Программа AWS Competency по розничной торговле

Партнеры-участники программы AWS Competency по розничной торговле предлагают решения для основных направлений бизнеса, таких как привлечение клиентов, корпоративный мерчандайзинг и планирование, цепочка поставок и дистрибуция, физические, цифровые и виртуальные магазины, расширенный анализ данных и основные бизнес-приложения для розничной торговли.

Категории программы Competency по розничной торговле

Партнеру APN также необходимо определить категорию сегмента для своего решения.

- **Привлечение клиентов:** лояльность, управление коммуникацией в социальных сетях, управление взаимоотношениями с клиентами (CRM), колл-центры, рассылка рекламных материалов (прямая и по электронной почте), поисковая оптимизация и решения по привлечению целевой аудитории, которые позволяют руководителям в сфере розничного маркетинга упреждающим образом привлекать и удерживать клиентов перед приобретением продукта и после него.

- **Корпоративный мерчандайзинг и планирование:** мерчандайзинг, пополнение запасов и планирование ассортимента продукции, составление планограммы и плана расстановки, продвижение продукции и ценовая оптимизация, управление ассортиментом товара и решения для сотрудничества с поставщиками, которые используются группами планирования и корпоративного мерчандайзинга.

- **Цепочка поставок и дистрибуции:** решения для работы с цепочкой поставок и дистрибуцией, которые можно использовать в системах управления складом (WMS), планировании ресурсов предприятия (ERP), автоматизации работы склада, процессах импорта-экспорта, транспортных услугах и логистике.

- **Физические, цифровые и виртуальные магазины:** решения для преобразования процесса покупок в физических и виртуальных магазинах, предназначенные для таких его аспектов, как торговое оборудование, системы управления заказами (OMS), единая система коммерции и интернет-коммерция, осуществление последнего этапа доставки, обеспечение процесса покупок без задержек, цифровые инновации (дополненная и виртуальная реальность, электронные ценники, Интернет вещей, маячки, голосовые функции, функции распознавания, цифровые киоски, умные зеркала, интерактивные дисплеи), системы управления электронными ресурсами (DAM) и выставление счетов.

- **Расширенный анализ данных по розничной торговле:** озеро данных по розничной торговле, аналитические решения и решения с использованием искусственного интеллекта и машинного обучения, которые делают работу более эффективной, а также повышают качество привлечения клиентов и аналитики по ним.

- **Основные бизнес-приложения для розничной торговли:** основные решения корпоративного уровня для розничной торговли, предназначенные для топ-менеджеров, управления персоналом и кадрами, ведения закупок и юридической деятельности, информационных технологий, а также сферы финансов.

Партнеры APN также должны указать категорию поставки своего решения.

1. **SaaS-решение:** обслуживает нескольких клиентов с единой инфраструктурой AWS. Все аккаунты AWS находятся под управлением партнера APN.

2. **Развертывание клиентом:** развертывание выполняется в принадлежащей клиенту среде AWS Все аккаунты AWS управляются клиентом

Требования для участия в программе AWS Competency по розничной торговле

Ниже приведены параметры, которые будут оцениваться менеджером программы AWS Competency. Прежде чем назначать время технологической проверки, необходимо собрать всю недостающую информацию.

1.0. Участие в программах APN		**Соответствие: да / нет**
1.1. Уровень партнера-технолога	Перед подачей заявки на участие в программе Competency по розничной торговле партнеру APN необходимо прочитать руководство по программе и соответствующие определения. Нажмите здесь, чтобы просмотреть подробные сведения о программе.	
1.2. Уровень партнера-технолога	Прежде чем подать заявку на участие в программе AWS Competency по розничной торговле, партнер APN должен получить статус опытного партнера-технолога APN.	
1.3. Категория решения	Партнер APN должен определить свое решение в ту или иную категорию сегмента. ☐ **Привлечение клиентов** ☐ **Корпоративный мерчандайзинг и планирование** ☐ **Цепочка поставок и дистрибуция** ☐ **Физические, цифровые и виртуальные магазины** ☐ **Расширенный анализ данных по розничной торговле** ☐ **Аналитика и основные бизнес-приложения для розничной торговли** Партнер APN должен определить свое решение в ту или иную категорию поставки. ☐ **SaaS-решение** ☐ **Развертывание клиентом**	
1.4. Внедрение клиентом	Партнер APN должен указать, сколько всего клиентов использует его решение.	
2.0. Примеры использования		**Соответствие: да / нет**
2.1. Примеры использования в сфере розничной торговли	Партнер APN должен представить четыре примера использования, связанных с одним рассматриваемым решением для розничной торговли. Каждый из четырех примеров использования должен содержать пример решения партнера APN и информацию о его использовании в одной из шести категорий сегмента (привлечение клиентов, корпоративный мерчандайзинг и планирование, цепочка поставок и дистрибуция, физические, цифровые и виртуальные магазины, расширенный анализ данных и основные бизнес-приложения для розничной торговли). Партнеры APN, которые являются участниками программ AWS Competency по обслуживанию клиентов в цифровых каналах (DCX), данным и аналитике, Интернету вещей, миграции и (или) машинному обучению, могут повторно предоставить до четырех примеров использования клиентами с тем условием, что они относятся к проектам с узкоспециальными решениями для конкретных отраслевых задач и оказания консультационных услуг с использованием уникальных отраслевых знаний в сфере розничной торговли. Для каждого примера использования партнер APN должен предоставить следующую информацию. ▪ Имя клиента ▪ Веб-сайт клиента ▪ Проблема клиента ▪ Каким образом было выполнено развертывание решения для устранения проблемы ▪ Использованные приложения или решения сторонних разработчиков ▪ Дата начала эксплуатации ▪ Итоги / результаты ▪ Конкретные схемы архитектур, руководства по развертыванию и другие материалы в зависимости от типа решения, как описано в следующем разделе	

	Эта информация будет запрошена в рамках процесса подачи заявки на участие в программе на портале партнеров APN. Информация, предоставленная в составе этого примера использования, может быть частной и не подлежать разглашению. Все четыре представленных примера использования будут оцениваться на этапе изучения документации в ходе технической проверки. Если партнер APN не сможет представить документацию, необходимую для оценки примера использования по каждому пункту контрольного списка, или какие-либо требования контрольного списка не будут удовлетворены, пример использования будет снят с рассмотрения на участие в программе Competency. Примеры использования должны содержать описания развертываний, выполненных в течение последних 18 месяцев. Кроме того, они должны представлять собой проекты, используемые клиентами в рабочей среде, а не «пилотные» проекты или опытные образцы.	
2.2. Публичные примеры использования	Публичные примеры использования применяются AWS после принятия партнера APN в программу Competency для того, чтобы продемонстрировать успех его решения с помощью измеримых показателей KPI и убедить клиентов в том, что партнер APN обладает надлежащим опытом и знаниями для разработки и предоставления решений, отвечающих поставленным целям. Партнер APN должен представить два из четырех клиентских развертываний, связанных с определенными примерами использования, в качестве публичных примеров использования. Эти публичные примеры использования могут представлять собой формальные примеры использования, технические описания или публикации в блогах.	
	Публичные примеры использования должны быть доступны на веб-сайте партнера APN, т. е. должна существовать возможность перехода к таким примерам использования с главной страницы партнера APN. Партнер APN должен предоставить ссылки на эти публичные примеры использования в своей заявке.	
	Публичные примеры использования должны содержать следующую информацию. ▪ Упоминания имени клиента, имени партнера APN и AWS ▪ Проблема клиента ▪ Каким образом было выполнено развертывание решения для устранения проблемы ▪ Каким образом сервисы AWS использовались при создании решения ▪ Итоги / результаты	
3.0. Присутствие в Интернете и позиционирование участника программы AWS как эксперта в сфере розничной торговли		**Соответствие: да / нет**
3.1. Целевая страница партнера APN по теме AWS	Присутствие партнера APN в Интернете, связанное с его решениями AWS для розничной торговли, является для клиентов подтверждением его возможностей и опыта. У партнера APN должна быть целевая страница по теме AWS, содержащая описание его решения в сфере розничной торговли на AWS, ссылки на публичные примеры использования, список партнеров-технологов и любую другую значимую информацию, которая демонстрирует опыт партнера APN в розничной торговле и подчеркивает его сотрудничество с AWS. Эта страница, посвященная розничной торговле на AWS, должна быть доступна с главной страницы партнера APN. Использовать саму домашнюю страницу в качестве целевой страницы AWS нельзя. Исключение представляет собой ситуация, когда партнер APN – компания, специализирующаяся на технологиях в сфере розничной торговли, и домашняя страница это отражает.	
3.2. Экспертное позиционирование в сфере розничной торговли	Предполагается, что партнеры программы AWS Competency со специализацией в сфере розничной торговли обладают экспертными знаниями в этой сфере и разработали инновационные решения, которые включают в себя сервисы AWS.	

	Партнеры APN должны предоставить публичные материалы (например, публикации в блогах, печатные статьи, видеоролики и т. д.), демонстрирующие специализацию партнера APN на розничной торговле и опыт работы в данной сфере. Необходимо предоставить ссылки на примеры материалов, опубликованных в течение последних 12 месяцев.	
4.0. Требования к бизнесу		
4.1. Инструментарии, готовые к применению	Партнер APN должен предоставить документацию и инструментарии продавца, в том числе четкое предложение продукта с описанием его преимуществ, которое можно изложить службе продаж AWS, вместе со всей значимой информацией, необходимой, чтобы определить возможность заинтересовать потенциального клиента (например, с рекламно-информационными материалами, презентацией и примерами использования клиентами). Доказательство должно быть представлено в форме рекламно-информационных материалов, включающих презентацию, одностраничную рекламу и контрольный список примеров использования.	
4.2. Поддержка продукта / служба технической поддержки	Партнер APN осуществляет поддержку клиентов через веб-чат, телефон или электронную почту. Подтверждение этого факта следует представить в виде описания поддержки, доступной клиентам по продуктам или решениям партнера.	
4.3. Размещение продукта в AWS Marketplace	Партнер APN предоставляет решение через AWS Marketplace. ☐ Да ☐ Нет Если да, партнер APN должен предоставить ссылку на AWS Marketplace. Если нет, дополнительной информации не требуется.	
4.4. Вознаграждение за продажи совместно с AWS	Партнер APN применяет для сотрудников своего отдела продаж планы вознаграждения за продажи, совершенные совместно с AWS. ☐ Да ☐ Нет ☐ Пояснение: _____ Доказательство должно быть представлено в форме краткого описания плана вознаграждения для сотрудников отдела продаж партнера APN.	
4.5. Заключение сделок совместными усилиями AWS и партнера APN	Партнер APN документально оформляет и публично освещает примеры заключения сделок совместными усилиями. Доказательство должно быть представлено в форме устного описания такого процесса.	
5.0. Самооценка партнера APN		**Соответствие: да / нет**
5.1. Контрольный список самооценки для партнерской программы AWS Competency	Партнер APN должен самостоятельно провести оценку своего соответствия требованиям контрольного списка для партнеров, занимающихся развитием технологий в сфере розничной торговли на AWS. ▪ Партнер APN должен заполнить все разделы контрольного списка. ▪ Заполненную самооценку необходимо отправить по адресу **competency-checklist@amazon.com**. Поле темы необходимо заполнить следующим образом: «[Имя партнера APN], Retail Competency Technology Partner Completed Self-Assessment». ▪ Перед отправкой заполненной самооценки в AWS партнеру APN рекомендуется обратиться к своему архитектору партнерских решений, представителю по развитию партнеров (PDR) или менеджеру по развитию партнеров (PDM) для предварительной проверки заявки. Эта рекомендация объясняется тем, что специалисты AWS, работающие с партнером APN, должны участвовать в процессе и предоставлять рекомендации еще до проверки. Кроме того, это повышает эффективность дальнейшей проверки.	

Программа Competency по розничной торговле: контрольный список для проверки партнера-технолога

Следующие пункты будут проверяться сторонними аудиторами и (или) архитекторами партнерских решений AWS. Недостающую информацию следует предоставить до планирования технической проверки.

Техническая проверка		Область действия		
		SaaS-решение	Развертывание клиентом на AWS	Соответствие: да / нет
Схема архитектуры	В зависимости от категории развертывания требуется одна или несколько схем архитектуры. На каждой схеме архитектуры должно быть показано следующее. ☐ Основные элементы архитектуры, а также то, как они сочетаются для предоставления партнерского решения клиентам ☐ Все задействованные сервисы AWS (с использованием соответствующих значков сервисов AWS). ☐ Способ развертывания сервисов AWS, включая информацию об Amazon Private Virtual Cloud (VPC), зонах доступности, подсетях и подключениях к системам за пределами AWS. ☐ Сюда же входят элементы, развертывание которых выполнено за пределами AWS, например локальные компоненты или аппаратные устройства.	Да – для решения в целом и для каждого примера использования.	Да – для каждого примера использования.	
Руководство по развертыванию	Руководство по развертыванию должно предоставлять рекомендации по развертыванию партнерского решения на AWS и включать все разделы, перечисленные в документе Baseline Requirements for Deployment Guides.	Нет	Да – одно для решения	
Заполненный контрольный список проверки	Для каждого из четырех примеров использования, представленных для партнерского решения, партнеру APN необходимо предоставить заполненный контрольный список, образец которого приведен ниже.	Да	Да	
1.0. Безопасность **Основополагающие элементы безопасности – защита информации и систем. К основным аспектам относятся конфиденциальность и целостность данных, определение возможностей пользователей и управление ими посредством привилегий, защита систем, а также установка элементов управления для обнаружения событий безопасности.**				
1.1. Пользователь root учетной записи AWS не используется для стандартных действий	Пользователя root учетной записи AWS запрещено использовать для выполнения стандартных действий. Сразу после создания учетной записи AWS необходимо создать учетные записи пользователей AWS Identity and Access Management (IAM), а затем использовать их для выполнения всех стандартных действий. После создания пользователей IAM необходимо в надежном месте сохранить данные пользователя root и использовать их только для выполнения отдельных задач, связанных с управлением аккаунтом и сервисами AWS, для которых это необходимо. Подробнее о том, как настраивать	Да	Нет	

	аккаунты и группы пользователей IAM для ежедневного использования, см. в разделе Creating Your First IAM Admin User and Group.			
1.2. Для пользователя root учетной записи AWS включена возможность Multi-Factor Authentication (MFA)	Для пользователя root учетной записи AWS необходимо включить возможность Multi-Factor Authentication (MFA). Поскольку пользователь root учетной записи AWS может выполнять конфиденциальные операции, дополнительный уровень аутентификации позволит надежнее защитить учетную запись. Доступно несколько типов MFA, в том числе виртуальная MFA и аппаратная MFA.	Да	Нет	
1.3. Для всех стандартных действий используются учетные записи пользователей IAM	Запрещается использовать пользователя root учетной записи AWS для выполнения задач, которые этого не требуют. Вместо этого создайте новых пользователей IAM для всех лиц, которым требуется доступ от имени администратора. Затем сделайте этих пользователей администраторами. Для этого поместите их в группу администраторов, к которой необходимо прикрепить управляемую политику AdministratorAccess. Пользователи, находящиеся в группе администраторов, должны настраивать группы, пользователей и т. д. для аккаунта AWS. Все последующие взаимодействия необходимо осуществлять через пользователей учетной записи AWS и их собственные ключи, а не через пользователя root. Однако для выполнения некоторых задач по управлению учетной записью и сервисами необходимо входить в систему с использованием учетных данных пользователя root.	Да	Нет	
1.4. Для всех интерактивных пользователей IAM включена возможность Multi-Factor Authentication (MFA)	Необходимо включить возможность Multi-Factor Authentication (MFA) для всех интерактивных пользователей IAM. Когда включена возможность MFA, у пользователей есть устройство, генерирующее уникальный код аутентификации (одноразовый пароль, или OTP). Пользователи должны предоставить как стандартные учетные данные (имя пользователя и пароль), так и OTP. В качестве устройства MFA может использоваться либо аппаратное обеспечение, либо виртуальное устройство (например, его можно запускать в приложении на смартфоне).	Да	Нет	
1.5. Выполняется регулярная ротация учетных данных IAM	Необходимо регулярно менять пароли и ключи доступа, а также следить за тем, чтобы это делали и другие пользователи IAM в вашей учетной записи. Таким образом, если пароль или ключ доступа будет скомпрометирован без вашего ведома, вы ограничите время, в течение которого можно получить доступ к ресурсам с использованием этих учетных данных. К учетной записи можно применить политику паролей, которая требует ротации паролей от всех пользователей IAM. Можно также выбрать частоту, с которой они должны это делать. Подробнее о ротации ключей доступа для пользователей IAM см. в разделе Rotating Access Keys.	Да	Нет	

1.6. Для пользователей IAM действует политика надежных паролей	Для пользователей IAM необходимо настроить политику надежных паролей. Если пользователям разрешено менять пароли самостоятельно, необходимо требовать, чтобы они создавали надежные пароли и выполняли их ротацию через определенные промежутки времени. Создать политику паролей для своей учетной записи можно на странице настроек учетной записи в консоли IAM. Политику паролей можно использовать для определения требований к паролям, таких как минимальная длина, необходимость использования небуквенных символов, частота ротации и т. д. Подробнее см. в разделе Setting an Account Password Policy for IAM Users.	Да	Нет	
1.7. Одни и те же данные для доступа IAM не используются для разных пользователей	Для каждого лица, которому требуется доступ к вашей учетной записи AWS, необходимо создать отдельную учетную запись пользователя IAM. Создайте пользователя IAM также и для себя, наделите его правами администратора и выполняйте всю работу от его имени. При создании отдельных пользователей IAM для лиц, которым требуется доступ к вашей учетной записи, каждому из них можно назначить уникальный набор учетных данных для доступа. Кроме того, всем пользователям IAM можно предоставлять различные разрешения. При необходимости в любой момент можно изменить или отменить разрешения пользователя IAM. (Если вы выдаете учетные данные пользователя root, отозвать их трудно. Кроме того, невозможно ограничить разрешения.)	Да	Нет	
1.8. Действие политик IAM подчиняется принципу минимальных привилегий	Необходимо следовать стандартной рекомендации по безопасности, суть которой заключается в предоставлении минимальных привилегий. Иными словами, даются только разрешения, необходимые для выполнения задачи. Определите, что должны сделать пользователи, и создайте для них политики, которые позволят им выполнить только эти задачи. Начните с минимального набора разрешений и по мере необходимости давайте дополнительные. Такой принцип работы безопаснее ситуации, когда приходится ужесточать изначально нестрогие разрешения. Чтобы задать надлежащий набор разрешений, необходимо провести небольшое исследование. Определите, что требуется для решения определенной задачи, какие действия поддерживает конкретный сервис и какие разрешения необходимы для выполнения этих действий.	Да	Нет	
1.9. Данные для доступа (например, ключи доступа) не прописаны в исходном коде	Необходимо следовать рекомендациям по управлению ключами доступа AWS и не прописывать учетные данные в исходном коде. При программном доступе к AWS ключ доступа используется для подтверждения личности и удостоверения приложений. Любое лицо, у которого имеется ваш ключ доступа, обладает тем же уровнем доступа к вашим ресурсам AWS, что и вы. Поэтому AWS делает все возможное для	Да	Да	

	защиты ваших ключей доступа, и, в соответствии с нашей моделью общей ответственности, вам следует поступать так же.			
1.10. Все данные для доступа зашифрованы при хранении	Главное требование – обеспечить шифрование всех хранимых данных для доступа.	Да	Да	
1.11. Ключи доступа AWS используются только интерактивными пользователями	Использование ключей доступа AWS допускается только в следующих случаях. 1. Ключи используются людьми для доступа к сервисам AWS и надежно хранятся на устройстве, которое находится под управлением конкретного человека. 2. Используется сервисом для доступа к сервисам AWS, но только в случаях, когда: a) нецелесообразно использовать роль инстанса Amazon EC2, роль задания Amazon Elastic Container Service (Amazon ECS) или аналогичный механизм, b) ключи доступа AWS изменяются не реже раза в неделю и c) политика IAM подчиняется жестким принципам, в результате чего: i) разрешает доступ только к конкретным методам и целям и ii) запрещает доступ к подсетям, из которых осуществляется доступ к ресурсам.	Да	Да	
1.12. Сервис AWS CloudTrail включен для всех учетных записей AWS во всех регионах	Необходимо включить сервис AWS CloudTrail для всех учетных записей AWS во всех регионах. Прозрачность действий в вашей учетной записи AWS – это принципиально важный аспект безопасности и одна из эксплуатационных рекомендаций. Сервис AWS CloudTrail можно использовать для просмотра, поиска, скачивания, архивирования, анализа действий в учетной записи в пределах инфраструктуры AWS, а также для реагирования на них. Вы можете определить, кем или чем выполнено определенное действие, какие ресурсы использовались, когда произошло событие, а также получить другие сведения, которые помогут при анализе и реагировании на активность в учетной записи AWS.	Да	Нет	
1.13. Журналы CloudTrail хранятся в корзине S3, принадлежащей другому аккаунту AWS	Журналы AWS CloudTrail необходимо помещать в корзину, принадлежащую другой учетной записи AWS, доступ к которой строго ограничен и предоставляется только для аудита и восстановления.	Да	Нет	
1.14. Для корзины S3 с журналами CloudTrail включено управление версиями или возможность MFA Delete	Корзину с журналами AWS CloudTrail необходимо защитить с помощью управления версиями или возможности MFA Delete.	Да	Нет	
1.15. Группы безопасности Amazon EC2 строго ограничены	Все группы безопасности Amazon EC2 должны ограничивать доступ в наибольшей возможной степени. Это подразумевает по меньшей мере следующее. 1. Внедрение групп безопасности для ограничения трафика между Интернетом и Amazon VPC. 2. Внедрение групп безопасности для ограничения трафика в пределах Amazon VPC. 3. Использование максимально возможных ограничений во всех случаях.	Да	Да	

1.16. Для корзин Amazon S3 в пределах вашей учетной записи установлены надлежащие уровни доступа	Необходимо внедрить надлежащие средства управления для контроля доступа к каждой корзине Amazon S3. При использовании AWS рекомендуется предоставлять доступ к ресурсам только тем лицам, которые не могут без них обойтись (принцип минимальных привилегий).	Да	Да	
1.17. Корзины Amazon S3 настроены надлежащим образом и не открыты для всеобщего доступа.	Корзины, которые не должны находиться в открытом доступе, необходимо настроить надлежащим образом, чтобы закрыть к ним публичный доступ. По умолчанию все корзины Amazon S3 являются частными и доступны только тем пользователям, которым явно предоставлен доступ. В большинстве примеров использования широкий публичный доступ для чтения файлов в корзинах Amazon S3 не требуется. Рекомендуется никогда не предоставлять общий доступ. Исключение составляет ситуация, когда Amazon S3 используется для размещения публичных ресурсов (например, изображений для использования на публичном веб-сайте).	Да	Да	
1.18. Имеется механизм мониторинга, позволяющий определять, когда корзины или объекты S3 становятся публичными	Необходимо применять механизм мониторинга или предупреждения, позволяющий определять, когда корзины Amazon S3 становятся публичными. С этой целью можно использовать, например, сервис AWS Trusted Advisor. AWS Trusted Advisor проверяет в Amazon S3 корзины, для которых имеются разрешения на открытый доступ. Разрешения для корзин, предоставляющие доступ на выполнение запроса List абсолютно всем, могут привести к непредвиденному росту затрат, если непредусмотренные пользователи с большой частотой просматривают список объектов в корзине. Разрешения для корзин, которые предоставляют доступ на загрузку / удаление объектов абсолютно всем, создают потенциальные уязвимости безопасности, поскольку позволяют всем добавлять, изменять или удалять объекты, находящиеся в корзине. При проверке Trusted Advisor изучаются явные разрешения для корзины и связанные с ними политики корзины, которые могут переопределить разрешения.	Да	Нет	
1.19. Для обнаружения изменений в инстансах и контейнерах Amazon EC2 применяется механизм мониторинга	Любые изменения в используемых инстансах или контейнерах Amazon S3 могут свидетельствовать о несанкционированных операциях. Их необходимо как минимум записывать в журналы, находящиеся в надежном месте, чтобы впоследствии можно было провести расследование. Механизм, применяемый для этой цели, должен по крайней мере: (1) обнаруживать все изменения в ОС или файлах приложений в инстансах или контейнерах Amazon S3, используемых в решении; (2) хранить данные об этих изменениях в надежном месте, находящемся за пределами инстанса или контейнера Amazon S3. К примерам подходящих механизмов относятся: (a) развертывание проверки целостности файлов	Да	Нет	

	через плановое управление конфигурацией (например, Chef, Puppet и т. д.) или специализированный инструмент (например, OSSEC, Tripwire или аналогичный инструмент); или (б) расширение инструментов для управления конфигурацией с целью проверки конфигурации хоста Amazon S3 и отправки уведомлений об обновлениях в конфигурационных файлах ключей или пакетах с использованием событий Canary (зарегистрированных инструкций no-op), настроенных таким образом, чтобы при выполнении обеспечить работоспособность сервиса на всех хостах в области видимости; или (с) развертывание системы обнаружения вторжения на хост, например решения с открытым исходным кодом, такого как OSSEC с ElasticSearch и Kibana, или решения партнера. Обратите внимание, что следующий механизм не отвечает этому требованию: (a) часто осуществляемые циклические изменения в инстансах или контейнерах Amazon S3.			
1.20. Все данные классифицированы по уровню конфиденциальности	Все данные клиентов, обработанные и хранящиеся в рабочей нагрузке, рассматриваются и классифицируются с целью определить уровень их конфиденциальности и методы, подходящие для работы с ними.	Да	Да	
1.21. Все конфиденциальные данные зашифрованы	Все данные клиентов, классифицированные как конфиденциальные, зашифровываются при передаче и хранении.	Да	Да	
1.22. Все криптографические ключи находятся под надежным управлением	Все криптографические ключи зашифровываются при хранении и передаче, а доступ к ним для использования контролируется с помощью решения AWS, такого как AWS Key Management Service (KMS), или партнерского решения, такого как HashiCorp Vault.	Да	Да	
1.23. Все передаваемые данные зашифрованы	Все данные, передаваемые в пределах Amazon Virtual Private Cloud, зашифрованы.	Да	Да	
1.24. Процедура реагирования на инциденты, связанные с компьютерной безопасностью, определена и отработана	Должна быть определена процедура реагирования на инциденты, связанные с компьютерной безопасностью, для управления такими инцидентами, как несанкционированный доступ к учетной записи AWS. Эту процедуру необходимо протестировать путем внедрения мер отработки процедуры реагирования на инциденты, например провести игровой день информационной безопасности. Репетиция должна быть проведена в течение последних 12 месяцев. Это необходимо для того, чтобы подтвердить следующее: a) у соответствующих лиц имеется доступ к рабочей среде; b) соответствующие инструменты доступны; c) соответствующие лица знают, как реагировать на различные инциденты компьютерной безопасности, перечисленные в плане.	Да	Нет	

1.25. Стандарт PCI DSS – сертификация или вопросник самооценки	Для приложений интернет-коммерции, единой системы коммерции и торгового оборудования, в которых хранятся данные держателей платежных карт, предусмотрена процедура ежегодной оценки рабочей нагрузки на необходимость соответствия стандарту PCI DSS. По результатам этой проверки при необходимости проводится сертификация на соответствие стандарту PCI DSS или заполнение вопросника самооценки. Подтверждение должно быть представлено в форме отчета о соответствии стандарту PCI DSS или заполненного вопросника самооценки (SAQ).	Да	Да	
1.26. Сквозное шифрование данных PCI	Для приложений интернет-коммерции, единой системы коммерции и торгового оборудования, в которых хранятся данные держателей платежных карт, передаваемые данные шифруются, в том числе в пределах Amazon VPC.	Да	Да	
1.27. Защита от DDoS-атак	Предоставляются инфраструктура и сервисы, которые смягчают последствия DDoS-атак на всех уровнях сетевой модели OSI.	Да	Нет	
1.28. Механизмы для смягчения последствий 10 сильнейших атак проекта Open Web Application Security Project (OWASP)	Предоставляются инфраструктуру и сервисы, которые смягчают последствия уязвимостей, найденных проектом Open Web Application Security Project (OWASP).	Да	Нет	
2.0. Надежность Основополагающий элемент надежности – способность предотвращать сбои и быстро восстанавливаться после них для удовлетворения спроса со стороны бизнеса и клиентов. К основным аспектам относятся базовые элементы, связанные с настройкой, межпроектные требования, планирование восстановления и работа с изменениями.				
2.1. Имеется высокодоступное сетевое подключение	Сетевое подключение к решению должно быть высокодоступным. При использовании VPN или AWS Direct Connect для подключения к сетям клиентов решение должно поддерживать резервные соединения, даже если клиенты внедряют их не всегда.	Да	Да	
2.2. Механизмы масштабирования инфраструктуры соответствуют бизнес-требованиям	Механизмы масштабирования инфраструктуры должны соответствовать бизнес-требованиям, что достигается одним из следующих способов. 1. Внедрение механизмов автомасштабирования на каждом уровне архитектуры. 2. Подтверждение, что для удовлетворения текущих бизнес-требований, в том числе потребностей в расходах и ожидаемого роста количества пользователей, не нужны механизмы автомасштабирования, Процедуры масштабирования вручную полностью задокументированы и регулярно тестируются.	Да	Да	
2.3. Осуществляется централизованное управление журналами AWS и приложений	Все содержимое журналов приложений и инфраструктуры AWS следует объединять в одну систему.	Да	Нет	
2.4. Осуществляется централизованное управление мониторингом AWS и	Управление инфраструктурой приложения и AWS необходимо осуществлять централизованно, а сформированные уведомления отправлять соответствующему	Да	Нет	

приложений, а также уведомлениями	персоналу, занимающемуся вопросами операционной деятельности.			
2.5. Выделение инфраструктуры и управление ею автоматизировано	Для выделения инфраструктуры AWS и управления ею решение должно использовать автоматизированный инструмент, такой как AWS CloudFormation или Terraform. Не следует использовать консоль AWS для внесения рутинных изменений в рабочую инфраструктуру AWS.	Да	Да	
2.6. Резервное копирование данных выполняется регулярно	Необходимо регулярно выполнять резервное копирование данных в надежную службу хранения. Резервные копии позволяют выполнить восстановление после административных, логических или физических сбоев. Для резервного копирования и архивирования в идеале следует использовать сервисы Amazon S3 и Amazon Glacier. Оба сервиса представляют собой надежные экономичные платформы хранения. Оба сервиса предлагают неограниченную емкость и не требуют управления объемом или носителями данных по мере роста резервных наборов данных. Благодаря применению модели оплаты по факту использования и низкой стоимости гигабайт-месяца эти сервисы прекрасно подходят для сценариев использования, связанных с защитой данных.	Да	Да	
2.7. Тестирование механизмов восстановления осуществляется регулярно, а также после значительных изменений в архитектуре	Тестировать механизмы и процедуры восстановления необходимо как периодически, так и после внесения значительных изменений в облачную среду. AWS предоставляет значительные ресурсы для управления резервным копированием и восстановлением данных.	Да	Нет	
2.8. Решение устойчиво к прерыванию работы зоны доступности	Решение должно продолжать функционировать в случае, если работа всех сервисов в пределах одной зоны доступности прерывается.	Да	Да	
2.9. Проверена отказоустойчивость решения	Устойчивость инфраструктуры к прерыванию работы одной зоны доступности проверена в реальных условиях, например в рамках игрового дня, не ранее, чем 12 месяцев назад.	Да	Нет	
2.10. Разработан план аварийного восстановления	Строго определенный план аварийного восстановления включает целевую точку восстановления (RPO) и целевое время восстановления (RTO). Необходимо определить RPO и RTO для всех включенных сервисов. RPO и RTO должны соответствовать соглашению об уровне обслуживания, которое вы предлагаете клиентам.	Да	Да	
2.11. Целевое время восстановления (RTO) не превышает 24 часов	Основополагающее требование заключается в том, чтобы RTO базовых сервисов не превышало 24 часов.	Да	Нет	
2.12. План аварийного восстановления надлежащим образом проверен	План аварийного восстановления необходимо проверять на соответствие целевой точке восстановления (RPO) и целевому времени восстановления (RTO) как регулярно, так и после крупных обновлений. До одобрения вашей заявки на присвоение статуса опытного	Да	Нет	

	партнера APN необходимо провести по крайней мере одну проверку аварийного восстановления.			
2.13. План аварийного восстановления включает восстановление в другом регионе	План аварийного восстановления должен включать стратегию восстановления в другом регионе AWS, а при проведении периодического тестирования необходимо проверять этот сценарий. В течение последних 12 месяцев должно быть проведено как минимум одно полное тестирование плана аварийного восстановления, включая по крайней мере восстановление в другом регионе AWS. Примечание. Несмотря на то что восстановление данных в тестовые среды или экспортирование данных для пользователей может использоваться для проверки резервного копирования, эти процедуры не соответствуют требованию по тестированию полного восстановления в другом регионе AWS.	Да	Нет	
3.0. Оптимизация бизнес-процессов Основополагающие элементы оптимизации бизнес-процессов – эксплуатация и мониторинг систем в целях повышения ценности бизнеса и постоянного совершенствования процессов и процедур. К основным аспектам относятся автоматизация изменений и управление ими, реагирование на события и определение стандартов успешного управления повседневными операциями.				
3.1. Развертывание изменений в коде автоматизировано	Решение должно использовать автоматизированный способ развертывания кода в инфраструктуре AWS. Интерактивные сессии Secure Shell (SSH) или Remote Desktop Protocol (RDP) запрещается использовать для развертывания обновлений в инфраструктуре AWS.	Да	Нет	
3.2. Определены процедуры Runbook и процедура эскалации	Необходимо разработать набор стандартных процедур Runbook, используемых для реагирования на различные события приложений и AWS. Необходимо определить процедуру эскалации для работы с предупреждениями и уведомлениями, сформированными системой, а также для реагирования на сообщенные клиентами инциденты. Процедура эскалации должна также включать передачу обращений в AWS Support в соответствующих случаях.	Да	Нет	
3.3. Для учетной записи AWS включена поддержка AWS Support уровня «Для бизнеса»	Необходимо включить поддержку AWS Support уровня «Для бизнеса». Наличие поддержки AWS Support «Для бизнеса» (или более высокого уровня) – это требование партнерской сети AWS к опытным партнерам-технологам APN. Чтобы получить статус опытного партнера, необходимо включить поддержку «Для бизнеса» по крайней мере для одной из учетных записей AWS.	Да	Нет	

4.0. Высокая производительность В основе высокой производительности лежит внимание к эффективному использованию вычислительных и ИТ-ресурсов. Основные направления включают правильный выбор типов и размеров ресурсов на основе требований к рабочим нагрузкам, мониторинг производительности, а также принятие обоснованных решений по вопросам поддержания эффективной работы по мере развития бизнеса.				
4.1. Тестирование производительности доступно после выполнения развертываний	Определены измеримые цели производительности. Проводится ее тестирование для того, чтобы проверить продукт на соответствие этим целям перед выпуском в рабочую среду.	Да	Да	
4.2. Наличие предельных значений для мониторинга	Реализован мониторинг производительности приложений. Используются механизмы, которые могут выводить предупреждения при превышении предельных значений.	Да	Да	

Ресурсы AWS:

Название	Описание
Как создать успешную целевую страницу	Руководство по созданию страницы об опыте и решениях партнера в соответствии с требованиями программы
Как подготовить описание публичного примера использования	Руководство по подготовке описания публичного примера использования в соответствии с требованиями программы
Как подготовить диаграмму архитектуры	Руководство по созданию диаграмм архитектуры в соответствии с требованиями программы
Документ для проверки готовности партнера	Руководство по требованиям программы с примерами рекомендаций
Веб-сайт AWS о концепции Well-Architected	Руководство, содержащее рекомендации по концепции Well-Architected