«Фармацевтическая отрасль», август № 4 (75) 2019

Целостность данных для облачных решений

PQE GROUP

Модели облачных вычислений в настоящее время активно используются во многих отраслях, что повышает надежность защиты данных и минимизирует связанные с этим расходы. Компании – производители фармацевтической продукции и изделий медицинского назначения начали полагаться на эту технологическую модель, хоть и с некоторой задержкой по сравнению с другими областями бизнеса.

В статье определены нормативные ожидания для записей GxP, управляемых через облачные сервисы, и меры контроля, которые должны быть реализованы в целях обеспечения целостности данных. Основное внимание уделено требованию, предъявляемому к валидации компьютеризированных систем, которое является основным для обеспечения надежности и конфиденциальности записей для систем этого типа. Данный подход позволяет снизить риски, возникающие в результате внедрения облачных решений, в которых сведения хранятся в дата-центрах, управляемых поставщиком под его полную ответственность, без видимости со стороны GxP-компании.

1. Предпосылки

При внедрении новых технологий GxP-индустрия всегда проявляла определенную консервативность, и облачные системы не являются исключением.

В целях обеспечения безопасности пациентов регулируемые компании (занимающиеся производством фармацевтической продукции и изделий медицинского назначения) подвергаются тщательному нормативному надзору и обязаны скрупулезно анализировать все риски, прежде чем внедрять какие-либо новые технологии. Тем не менее отрасли сталкиваются с необходимостью упростить свои сложные бизнес-процессы и сократить расходы. Одним из способов такой оптимизации стало внедрение сервисов облачных вычислений.

Национальный институт стандартов и технологий [1] определяет облачные вычисления как «модель для обеспечения повсеместного, удобного сетевого доступа «по требованию» к общему пулу настраиваемых вычислительных ресурсов (например, сетей, серверов, хранилищ, приложений, услуг), которые могут быть быстро предоставлены и реализованы с минимальными усилиями руководства или путем взаимодействия с поставщиком услуг». Обычно услуги в сфере облачных вычислений оказывает сторонний поставщик, который обладает необходимой для этого инфраструктурой. В последнее время облачные вычисления стали одной из самых обсуждаемых технологий и привлекают большое внимание средств массовой информации, а также аналитиков благодаря предлагаемым возможностям.

Потенциальные преимущества, которые применимы практически ко всем типам облачных вычислений:

- экономия средств, поскольку компании могут минимизировать свои капитальные затраты, заменяя их эксплуатационными расходами;
- адаптивность облачных вычислений, что позволяет компаниям наращивать ИТ-возможности в пиковые периоды времени для удовлетворения запросов потребителей;
- наличие сервисов, использующих несколько резервных площадок, которые могут поддерживать непрерывность бизнеса и производить аварийное восстановление;
- обслуживание поставщиками облачных услуг систем, не требующее установки приложений на ПК, что сводит к минимуму нагрузку на внутренний ИТ-отдел;
- повышение производительности мобильных работников благодаря наличию систем в инфраструктуре, доступных в любой точке мира;
- высокая доступность, поскольку дополнительные серверы можно добавить к предоставленной услуге без прерывания службы или необходимости перенастройки решения для поставки приложений;
- уменьшение потребности в ИТ-знаниях и ИТ-инвестициях.

При использовании подобных электронных услуг с целью обработки регулируемых данных в фармацевтической компании возникают новые риски, включающие:

- наличие систем и данных, внедренных в ИТ-инфраструктуру вне зоны контроля компании;
- отсутствие надзора за обслуживанием ПО (например, внесение изменений) и управлением центром обработки данных (например, контроль безопасности);
- различные поставщики, работающие вместе, чтобы обеспечить использование ПО и ИТ-инфраструктуры;
- риски кибербезопасности;
- необходимость применения индивидуального подхода к процессам валидации и квалификации.

Риски должны быть снижены, чтобы обеспечить целостность данных GxP, которая всегда находится в ведении регулируемой

компании. Для этого компания должна установить надлежащие и специальные средства контроля в целях обеспечения целостности управляемых данных. Недостаточная целостность данных и уязвимость подрывают качество записей и могут в конечном итоге привести к снижению качества лекарственных средств.

Документ ориентирован на определение нормативных ожиданий для регулируемых записей, управляемых через облачные сервисы, и основных тем, которые необходимо учитывать для обеспечения целостности данных, с учетом требований, предъявляемых к валидации компьютеризированных систем. Это является главным требованием для обеспечения надежности и конфиденциальности записей.

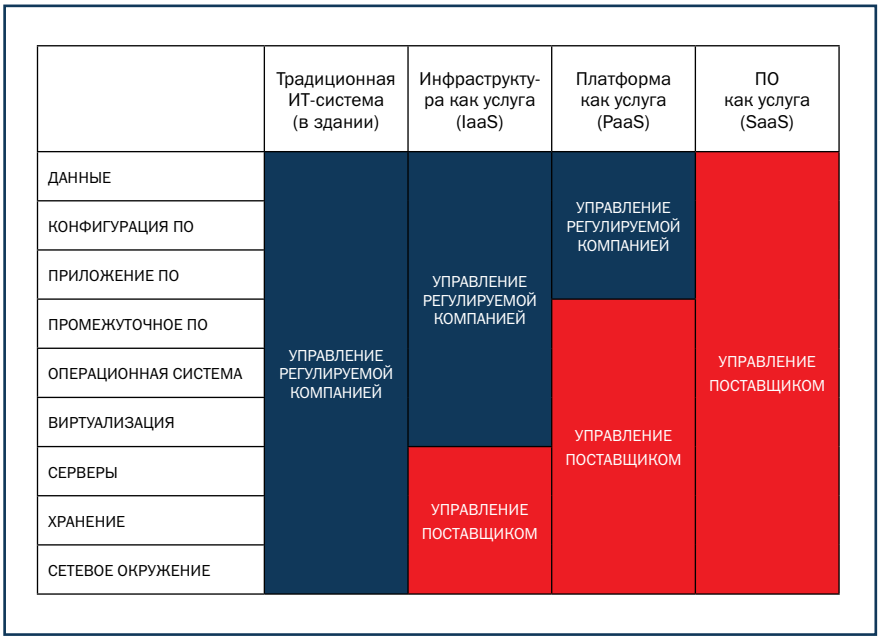

Рис. 1. Модели поставки систем

2. Типы облачных решений и модель ответственности

В настоящее время регулируемым компаниям предоставляются следующие виды услуг:

ПО как услуга (SaaS). Регулируемые компании используют приложения, работающие на инфраструктуре, принадлежащей поставщику ИТ-услуг. Регулируемые компании не управляют и не контролируют базовую инфраструктуру, но у них есть возможности регулирования пользовательских настроек приложений через конфигурацию и кастомизацию этих приложений.

Платформа как услуга (PaaS). Регулируемые компании используют ИТ-инфраструктуру, размещенную у поставщика ИТ-услуг, для запуска приложений, созданных с использованием операционных систем, языков программирования и инструментов, поддерживаемых поставщиком ИТ-услуг. Регулируемые компании не управляют и не контролируют базовую облачную инфраструктуру, включая сеть, серверы, операционные системы или хранилище, но по-прежнему контролируют развернутые приложения и, возможно, конфигурации среды размещения приложений.

Инфраструктура как услуга (IaaS). Владелец использует основные вычислительные ресурсы, такие как обработка, хранение, сети, где заказчик может развертывать и запускать произвольное ПО, которое может включать в себя операционные системы и приложения. Заказчик не управляет и не контролирует базовую облачную инфраструктуру, но контролирует операционные системы, хранилище, развернутые приложения и, возможно, осуществляет ограниченный контроль над отдельными сетевыми компонентами (например, межсетевыми экранами хоста).

На рис. 1 показаны виды ответственности трех типов услуг по отношению к традиционной ИТ-инфраструктуре с учетом рекомендаций GAMP [2].

Согласно соответствующему руководству NIST [3] облачные системы могут быть развернуты в соответствии с четырьмя различными моделями (частное облако, облачное сообщество, публичное облако и гибридное облако).

3. Нормативные ожидания

В настоящее время использование облачных систем разрешено регуляторными агентствами при условии, что связанные с этим дополнительные риски адекватно снижены. Ожидания, установленные регуляторными органами, перечислены ниже.

US FDA

С 1997 г. в соответствии с 21 CFR Part 11 [3], FDA США определило требования, предъявляемые к открытым системам. Для этих систем в § 11.30 FDA рекомендует «Люди должны использовать процедуры и средства контроля, предназначенные для обеспечения подлинности, целостности и, где это уместно, конфиденциальности электронных документов с момента их создания до момента получения». Эти процедуры и средства контроля включают те, которые указаны в § 11.10, и, при необходимости, дополнительные меры, такие как шифрование документов и использование стандартов цифровой подписи, для обеспечения, в зависимости от обстоятельств, подлинности, целостности и конфиденциальности записей.

В проекте руководства, выпущенном в июне 2017 г. [6], FDA признает, что спонсоры и другие регулируемые организации могут принять решение об аутсорсинге электронных услуг. Примерами этих типов электронных услуг являются услуги по управлению данными, включая услуги облачных вычислений. В руководстве FDA подробно изложены конкретные требования, предъявляемые к облачной системе, используемой в клинических исследованиях.

В частности, в руководстве подчеркивается, что при использовании облачных сервисов спонсор должен проверять следующие аспекты:

- валидационную документацию;
- возможность генерировать точные и полные копии записей;
- наличие и хранение записей для проверки FDA до тех пор, пока этого требует действующее законодательство;
- возможности архивирования;
- контроль доступа и проверку полномочий для действий пользователей;
- безопасные, сгенерированные компьютером контрольные журналы с отметками о времени действий пользователей и внесении изменений в данные;
- шифрование данных в покое и в пути;
- контроль электронной подписи;
- производительность записи поставщика электронных услуг и предоставляемых электронных услуг;
- возможность контролировать соответствие поставщика электронных услуг безопасности электронных услуг и средствам контроля целостности данных.

Спонсор должен получить соглашение об обслуживании с поставщиком электронных услуг. Прежде чем заключать соглашение, ему следует оценить и выбрать электронные услуги на основе способности поставщика электронных услуг соответствовать требованиям части 11 и мерам безопасности данных, описанным в предыдущем маркированном списке. В соглашении на обслуживание должны быть четко описаны указанные требования, а также определены роли и обязанности поставщика электронных услуг.

При наличии соответствующих средств контроля нет никаких ограничений в отношении географического расположения служб облачных вычислений. Однако для регулируемой компании очень важно понимать поток данных и знать местонахождение аппаратного обеспечения службы облачных вычислений, чтобы объективно оценить риски в отношении доступа, целостности и безопасности данных. Законы о конфиденциальности данных могут отличаться в разных странах, поэтому спонсорам и другим регулирующим организациям следует проводить соответствующие оценки рисков, чтобы гарантировать, что данные, хранящиеся на устройствах хранения за пределами их страны, могут быть извлечены и доступны во время инспекций FDA.

ВОЗ

В соответствии с соглашением о субподряде в руководстве ВОЗ [4] подчеркнута необходимость установления и надежного поддержания определенных ролей и обязанностей для обеспечения полноты и точности всех данных и записей.

Аутсорсинговая организация несет ответственность за достоверность всех полученных результатов. Эта ответственность распространяется на любых поставщиков соответствующих вычислительных услуг, таких как контрактные ИТ-центры обработки данных, контрактные ИТ-системы, персонал поддержки баз данных и поставщики решений облачных вычислений. Аутсорсинговые организации обязаны проверять адекватность систем управления получателя контракта посредством проведения аудита или с помощью других подходящих для этого средств.

Ожидаемые стратегии контроля целостности данных должны быть включены в соглашения о качестве, в контракты и технические соглашения, в зависимости от определенной ситуации и с учетом необходимости, между лицом, предоставляющим контракт, и лицом, принимающим контракт.

MHRA

В своем руководстве [7] MHRA утверждает, что следует уделить внимание пониманию предоставляемых услуг, владению, поиску, хранению и безопасности данных. Физическое / географическое расположение данных должно вызывать обеспокоенность и учитывать влияние применимости любого закона. Обязанности подрядчика и заказчика контракта должны быть определены в техническом соглашении или в контракте, что обеспечит своевременный доступ к данным (включая метаданные и контрольный след) владельцу данных и национальным компетентным органам по запросу. В контрактах с поставщиками должна быть определена ответственность за архивирование и постоянную читаемость данных в течение всего срока их хранения. Необходимо разработать соответствующие меры для восстановления ПО / системы в соответствии с их исходным валидированным состоянием, включая информацию о валидации и управлении изменениями, чтобы разрешить данное восстановление.

Механизмы обеспечения непрерывности бизнеса должны быть включены в контракт и проверены. Необходимость проведения аудита деятельности поставщика услуг должна быть основана на учете риска.

ISPE

В разных руководствах ISPE обсуждены аспекты, связанные с услугами облачных вычислений.

В Руководстве по инфраструктуре GAMP [2] содержатся специальные разделы об элементах ИТ и облачной инфраструктуры, рисках и конкретных аспектах соответствия и контроля, связанных с аутсорсингом инфраструктуры, виртуализацией и внедрением облачных технологий.

Специальное приложение GAMP «Записи и целостность данных» [5] сфокусировано на проблемах целостности данных, что связано с архитектурой системы: в частности, выделены риски для управления изменениями, аварийного восстановления и управления инцидентами для различных типов облаков – SaaS, IaaS и PaaS.

4. Меры по обеспечению целостности данных

В соответствии с вышеописанными ожиданиями регулирующих органов регулируемая компания несет основную ответственность за обеспечение надежности регулируемых данных, создаваемых и поддерживаемых с помощью облачных ИТ-решений.

Это нормативное ожидание должно быть выполнено посредством процесса валидации компьютеризированных систем, основанного на строгой квалификации поставщика и заранее установленном соглашении об уровне обслуживания, заключенном с поставщиком. Эти критические факторы необходимо учитывать, и они должны быть ориентированы на снижение рисков в отношении целостности данных, возникающих в результате использования облачных решений.

4.1 Квалификация поставщика и соглашение об уровне обслуживания

Квалификация поставщика должна быть ориентирована на оценку мер контроля, применяемых поставщиком для жизненного цикла разработки ПО и обслуживания регулируемых данных, которыми планируется управлять через облачную систему.

Для управляющих записями систем, которые могут оказать непосредственное влияние на безопасность пациентов и качество продукта, рекомендовано провести локальный аудит поставщика; для менее критичных систем (например, управление записями обучения) возможен удаленный аудит.

Будущие проверки должны быть сосредоточены на таких элементах:

- Спецификация и тестовая документация, связанная со стандартными функциональными возможностями, предоставляемыми поставщиком.
- Авторизация безопасности и разделение служебных обязанностей.
- Контрольный след и мониторинг журнала событий.
- Механизм контроля доступа.
- Механизм идентификации и аутентификации.
- Операции по управлению изменениями (включая любые методы выгрузки периодических исправлений), временные рамки и связанное с ними регрессионное тестирование.
- Возможности хранения данных.
- Предоставление поставщиком сведений в регулируемую компанию о проблемах, которые влияют на целостность данных, включая, помимо прочего, технические и хостинговые решения, связанные с ними нарушения безопасности, ошибки в ПО, проблемы резервного копирования и восстановления и/или выполнение плана аварийного восстановления.
- Квалификация инфраструктуры или эквивалентные меры контроля (также в тех случаях, когда инфраструктурой управляет третья сторона).
- Управление поставщиками и соответствующие соглашения об уровне обслуживания.
- Меры контроля для обеспечения кибербезопасности.
- Наличие доступных сертификатов (например, SSAE 16, ISO 27001, SOC 1/2 FedRAMP, HITRUST) для подтверждения соответствия передовым ИТ-практикам.

В случае, если одна или несколько существующих мер контроля признаны неадекватными, результирующие воздействия на процесс валидации следует должным образом оценить, а поставщику необходимо принять меры по смягчению выявленных результатов с помощью плана корректирующих действий.

Процессы, находящиеся под ответственностью поставщика и необходимые для обеспечения целостности регулируемых данных, должны быть определены в заранее утвержденном соглашении об уровне обслуживания, которое отражено в договорных обязательствах с поставщиком, включая штрафы за любое несоответствие. Эти процессы могут быть определены в специальном разделе документа с требованиями пользователя, который должен соответствовать соглашению об уровне обслуживания, касающемся следующих факторов:

- Управление и уведомление о любых изменениях, которые могут повлиять на предполагаемое использование вычислительной среды и связанных с ними сроков, включая обязательство обеспечить адекватное регрессионное тестирование.
- Наличие системных сред, доступных для выполнения любых тестовых операций.
- Управление инцидентами и уведомление фармацевтической компании о проблемах, влияющих на целостность данных.
- Ведение валидационной документации под ответственность поставщика.
- Меры безопасности, реализуемые поставщиком.

- Операции по резервному копированию и восстановлению.
- Планирование проведения аварийного восстановления, тестирование и требования, предъявляемые к уведомлениям.
- Соглашение о технической поддержке, определяющее временные ограничения для обработки запросов об инцидентах и изменениях.
- Соглашения о конфиденциальности.
- Право на аудит системы, ИТ-инфраструктуры и данных.
- Субподрядные ограничения.
- Соглашения об условном депонировании.

Процесс валидации должен быть разработан в соответствии с общими директивами, изложенными в руководящих принципах (GAMP 5 [8], PIC/S [9]), и адаптирован к конкретным рискам, связанным с моделью облачного сервиса, который планируется использовать.

4.2 Жизненный цикл валидации SaaS

Жизненный цикл валидации должен быть выполнен. Это гарантирует, что компьютеризированная система надлежащим образом протестирована / валидирована с учетом следующих конкретных мер:

- Оценка поставщика должна быть выполнена на площадке до определения стратегии по валидации в соответствующем плане валидации.
- В плане валидации необходимо учесть итоги этапа оценки поставщика и риски, возникающие вследствие отклонений, обнаруженных в ходе проведения аудита.
- В документации о валидации должны быть соотнесены спецификации, документация по тестированию монтажа (IQ) и тестированию функциональности (OQ), предоставленные поставщиком, при условии, что эти документы признаны адекватными в ходе оценки поставщика; в случае, если поставщик не имеет адекватной и отслеживаемой документации для тестирования, функциональную проверку должна выполнять регулируемая компания.
- Необходимые вспомогательные процессы (например, управление изменениями, управление инцидентами) следует осуществлять с помощью специализированных процедур, согласованных с практиками поставщика.
- На этапе тестирования проверки конфигурации (также называемой квалификацией монтажа) проверяют действующий статус соглашения об уровне обслуживания (то есть проверка наличия утвержденного SLA) и необходимых вспомогательных процедур.
- Проверка функциональности (также называемая квалификацией функциональности) ограничена теми функциональными возможностями, на которые в значительной степени влияет конкретная конфигурация, и настраиваемыми компонентами (например, интерфейсами с внешними системами).
- Фазу проверки требований (также называемую квалификацией эксплуатации – PQ или тестом приемлемости пользователя – UAT) должна выполнять регулируемая компания, которая проверяет использование системы по назначению (на основе соответствующих спецификаций требований пользователя) во всех предполагаемых рабочих диапазонах.

Сведения о типичной взаимной ответственности (которая должна быть подтверждена в соглашении об уровне обслуживания) приведены в Таблице 1.

Таблица 1. Ответственность по валидации систем SaaS

Результаты валидации для SaaS	Ответственный	
	Регулируемая компания	Поставщик
Оценка GxP-воздействия системы	•	
Требования пользователя	•	
Оценка поставщика	•	
План валидации	•	
Оценка функционального риска	•	•
Функциональные и проектные спецификации		•
Спецификации конфигурации	•	•
Квалификация монтажа (IQ)		•
Квалификация функциональности (OQ)	•*	•
Квалификация эксплуатации или тестирование приемлемости пользователя PQ	•	
Отчет о процессе валидации	•	
Квалификация инфраструктуры		•

* Только для специфических конфигураций компании и изготовленных на заказ компонентов.

В соответствии с классификацией системы, определенной руководством GAMP 5 [8], для облачных приложений следует рассматривать только категории 4 и 5 по GAMP. С точки зрения регулируемой организации, конфигурацию облачных приложений необходимо рассматривать как ка-

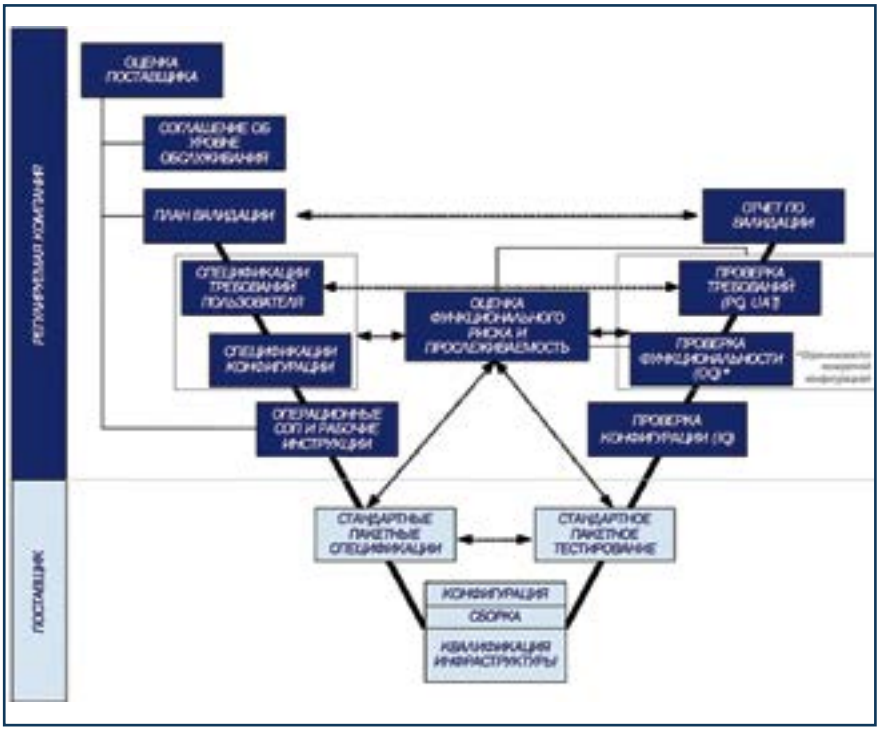

Рис. 2. Жизненный цикл валидации SaaS

тегорию 4, в то время как любую пользовательскую разработку для значимых интерфейсов GxP или источника данных, который взаимодействует с облачным приложением, – как категорию 5 и тестировать соответствующим образом.

В процессе валидации SaaS (рис. 2) фаза тестирования является ключевой, поскольку она обеспечивает доказательство того, что предполагаемое использование, определенное регулируемой компанией, выполнено. Оно должно быть сосредоточено на следующих мероприятиях:

- Тестирование поставщиком стандартного пакета предоставляется при условии, что предварительно его оценили как приемлемый для фармацевтической компании.
- Валидационное тестирование регулируемой компании – дополнительные мероприятия по тестированию, которые в основном сосредоточены на конкретном предполагаемом их использовании компанией с учетом индивидуальных конфигураций и/или настроек компании.
- Поскольку данные (в электронном виде) размещаются в сторонней компьютерной среде, необходимо принять дополнительные меры безопасности для облачной системы, такие как шифрование данных и использование соответствующих стандартов электронной подписи для обеспечения подлинности, целостности и конфиденциальности записей. Это означает, что данные должны быть зашифрованы во время передачи (например, с использованием зашифрованного / защищенного соединения, такого как VPN) и быть в состоянии покоя (например, через зашифрованную базу данных), а функции утверждения должны гарантировать идентичность подписывающих сторон (с использованием цифровых подписей, механизмов хеширования для обеспечения соблюдения неизменности записей, заверенных электронной подписью).
- План тестирования системы SaaS должен включать раздел о регрессионном тестировании: все GxP-критические или бизнес-критические процессы необходимо учесть во время такого тестирования.
- Регрессионные тесты должен выполнять поставщик SaaS для каждой новой версии и в соответствии с заранее определенной оценкой воздействия.

После завершения фазы тестирования система может быть запущена для ее успешного использования: выполнение регулируемых процессов через SaaS требует более высокого уровня мониторинга по сравнению с традиционными системами, проверки эффективности процедур и соблюдения рабочих инструкций, направленных на поддержание валидированного статуса системы.

4.3 Жизненный цикл валидации для систем, включающих IaaS или PaaS

В случае, если планируется внедрить систему на основе облачной инфраструктуры (IaaS) или платформы (PaaS), традиционный процесс валидации должен включать меры контроля, цель которых – обеспечить надежность и мониторинг инфраструктуры ИТ.

Также в этом случае применяются требования, предъявляемые к тщательной оценке поставщика (включая проверку управления конфигурацией и контроль изменений компонентов инфраструктуры) и заранее определенному уровню обслуживания, которые должны быть сосредоточены на ИТ-компонентах, находящихся под управлением и ответственностью поставщика.

В соответствии с диаграммой, представленной на рис. 3, все результаты валидации должны быть созданы регулируемой ком-

панией, за исключением квалификационной документации базовых компонентов ИТ-инфраструктуры, которые обязан предоставить поставщик.

Документация поставщика должна гарантировать, что ИТ-компоненты находятся под надлежащим контролем в случае IaaS (серверы, сеть, питание и охлаждение) и PaaS (база данных, промежуточное ПО, ОС и компоненты инфраструктуры): эти документы должны использоваться регулируемой компанией и упоминаться в пакете документации по процессу валидации системы.

5. Заключение

В настоящее время облачные решения являются зрелыми с технологической точки зрения, что обеспечивает преимущество в отношении снижения затрат, безопасности и предоставлении возможностей для динамического масштабирования. Производители фармацевтической продукции и изделий медицинского назначения могут принять эти услуги при условии соблюдения ожиданий соответствия, недавно установленных большинством регулирующих органов. Для выполнения данной задачи регулируемым компаниям следует принимать такие решения взвешенно: поставщиков решений на основе облака необходимо тщательно выбирать, включая надлежащую оценку меры контроля, применяемой поставщиком до начала предоставления услуг. Ожидается, что эта мера, встроенная в процесс валидации, обеспечит целостность GxP-релевантных данных, созданных и поддерживаемых регулируемыми компаниями с помощью облачных решений. ◘

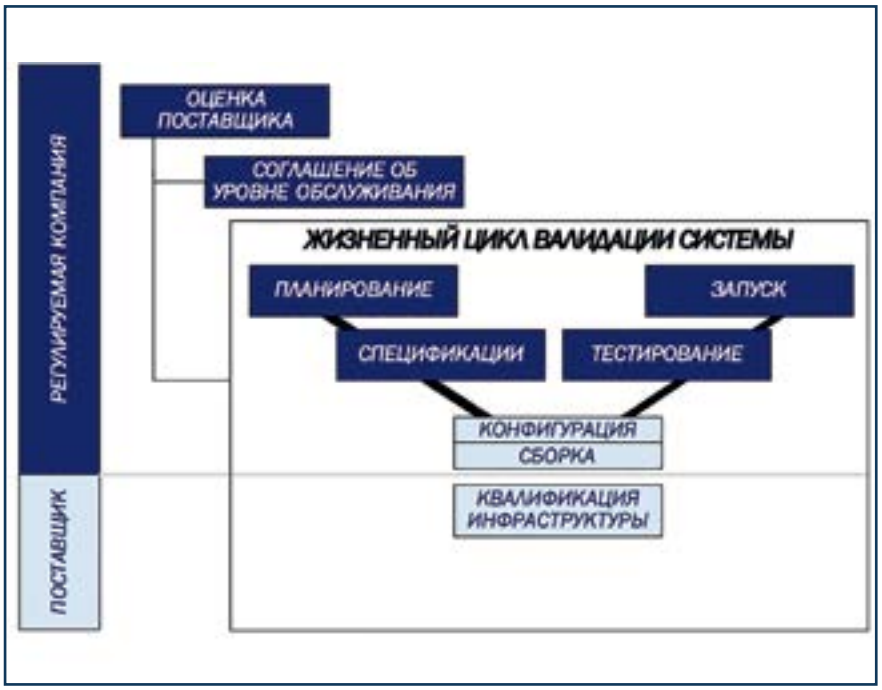

Рис. 3. Жизненный цикл валидации системы на основе IaaS / PaaS

Контактная информация:

Сандлер Юрий
Управляющий директор
Тороповский Александр
Менеджер по развитию бизнеса
Тел.: +7 (929) 616 - 53 - 23
РФ, 127015, г. Москва
ул. Новодмитровская 2к2
БЦ Савеловский Сити, башня Davis
Тел.: +7 (495) 133 - 98 - 36
e-mail: a.toropovskiy@pqegroup.ru
www.pqegroup.ru

Список литературы:

1. *NIST Special Publication 800 – 145, the NIST Definition of Cloud Computing, September 2011, National Institute of Standards and Technology (NIST), www.iec.ch*
2. *GAMP Good Practice Guide – IT Infrastructure Control and Compliance, August 2017.*
3. *NIST Special Publication 800 – 145 The NIST Definition of Cloud Computing.*
4. *US FDA 21 CFR part 11, March 1997.*
5. *WHO Technical Report Series No. 996, Annex 5 – Guidance on Good Data and record management practices – June 2016.*
6. *ISPE GAMP Guide – Records and Data Integrity – 2017.*
7. *FDA Guidance for Industry – Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers, Draft, June 2017.*
8. *MHRA – GXP Data Integrity Guidance and Definitions – Revision 1, March 2018.*
9. *GAMP 5 – A Risk-Based Approach to Compliant GxP Computerized Systems, GAMP5, 2008, issued by the GAMP Forum.*
10. *PIC/S Guidance – Good Practices for Computerised Systems in Regulated «GxP» Environments, 2007.*