# Можно ли обеспечить безопасное использование облачных технологий?

**Не приведет ли переход к облачной модели использования ИТ к нарушению информационной безопасности с серьезными последствиями? Что можно сделать, чтобы избежать этих последствий? Об этом рассказывают наши эксперты.**

***- В чем вы видите основную идею облачных вычислений? Насколько (и в чём) использование облачных сервисов может быть привлекательным для банка?***

**Александр Неваленный:** В первую очередь, это публичность тех или иных сервисов - ведь облачные решения нашли свои применения именно в бесплатных почтовых сервисах. Если говорить о внешнем облаке, то это привлекательным может стать, например, перенос риска, связанного с отказоустойчивостью, на другое лицо.

**Константин Феоктистов:** Основанная идея облачных вычислений заключается в возможности снять с организации непрофильные затраты, связанные с необходимостью эксплуатации ИТ-инструментов в интересах основного бизнеса и предоставить простой и быстрый способ использования этих инструментов в случае возникновения потребности. Пусть управлением финансами занимаются профессионалы в области финансов, а необходимыми для их работы информационными системами, приложениями и сервисами должны заниматься профессионалы в области информационных технологий. Если бизнесу для работы нужен инструмент, то облачная модель предоставления услуг должна позволить ему воспользоваться им максимально быстро, с минимальным привлечением сторонних организаций, и в том объеме, который необходим для получения ожидаемого результата.

Зачем покупать таксопарк, чтобы иметь возможность раз в неделю добраться из одного офиса в другой? Достаточно просто вызвать такси! Так и с информационными системами: не нужно строить громоздкую инфраструктуру, нанимать на работу еще одного системного администратора и разработчика программ, чтобы воспользоваться самой удобной в отрасли CRM-системой или протестировать новый сервис онлайн-регистрации участников рекламной компании. Всё это можно купить по мере появления необходимости и не переплачивать за неудачные проекты.

В теории, основной довод внедрения облачных вычислений обещает снижение затрат на эксплуатацию облачных решений по сравнению с затратами на создание и содержание собственных решений компаний, размещаемых в собственных серверных, поддерживаемых собственными разработчиками и администраторами. Как показала практика использования облачных вычислений за последние несколько лет развития этого вида услуг, в отличие от теории, облачные вычисления несут организациям различного уровня отнюдь не снижение общих затрат.

Сегодня привлекательность использования сервисов облачных вычислений заключается, прежде всего, в скорости реализации требований бизнеса, скорости оперативной реакции создаваемых систем на изменение условий их эксплуатации, скорости вывода новых решений и продуктов на рынок, оперативности реализации пилотных проектов и тестовых решений. Чем быстрее ИТ-подразделение с минимальными первоначальными затратами может реализовать новую функцию или электронную услугу – тем существеннее польза от применения облачных решений.

**Николай Носов:** Основная идея облачных вычислений – получить вычислительные мощности и программные средства по требованию, а также аутсорсинг их поддержки.

Основная привлекательность для банка - нет необходимости держать у себя сложную в поддержке и дорогую ИТ- инфраструктуру, экономия на CAPEX за счет OPEX.

**Никита Нецкин:** Основная идея облачных вычислений – это получение оптимального количества ресурсов в кратчайший срок для решения конкретной задачи, отсутствие необходимости тратить время и деньги на закупку, установку и наладку дорогостоящего оборудования. И это несомненный плюс для Банка.

Но с другой стороны любое нововведение сопряжено со определенными рисками. И в данном случае возникает задача минимизации риска перехвата и фальсификации передаваемых данных.

***- Может ли упроститься поддержание безопасности ИТ-инфраструктуры организации при более широком использовании облачных сервисов?***

Текст: Андрей Новиков

**Николай Носов:** Да, может. Чем шире будут использоваться облачные технологии, тем больше будет внимания работам по облачным проблемам ИБ.

**Александр Неваленный:** Если идет речь о внешнем облаке, то да, конечно – сервис будет находиться в эксплуатации сторонней организации, и качество обслуживания сведется к детализации SLA.

**Никита Нецкин:** Я вижу только один сценарий, при котором будет проще поддерживать безопасность ИТ-инфраструктуры организации, и это возможно только в случае значительного роста доверия к облачным сервисам.

Сегодня, с одной стороны, мы видим развитие и совершенствование предоставляемых облачных сервисов. С другой стороны, в сеть с регулярной периодичности попадают новости об утечке информации с облаков.

**Константин Феоктистов:** В нынешних условиях упрощение поддержания безопасности обратно пропорционально стоимости этого упрощения. Чем проще, с точки зрения потребителя, решается задача обеспечения конкретных требований безопасности, тем большую цену за это решение придется заплатить. Большинство поставщиков услуг облачных вычислений рассматривают услуги по обеспечению безопасности, как дополнительные опции по требованию заказчика, и готовы сделать любое предложение по желанию клиента. Естественно, в пересчете на уникальность данных предложений [не для массового применения] это приводит к индивидуальной цене, сопоставимой с ценой создания аналогичной системы обеспечения безопасности в рамках собственной инфраструктуры, а не в облаке.

Вместе с тем, создание «частных облаков» в рамках крупных банков с разветвленной сетью филиальных подразделений, в общем случае, приведет к централизации управления, стандартизации подходов и консолидации средств защиты в рамках собственного облака. В результате, это может послужить основой для экономии средств в рамках всей организации, но в каждом случае эта экономия будет зависеть от масштаба решаемой задачи.

В большинстве случаев, осмысленный «поход в облака» для организации оказывается достаточно дорогим путешествием, требующим существенного пересмотра подходов к построению ИТ и серьезного отношения к вопросам обеспечения безопасности по сравнению с обычной инфраструктурой.

***- Какие проблемы информационной безопасности могут возникнуть у банка при использовании облачных сервисов?***

**Константин Феоктистов,** главный архитектор департамента комплексных проектов компании «Информзащита» • **Александр Неваленный,** независимый эксперт • **Никита Нецкин,** менеджер по работе с финансово-кредитными организациями, компания «Актив» • **Николай Носов,** к.т.н., главный специалист по ИБ КБ Кутузовский

**Александр Неваленный:** В первую очередь, это требования законодательства, которое не предусматривает возможности передачи сведений, относящихся к банковской тайне, третьему лицу даже с согласия клиента. Также могут возникнуть сложности при передаче персональных данных, если облако находится за рубежом. С технической точки зрения, чем более распределенная инфраструктура, тем больше проблем, связанных с ее контролем, включая моменты доверия к месту, где размещено облако.

Никита Нецкин: Я считаю, что основные проблемы связаны предоставлением и ограничением доступа к сервису и информации. Возрастает потребность в надежном и проверенном механизме аутентификации и идентификации пользователя. Так же требуется обеспечить защиту канала передачи данных.

**Константин Феоктистов:** Основной проблемой при пользовании облачными сервисами является доверие поставщику услуг со стороны потребителя – банка и его службы безопасности. Как правило, бизнес облачных поставщиков строится с фокусом на снижение собственных издержек и ценовой конкуренции, как результат – снижение требований к безопасности и, в некоторых случаях, даже надежности инфраструктуры. Если потребитель услуг самостоятельно не обеспечит в таких условиях надлежащего контроля за уровнем безопасности, доступности, не позаботится о вопросах резервирования решения и восстановления на случай непредвиденных обстоятельств, то, вместе с приобретением, казалось бы, более дешевого по сравнению с собственной инфраструктурой, сервиса, банк может получить высокие риски потери контроля над собственными данными, приложениями, бизнес-процессами. Только продуманный подход к вопросам миграции в облако существующих в банке информационных систем, взвешенный

выбор поставщика облачных услуг и зрелый подход к разработке архитектуры облачного решения позволят, переходя в «облака», не приобретать дополнительных проблем к существующим у банка проблемам безопасности информационных систем.

**Николай Носов:** Главная проблема – недоступность сервисов из-за «падения» каналов. Не всегда удается сделать их надежное резервирование. Есть опасения и по поводу физической защиты серверов у провайдера облачных услуг. Mission-critical сервисы банков слишком рискованно размещать в публичных облаках из-за возможных атак через гипервизор.

***- Как обеспечить безопасный доступ к облачному сервису (защититься от атак на устройство пользователя, от атак на канал доступа – в общем, аналогично интернет-банкингу)?***

**Никита Нецкин:** С помощью многофакторной аутентификации и комплексного подхода к обеспечению безопасности. Но самое главное это разумность переноса сервисов и информации в облако.

**Николай Носов:** Сейчас представляется относительно надежным вариант двухфакторной идентификации, с получением кода по СМС на мобильное устройство, отличное от того, где предоставляется доступ к сервису.

**Константин Феоктистов:** Подход к обеспечению защиты каналов облачного решения практически ничем не отличается от подхода к защите частной инфраструктуры – используются те же самые средства построения VPN, средства построения SSL/TLS защищенных соединений на базе цифровых сертификатов, те же мобильные пользовательские клиенты с усиленной аутентификацией пользователей.

Средства защиты, с помощью которых бизнес противостоит атакам на системы интернет-банкинга, размещенные в облаке, мало чем отличается от аналогичных подходов для систем, развернутых в рамках собственной инфраструктуры. Различия могут быть только на уровне контроля над средствами защиты: что из защитных мер реализуется поставщиком услуг облачной платформы, поставщиком услуг транспортной сети, поставщиком сервисов безопасности, а что реализуется самим потребителем в разворачиваемой в облаке системе. Если каких-то средств защиты поставщик услуг облачных вычислений предоставить не может, потребителю необходимо самостоятельно озаботиться вопросами обеспечения защиты каналов доступа к сервису: закупить и разместить соответствующие средства на площадке «облака», если такое представляется возможным, или обратиться к третьей стороне – поставщику соответствующих услуг безопасности. В качестве примера: защита от DDoS атак может быть реализована 1) самим поставщиком облачной инфраструктуры, в которой размещается система заказчика, 2) на уровне поставщиков телекоммуникационных услуг – телеком-оператором, 3) на уровне внешнего сервиса зачистки трафика от DDoS, и, наконец, 4) самим заказчиком в случае размещения оборудования в облачном ЦОДе.

Подход к защите конечных пользовательских устройств так же мало чем отличается от классического подхода: необходимо использовать средства защиты канала (VPN/SSL/TLS шифраторы), проверять серверную сторону в процессе подключения (SSL/TLS сертификаты), контролировать оконечные устройства при наличие такой возможности (антивирусы, MDM-решения), применять средства дополнительной/усиленной аутентификации пользователей при входе в пользовательское приложение, обеспечить хранение локальных кэшируемых на клиенте данных в защищенном хранилище (в том числе с использованием шифрования). Если у владельца размещаемой в облаке системы есть возможность влиять на процесс разработки приложения для конечного устройства пользователя, то надо формировать требования по безопасности на этапе разработки и встраивать функции защиты в мобильное приложение, анализируя существующие в настоящее время угрозы для данного класса приложений. Кроме этого необходимо информировать пользователей о наиболее актуальных угрозах и обучать навыкам работы с мобильными устройствами в условиях агрессивной среды Интернета. Как видите, указанные меры не имеют какой-то облачной специфики.

**Александр Неваленный:** Если говорить о внутренних сервисах, к которым не нужен доступ извне, то лучший вариант - выделенный канал, физический «провод» от офиса до облака. Некоторые организации в Москве так и делают. К защите внешних сервисов, к которым необходим доступ через интернет, важно подойти комплексно: обеспечить резервирование каналов, серверов, обучение персонала, проведение тестов на проникновение, и, конечно же, анализ кода самого сайта или приложения на наличие уязвимостей.

***- Можно ли защитить информационные активы организации, пользующейся облаками, если нет абсолютного доверия к провайдеру облачного сервиса? Помогает ли обретению доверия***

***к провайдеру его сертификация по разным стандартам?***

**Никита Нецкин:** Защитить можно и нужно. Другой вопрос: как защитить так, чтобы вызвать доверие и желание использовать сервис? Доверие нарабатывается со временем, и сертификаты на данный процесс сильно не повлияют.

**Николай Носов:** Я, напротив, считаю, что сертификация провайдера помогает повышению доверия к нему. Например, сертификация его ЦОД по Tier III. Но облачных стандартов в России нет. Этим надо заниматься.

**Александр Неваленный:** Абсолютную защиту обеспечить невозможно нигде, но создать условия, при которых наступление негативных последствий минимально – возможно. Например, если говорить об электронной почте, можно встроить использование средств электронной подписи и шифрования, тогда письма будут защищены от изменения и чтения посторонними. Другое дело, что возникает вопрос защищенного хранения ключей пользователей и восстановления писем в случае кражи или блокировки ключей электронной подписи и шифрования.

**Константин Феоктистов:** Защитить информационные активы организации можно и в условиях построения системы на базе публичных облаков. Просто при разработке такого решения необходимо уделять пристальное внимание вопросам организации обеспечения безопасности у поставщика облачных услуг и не отдавать ответственность за все вопросы безопасности, надежности, доступности создаваемой системы на откуп поставщику.

Применение необходимого и достаточного набора классических и специализированных [для виртуальных сред и облачных приложений] программных и технических средств защиты при построении решения, дублирование и резервирование компонентов системы на различных площадках, автоматизация процесса мониторинга доступности информационных сервисов, разработка процедур перевода сервисов на резервные платформы, подготовка персонала к действию в непредвиденных обстоятельствах, внимание к вопросам резервного копирования на доверенную инфраструктуру, шифрование данных при хранении и передаче по сетям – всё это будет повышать защищенность облачного решения не менее, чем в классической инфраструктуре.

Конечно, такой подход не делает облачное решение дешевым. Но такова цена недоверия поставщику облачных услуг в вопросах обеспечения безопасности. Если же бизнес ставит своей целью снижение издержек, то он вынужден будет мириться с тем, что часть нагрузки по обеспечению безопасности будет перенесена на плечи поставщика облачных услуг или поставщика услуг безопасности. Правда, передать ответственность будет недостаточно: доверяй, но проверяй! Контрольные функции [там, где это технически возможно] должны всё-таки остаться в руках заказчика облачных услуг, и в момент эксплуатации, и, прежде всего, при принятии решения о выборе конкретного поставщика.

Так, международная организация Cloud Security Alliance (CSA), являющаяся одним из ведущих разработчиков стандартов безопасности для отрасли облачных вычислений, предлагает подход, включающий проведения самостоятельной оценки поставщиком уровня обеспечения безопасности в рамках предоставляемых услуг, и последующей возможности потребителю выбрать того поставщика, который наилучшим образом удовлетворяет требованиям по безопасности. Американские программы FISMA Cloud Computing & FedRAMP Program сертификации поставщиков облачных услуг так же опираются на проведении самооценки и декларации соответствия с целью повышения доверия потребителей облачных услуг к уровню обеспечения безопасности поставщика.

В России пока таких стандартов и подходов нет, точнее они не применяются. Максимум, на что может рассчитывать потребитель облачных услуг – это аттестация инфраструктуры по требованиям безопасности ФСТЭК и/или размещение инфраструктуры облака в датацентре, сертифицированном Uptime Institute по стандарту Tier.

***- Насколько серьезные проблемы использованию облачных сервисов может создать Закон «О персональных данных»? Насколько дорого обойдется их устранение?***

**Александр Неваленный:** Вопрос скорее юридический, чем технический. Если действовать по модели аренды оборудования, то вопрос передачи персональных данных становится не таким актуальным. Если же банк станет арендовать некий сервис, обрабатывающий персональные данные клиентов банка, то проблем может возникнуть много: нужно найти основание для передачи данных третьему лицу, получить на это согласие всех субъектов данных и многое другое.

**Николай Носов:** Пока трудно понять, насколько жестко он будет работать на практике. И будут ли проблемы у тех, кто его не выполняет.

**Константин Феоктистов:** Закон 152-ФЗ в текущей

его версии не сильно вредит использованию облачных решений при создании или переносе классических ИСПДн в облачную среду. Но есть нюансы. Прежде всего, в зависимости от уровня защищенности и уровня предъявляемых требований безопасности, стоит вопрос об использовании сертифицированных решений, которые в настоящее время установлены и используются только у российских поставщиков облачных услуг. Во-вторых, изменения, внесенные в закон статьями 242-ФЗ о размещении БД ПДн граждан РФ только на территории РФ, приводят к использованию публичных облачных платформ только тех поставщиков, оборудование которых физически размещено в пределах государственной границы РФ. Ни Amazon, ни Microsoft, ни Google, ни IBM, ни Rackspace или иные западные поставщики не могут быть использованы в качестве основы для построения ядра облачной ИСПДн, содержащей хранилище персональных данных, если они не имеют собственных площадок на территории РФ. А в настоящее время дело так и обстоит. Существуют отдельные партнерские проекты MS Azure, реализующие локальные площадки в России, но к полноценному облаку Azure они не относятся.

Если поставщик облачных услуг может обеспечить большинство требований по безопасности к ИСПДн на уровне инфраструктуры и платформы (в том числе, с учетом требований по использованию сертифицированных средств защиты), то потребителю останется толь систематически оплачивать их использование. Иначе, реализацию этих требований потребителю придется взять на себя, что в принципе, с точки зрения стоимости, не сильно отличает собственное решение по защите от арендуемого сервиса поставщика. Но, как говорилось выше, есть нюансы конкретных условий и особенности архитектур, требующих внимания на этапе подготовки решения.

***- «Публичное облако» vs «частное облако»: с чем проще работать банку с точки зрения ИБ?***

**Николай Носов:** Однозначно частное лучше. Его можно использовать даже для mission-critical систем банка.

**Константин Феоктистов:** Безусловно, в целях обеспечения конфиденциальности обрабатываемых данных, в том числе, платежных карт и обеспечения банковской тайны, банкам в процессе развития собственной инфраструктуры выгоднее использовать решения, опирающиеся на «частные облака». «Публичные облака» несут повышенный риск выхода обрабатываемых данных из-под контроля службы безопасности банка. Но ситуация не однозначна и в каждом случае требует проработки решения и выбора наиболее подходящего «типа облака» под конкретную задачу.

**Александр Неваленный:** Вопрос неоднозначный. На одной чаше весов - перекладывание рисков, связанных с ИБ, на другую организацию, если это прописано в SLA. на другой - полный контроль сервиса в рамках собственной организации, который исключает возможность злонамеренных действий со стороны провайдера, а так же моменты, связанные с передачей сведений силовым ведомствам.  Мне баланс видится так: облако должно быть частным, но в штате должны быть хорошие специалисты.

***- Как вы видите будущее развитие средств обеспечения информационной безопасности, если всё больше решаемых пользователями задач будет выполняться в облачной модели вычислений?***

**Александр Неваленный:** Облачные решения пока не перевернули архитектуру информационных технологий. И риски остаются прежними, и приемы их снижения. Главное - в том, что многие сервисы становятся публичными. Поэтому важно уметь бороться с DDoS -атаками, защищать код сайта и приложений, шифровать передаваемую информацию и обучать людей правилам безопасной работы в сети Интернет.

**Николай Носов:** Будет больше уделяться внимания рискам, связанным именно с облачными технологиями, и вопросам доступности облачных сервисов.

**Никита Нецкин:** Все более важным становится вопрос обеспечения надежного и удобного доступа к информации и сервисам. При этом задача обеспечения безопасности все время усложняется, так как пользователь сконцентрирован в первую очередь на удобстве и простоте работы с сервисом. Мошенники, в свою очередь, становятся все более организованы. И при сохранении данного тренда ситуация для конечного пользователя облачных технологий в какой-то момент может стать критической.

**Константин Феоктистов:** В процессе постепенного перестроения сознания руководства ИТ-служб и служб безопасности в части вопросов использования решений, основывающихся на моделях облачных вычислений, будет меняться и отношение к обеспечению безопасности. Эти изменения будут выражены в появлении и использовании новых средств защиты и решений безопасности (в том числе, облачных), интегрирующихся с облачными платформами, сред-

ствами управления облачными инфраструктурами, обеспечивающих необходимый заказчикам уровень безопасности.

Большое количество классических продуктов безопасности уже активно используют облачные вычисления для своих нужд: Symantec, McAfee, Check Point, Panda Software, Лаборатория Касперского и многие другие – эти бренды содержат различную часть инфраструктуры сервисов безопасности в облаках. Производители облачных продуктов: VMware, IBM, Oracle, Microsoft, Citrix, Amazon - интегрируют в состав создаваемых облачных платформ средства обеспечения безопасности и предоставляют интерфейсы для разработчиков средств защиты.

С другой стороны, поставщики облачных сервисов и приложений, расширяя свой бизнес, будут обращать больше внимания на повышение базового уровня безопасности своих облачных платформ и предоставление расширенных продуктов, призванных удовлетворять повышенным требованиям к безопасности заказчиков, готовых платить по повышенному чеку за дополнительное спокойствие.

Отраслевые регуляторы прикладывают в настоящее время много усилий, формируя нормативную базу и стандартизируя подходы, позволяющие потребителям и поставщикам облачных услуг эффективно взаимодействовать в юридическом поле распределения ответственности за вопросы безопасность. Существуют и активно применяются признанные международные стандарты, направленные на отражение требований безопасности к услугам «облачных вычислений» и связанных с ними продуктам.

Появление услуг безопасности, предоставляемых по модели «облачных вычислений» SecaaS так же будет способствовать росту доверия заказчиков к «облачным вычислениям» и решениям, построенным на их основе. В конечном итоге, возможно появление решений, полностью выносящих средства обеспечения безопасности из классической собственной инфраструктуры в «публичное» или «частное» облако, размещаемое в арендуемом датацентре.

Как один из примеров трансформации я бы привел появившиеся на рынке оперативные центры мониторинга и реагирования на инциденты информационной безопасности (Security Operation Center, SOC). Появившись несколько лет назад как чистый аутсорсинг безопасности, в настоящее время они превращаются в классические облачные продукты, дающие потребителям качество, готовность персонала, быстроту внедрения с минимальными затратами потребителей на инфраструктуру и капитальные вложения и подготовку сотрудников.