Тема информационной безопасности много лет поднимается при любых разговорах об облачных сервисах, хотя вендоры уже давно заявляют о техническом решении всех проблем с безопасностью в облаке.

?«ИКС»: Насколько сейчас актуальна для заказчиков проблема безопасности их данных в облаке? Требуют ли они от провайдера доказательств адекватной защиты?

Евгений ВЕЛЕСЕВИЧ, руководитель направления России и стран СНГ, Anaplan: Вопрос информационной безопасности «в облаках» долгое время сдерживал интенсивное развитие этого рынка в России – среди пользователей было распространено мнение о том, что любой шаг навстречу облакам (даже перенос электронной почты в облако) неминуемо ударит по информационной безопасности. Конечно, сегодня ситуация изменилась, но многие заказчики до сих пор воспринимают облачные сервисы, особенно публичные, как угрозу стабильности бизнес-процессов. Мы решаем эту проблему при помощи индивидуальной работы с каждым заказчиком по теме информационной безопасности. Кроме того, каждый год мы проходим множество security-аудитов у своих текущих и потенциальных клиентов, чтобы доказать, что предлагаемая нами система соответствуем самым серьезным требованиям в этой области.

Александр САМУХОВ, генеральный директор, BDC: В настоящее время ИТ-безопасность является одной из наиболее обсуждаемых тем, поэтому мы также очень интенсивно фокусируемся именно на этой сфере, ведь под нашим управлением работают 7 центров обработки и хранения данных. Мы развиваем и услуги защиты от DDoS-атак, предлагаем стандартизированные и уникальные услуги защиты ИТ для бизнеса. Кроме того, и в управляемых нами дата-центрах мы применяем специализированные решения в области безопасности. Клиенты все чаще сталкиваются с инцидентами в сфере безопасности информационных систем и начинают искать решение этой проблемы. Поэтому безопасность как услуга (SecaaS) приобретает все большую популярность. Мы предлагаем самые разные решения проблемы безопасности – от уникальных, разработанных для конкретного клиента, до стандартных, таких как Firewall нового поколения, антивирусные и фильтрующие программы (Antivirus, AntiSpam), WAF (Web Access Firewall).

Максим ЗАБЕЛИН, гендиректор, Max Support: Как правило в СМБ-секторе защищенность ИС в облаке выше нежели в on-premise системах. Хранение данных в нормальном дата-центре, на отказоустойчивых кластерах, с круглосуточным мониторингом, отлаженной системой резервного копирования и прочими enterprise- «плюшками», нельзя даже сравнивать по степени защищенности с «самосборным сервером» стоящим под столом у приходящего на 2 часа в неделю администратора.

Александр ВЕСЕЛОВ, начальник отдела технического консалтинга, «С-Терра СиЭсПи»: Использование многими компаниями облачных технологий привело к переходу от самостоятельного содержания инфраструктуры (в том числе обеспечения информационной безопасности) к привлечению для этой задачи сторонней организации. С одной стороны заказчику не нужно задумываться о проектировании и обслуживании системы и что-либо доделывать самостоятельно, с другой - полная передача собственной ИТ-инфраструктуры сторонней организации создает определенную зависимость от поставщика услуги, а также увеличивает опасность нарушения конфиденциальности, доступности и целостности информации. И если с физической безопасностью проблем практически нет: круглосуточная охрана, пропускной режим и т.д. организованы в каждом ЦОД, то с обеспечением безопасного удаленного доступа к данным могут возникнуть серьезные проблемы.

Ранее частой проблемой была недоступность сервиса вследствие, например, DDOS атаки. Сейчас на первый план выходит нарушение конфиденциальности и целостности при передаче данных между клиентом и ЦОД вследствие перехвата трафика. Обеспечить защиту от такого типа угроз можно с помощью шифрования трафика. Причем во многих случаях применение отечественной криптографии не просто желательно, а обязательно в соответствии с законодательством РФ. Российские разработчики уже имеют в своем арсенале сертифицированные регуляторами VPN-продукты, которые могут быть легко интегрированы в виртуальную среду (например, С-Терра Виртуальный шлюз). Они позволяют встроить VPN концентратор непосредственно в виртуальную среду и сделать услугу «безопасность как сервис» более полной. Именно так и поступают наиболее крупные операторы.

Применение сертифицированных продуктов позволяет заказчику быть уверенным в качестве средств защиты, но нужно иметь в виду, что обеспечение информационной безопасности может являться лицензированным видом деятельности и не все поставщики услуг являются таковыми. Важным этапом приемки системы у поставщика услуг является PEN тест (так называемый тест на проникновение), показывающий независимую оценку защищенности. Такая оценка для заказчика более объективна, чем «обещания защищенности» от поставщика.

Сергей ЕРИН, директор департамента информационных технологий, ЛанКей: Вопрос безопасности очень популярен у заказчиков. Заказчики выясняют у провайдера, где находится оборудование, как оно защищено, кто имеет доступ к данным, какая защита от DDoS-атак, … Касаемо популярности сервиса безопасности Security as a Service (SecaaS), здесь важно определиться с понятием. Ведь по сути антивирусы, установленные на наших компьютерах и серверах, являются SecaaS-услугой: мы получаем обновления антивирусных сигнатур «из облака», за которые платим деньги. То же самое касается и различных анти-спам серверов и серверов Web-фильтрации. Если смотреть в таком ключе, то SecaaS – услуга очень популярная. Но, если под Security as a Service понимать такие услуги, при котором ваш почтовый или веб-трафик проходит через серверы провайдера, где осуществляется его очистка, или аутсорсинговые защиты отDDoS-атак, или системы облачного шифрования данных – то такие услуги пока мало популярны. Тем не менее и этот рынок растёт.

Сергей ТАРАН, генеральный директор, «Онланта»: Обеспечение информационной безопасности (ИБ) – тема чрезвычайно актуальная для заказчиков. Какие гарантии заказчик может получить от провайдера? Одна из наиболее надежных – соответствие услуги набору стандартов и требований к обеспечению ИБ, начиная с ISO 27000 и заканчивая различными свидетельствами и сертификатами соответствия требованиям закона о защите банковской тайны, требованиям ФСТЭК по обеспечению безопасности конфиденциальной информации по разным классам.

Николай ДАНИЛКИН, начальник отдела инфраструктурной поддержки проектов, ОАО «Ростелеком»: Все программное обеспечение облачных услуг «Ростелеком» размещает на собственной ИТ-инфраструктуре, построенной с применением технологии виртуализации и расположенной в специально оборудованных и географически разнесенных ЦОДах на территории РФ, что обеспечивает высокий уровень надежности и безопасности сервисов, защиту информации, а также регулярное резервное копирование данных.

Максим БЕРЕЗИН, руководитель виртуального дата-центра, КРОК: Часто компании относятся настороженно к «облакам», думая, что они менее защищены во внешней среде, чем в собственном ЦОДе. Это один из наиболее распространенных стереотипов, который, мы надеемся, вскоре уйдет в прошлое. К счастью, многие заказчики сегодня отдают отчет, что работа с бизнес-системами «у себя» может быть не так надежна, как хотелось бы, из-за сбоев в работе корпоративного ЦОДа или действий инсайдеров. От таких рисков коммерческие дата-центры (если речь идет про крупных игроков, сертифицирующих своих площадки и сервисы информационной безопасности) защищены в большей степени. В нашей практике был пример, когда крупный финансовый заказчик, перенеся в наше «облако» часть своих ИТ-систем, аттестовал их на соответствие закону о персональных данных. Фактически это подтверждение того, что сегодня существуют механизмы для защищенного хранения данных в «облаке» в соответствии с требованиями регуляторов.

Ярослав ФАРОБИН, руководитель направления облачных сервисов и инфраструктурных решений, «Сервионика» (ГК «Ай-Теко»): Если говорить об информационной подкованности, то ИТ-специалисты с обеих сторон процесса облачной интеграции (провайдер-заказчик), прекрасно понимают, как все должно быть реализованно в идеале – но и из-за несовершенства законодательства, и из-за отсутствия некоторых сертифицированных компонентов в РФ реализация этого уровня крайне затруднена. Например, соответствовать закону «О персональных данных» крайне сложно: в одной из его статей написано – «...программно-аппаратный комплекс, обрабатывающий данные, не может быть предоставлен для нескольких заказчиков...». Мы можем сколько угодно понимать, что базы данных разных заказчиков разносятся на одном сервере так, что они никогда в жизни друг с другом никак не пересекутся, но законодательно это нигде не прописано: ставь, провайдер, два «железа». Так что здесь речь идет не о требованиях предоставить подтверждения способности обеспечить защиту, а о понимании возможностей ее обеспечить в соответствии с выдвигаемыми требованиями.

Алексей БЕССАРАБСКИЙ, руководитель отдела брендинга и PR, «Манго Телеком»: Конечно, защита данных, например, клиентской базы, хранящейся в облачной CRM, для заказчика важна. При этом мы не сталкиваемся с какими-то особыми требованиями. Мы обеспечиваем стандартный высокий уровень защиты данных, соответствующий требованиям российского законодательства. Для наших заказчиков – предприятий среднего и малого бизнеса – этого вполне достаточно. Надо отметить, что в СМБ большой процент случаев несанкционированного доступа связан с небрежностью самих пользователей – это применение слишком простых паролей, небрежное хранение регистрационных данных и т.п. Поэтому со стороны провайдеров необходимо активное информирование клиентов о «технике безопасности». Это не менее важно, чем технические меры.

Максим ЗАХАРЕНКО, генеральный директор, Облакотека: Клиенты с точки зрения отношения к теме безопасности все разные, но в целом, чем меньше компания, тем проще она относится к вопросам безопасности в облаке, понимая, что ничего подобного облаку у себя она обеспечить не сумеет. SecaaS внутри облака используется часто, а как внешний сервис для обеспечения безопасности облачной ИТ-инфраструктуры в офисе достаточно редко по причине консервативности ИБ-службы.

Андрей НИКОЛАЕВ, руководитель направления облачных решений, EMC в России и СНГ: Безопасность, безусловно, является критически важным фактором для корпоративных клиентов, и, во многих случаях, одной из ключевых причин, по которой облачные сервисы в корпоративном сегменте растут не так быстро.

Подготовила **Евгения Волынкина**