Ведущая темы
Лилия ПАВЛОВА

Дорожная

«Небезопасно» – вот главный аргумент компаний, не спешащих выводить свой бизнес на облачное шоссе. Но деликатность ситуации в том, что информационная безопасность облаков не существует сама по себе, она – неотъемлемая часть облачных сервисов. Иначе сказать, часть услуги, которую предоставляют облачные провайдеры.

Конфликт «услуги в услуге» не будет разрешен, пока провайдеры не ответят на десяток конкретных вопросов служб информационной безопасности предприятий, пока к обсуждению проектов нормативно-правовых актов не подключится профессиональное сообщество, пока не будет создана цепочка доверия...

Между тем рынок облачных сервисов год от года прирастает объемами, новыми игроками, решениями, услугами, проектами – и с ним растет актуальность обеспечения ИБ в облаках. Что было, что есть, что будет в облачной информационной безопасности? К обсуждению этих вопросов с энтузиазмом подключились многочисленные эксперты, и с их помощью нам удалось сформировать «дорожную карту». Подход к ее составлению вполне соответствует принципам традиционного дорожного картирования. Во-первых, проведена ревизия изучаемого объекта с указанием узких мест, угроз и перспектив развития (что принципиально важно, анализ проделан на основе многоаспектного экспертного обсуждения). Во-вторых, в карте просматриваются не только вероятные сценарии развития объекта, но и их потенциальная рентабельность, что позволяет определить оптимальные пути с точки зрения ресурсной затратности и экономической эффективности. В-третьих, карта сопровождается четырьмя пакетами рекомендаций для субъектов рынка, аффилированных с объектом.

Итак, карту в руки и – в путь?

карта облачной безопасности

фокус

Бетонный блок на облачном шоссе

Перспективы растущего в разы российского рынка облачных услуг аналитики оценивают оптимистично. Так, согласно IDC, в прошлом году его объем составил $90 млн, в нынешнем удвоится, а в следующем достигнет $360 млн. Две трети этих денег ($60 млн) принадлежат частным облакам и гибридным, а оставшиеся $30 млн – очень скромная по меркам национального рынка сумма – публичным облакам. Это соотношение, вероятно, сохранится и в ближайшие годы при общем росте рынка.

Общим местом стало утверждение (оно подтверждается многочисленными исследованиями и опросами), что главный тормоз российского рынка облачных услуг – сомнения потенциальных пользователей в достаточном уровне информационной безопасности в облачных моделях. Недавно на одной из «облачных» конференций инфобезопасность была названа «большим бетонным блоком на облачном шоссе, который приходится постоянно объезжать». К слову, опрос «ИКС», в котором приняли участие 25 экспертов, показал, что этот «бетонный блок» имеет мало общего с технологическими проблемами, он скорее сложился из неготовности нормативно-правовой базы к урегулированию отношений между участниками рынка, из отсутствия необходимых требований и четких стандартов. И, пожалуй, блок «в головах» – в «частнособственнической психологии». В обоих случаях должно пройти какое-то время, чтобы и правовую базу получить, и менталитет сменить.

Раскручивают маховик облачного рынка три основные силы – разработчики решений, системные интеграторы, провайдеры облачных услуг (порой все три «в одном юрлице»), они же и заинтересованы в преодолении пресловутого «бетонного блока». Что, кстати, хорошо иллюстрирует состав экспертов «ИКС» – огромную заинтересованность проявили представители этой «тройки» (чего никак не скажешь о заказчиках облачных услуг), причем драйверы рынка продемонстрировали конструктивность в критике друг друга.

Кто готов к защите облаков?

По большому счету, готовность большинства участников рынка к защите облаков до сих пор далека от идеала, признают эксперты, но степень ее для каждой из трех сторон оценивают по-разному. Например, А. Гарусев (CDNvideo) считает, что сейчас наиболее готовы именно сервис-провайдеры, поскольку для провайдера нарушение требований безопасности – это огромный репутационный риск, который может обернуться даже выходом из бизнеса. Ни одна другая сторона не мотивирована в такой степени, считает эксперт, отмечая также, что у серьезных провайдеров все аспекты деятельности максимально автоматизированы, все находится под двойным и тройным перекрестным контролем специальных программно-аппаратных комплексов. В то же время, полагают другие эксперты, провайдеры не готовы брать на себя ответственность и давать гарантии сохранности переданной им информации и доступности оказываемых услуг. Они также не стремятся раскрывать свои внутренние процессы по организации информационной безопасности, что тормозит подключение к их услугам крупных компаний.

Так может, первую скрипку играют вендоры? По мнению ряда экспертов, именно они задают тон на рынке, поскольку все остальные участники пользуются конкретными решениями и им крайне сложно сформировать какую-либо свою систему без участия вендора. А. Колыбельников («Микротест») отмечает, что обеспечение

безопасности в облаках – еще только зарождающийся сегмент рынка и соответственно зарождающийся новый класс решений. Поэтому все ориентируются на крупнейших международных вендоров и все ожидают готовых решений именно от них. Разумеется, и у этой позиции есть свои недостатки. Например, далеко не все вендоры в области инфобезопасности имеют отработанную схему предоставления своих решений в облаке, что связано в первую очередь с нежеланием менять систему продаж.

Что касается системных интеграторов, то они действуют в основном на площадке частных облаков. Поскольку публичные облака предоставляют сервисы, рассчитанные на массового потребителя или небольшие организации, которые не особо озабочены вопросами информационной безопасности, они, по словам А. Бондаренко (LETA), не слишком интересны крупным интеграторам или поставщикам программно-аппаратных решений. А вот в области безопасности для частных облаков именно интеграторов часть экспертов считает «коренными в тройке», поскольку большинство вендоров работают через партнеров, которые, в свою очередь, взаимодействуют с клиентами и хорошо представляют себе их потребности – текущие и будущие. При этом, отмечает Д. Митрофанов («Ай-Теко»), в силу большей гибкости в развитии бизнеса в сравнении с крупными производителями интеграторы создают собственные облачные решения, восполняя нехватку таковых у вендоров. В итоге, по мнению эксперта, большой проблемой рынка облачной инфобезопасности (для «частников») можно назвать отсутствие комплексного предложения, удовлетворяющего все запросы клиентов: каждый из трех игроков держит в руках свой «кусочек пазла». Что же касается публичных облаков, то уровень их информационной безопасности В. Алеев («Ситроникс») называет неудовлетворительным. Исключения составляют государственные услуги, размещаемые в облаках компаний – агентов правительства и отвечающие законодательным требованиям по защите данных пользователей (граждан и организаций), уточняет эксперт.

Такая двойственность позиции каждой группы участников во многом объясняется отсутствием опоры в виде решений регулятора, который, по словам В. Андреева (ИВК), должен выступать гарантом облачной безопасности, проработав основные ее вопросы (как это уже сделано для традиционной информационной безопасности), выпустив необходимые руководящие документы (регламенты, стандарты и пр.), а также удостоверившись в том, что конкретная реализация облака (частного, гибридного, публичного) отвечает этим документам. При этом, как замечает Д. Матиев (IBS Platformix), хотя российские регуляторы (ФСБ и ФСТЭК) обещают разработать нормативные требования по защите облачных сред, без широкого обсуждения с бизнесом эти требования могут оказаться оторванными от действительности. Кроме того, беспокойство у участников рынка вызывает неопределенность сроков выхода нормативных документов. Остается лишь надеяться, что они не заставят себя ждать несколько лет.

В поисках опоры

Вообще говоря, законодательство отстает от технологий по всем позициям в отрасли телеком – ИТ – медиа, и сегмент инфобезопасности – не исключение. Причем не только у нас, но и во всем мире. Проблема, по мнению Д. Матиева, состоит в том, что на локальных рынках отсутствуют требования к защите облачных технологий, в то время как многие компании взяли курс на инновации (сюда причисляются и облачные технологии, и виртуализация). Это означает высокие риски использования новых технологий. В то же время в отставании нормативно-правовой базы от жизни есть и свои плюсы – возможность без помех установить де-факто стандарты, подходы и принципы применения технологий, которые впоследствии будут законодательно закреплены. Как заметил А. Колыбельников, документ, регулирующий безопасность облака, нужен – но нужно также понимать, что подобные документы разрабатываются после того, как была внедрена новая технология (такова мировая практика), невозможно действовать на опережение.

А сейчас, по мнению экспертов, опорой могут служить стандарты и рекомендации по обеспечению информационной безопасности в облачных средах. Их разработано немало. Одним из самых респектабельных можно назвать набор документов Cloud Security Alliance (CSA). Д. Безкоровайный (Trend Micro) отмечает, что во всем мире лучшие практики CSA уже используются как отправная точка для клиентов и облачных провайдеров, задумывающихся об обеспечении ИБ. Сейчас эта организация ведет активную работу с ISO для расширения более общих стандартов ISO 2700x и включения в них вопросов, касающихся безопасности в облаке. Опираясь на серию ISO 27000, можно уже сейчас построить полноценную систему инфобезопасности и управления ею как для провайдеров облачных услуг, так и для их клиентов, считают эксперты. Кроме того, рекомендации по обеспечению безопасности облаков изложены в документах ряда организаций – ISACA, ENISA, BSI, в стандартах NIST.

Дальнейшее развитие стандартов будет идти по двум направлениям: для технологий (например, предписывающие стандарты самого верхнего уровня, обеспечивающие интеграцию для SOA) и для провайдеров (оценочные стандарты деятельности организации). Кроме того, сейчас разрабатываются международные стандарты инфобезопасности для облачных вычислений и модели SaaS, выход первых версий которых ожидается в 2013 г. По мнению Д. Безкоровайного, в разработке единого стандарта ИБ для всех сфер применения

Безопасная миграция в облако
Конспект «дорожной карты»

1. Сервисы коммуникаций
2. Медиа
3. Сервисы услуг
4. Сервисы планирования и контроля проектов
5. Сервисы обмена знаниями по проектам
6. Сервисы предоставления контента по теме
7. Бизнес-приложения.

Источник: *рекомендации экспертов по данным опроса «ИКС»*

облачных вычислений нет необходимости, поскольку задачи и обрабатываемые данные в облаках могут существенно отличаться; клиенты и провайдеры сами должны выбирать необходимые требования к защите данных, исходя из их критичности, важности обеспечения их целостности и доступности.

Д. Митрофанов считает, что нам нужны стандарты, учитывающие и российскую специфику, и лучшие мировые практики, и требования законодательства. Разрабатывать их должны крупные и авторитетные объединения компаний, центры компетенций, отраслевое лобби. В. Медведев («Доктор Веб») уверен, что не хватает не стандарта по обеспечению безопасности — не хватает общедоступных методик и процедур работы (аналога процедур ITIL); не хватает специалистов на местах, имеющих высокую квалификацию, достаточную для обеспечения безопасности клиентов; не хватает, наконец, некоего сертифицирующего органа — добровольной организации, сертификат которой гарантировал бы клиенту качество услуги. Тем не менее появление специализированного стандарта позволит унифицировать принципы и подходы к защите облаков, а также устранит терминологическую путаницу в понятиях, которая всегда имеет место при появлении новых технологий, уверен М. Башлыков (КРОК). В поддержку этого мнения А.Санин (Avanpost) отмечает, что к настоящему времени в облачной безопасности уже накоплена база знаний, которую требуется структурировать, иначе она станет тормозом дальнейшего развития.

IaaS, PaaS, SaaS: специфика спроса и безопасности

Чем крупнее заказчик, тем выше у него требования к обеспечению отказоустойчивости облачной среды – это аксиома. И если в публичном облаке невозможно (в рамках существующей нормативно-правовой базы) организовать аттестацию соответствующей автоматизированной системы, то придется строить частное облако – корпоративный ЦОД. Так поступает крупный бизнес.

Следующий шаг – переход к модели IaaS, представляющей собой логичное расширение ЦОДа, где уже выстроены системы ИБ, освоены ролевые модели управления доступом и политики безопасности, внедрены системы аутентификации (все чаще – с аппаратными ключами), электронной подписи и проч. По мнению В. Медведева, крупные компании фактически уже стали «облачными», только обслуживанием облака занимается внутреннее подразделение, а не провайдер услуг. К слову, для многих таких компаний логичен следующий шаг – выделение ИТ-подразделения во внешнюю структуру и превращение его в провайдера облачных услуг.

Предприятия же SMB, перед которыми чаще всего стоят задачи быстрого и гибкого реагирования на новые потребности для развития бизнеса и снижения непроизводительных расходов, предпочитают модель SaaS, когда стартовые инвестиции минимальны, нет необходимости в содержании собственного ИТ-отдела и практически вся забота о безопасности ложится на плечи провайдера. При использовании публичных облачных сервисов главная задача SMB состоит в защите данных от конкурентов в течение сравнительно небольшого промежутка времени, пока эти данные актуальны.

Наконец, специфика государственных компаний – регулирование их деятельности различными ГОСТами и предписаниями, которые нередко сложно реализовать в рамках облачных структур, особенно если организация имеет дело с гостайной. Этим, по мнению экспертов, и объясняется гораздо более низкий уровень информатизации «определенных ведомственных

Составляем SLA

При заключении договора с поставщиком облачных услуг прописываются:

1. Администраторская часть, связанная с разграничением прав доступа к сервису, с наличием неких контрольных точек, благодаря которым можно будет делать независимый срез по ИБ.

2. Система взаимных согласований, уведомлений о любых изменениях информации, важной с точки зрения безопасности.

3. Действия на случай несоблюдения трех правил инфобезопасности (целостность услуг, доступность услуг, конфиденциальность информации клиента).

4. Шифрование каналов.

5. Уровень доступности услуг.

6. Политика резервного хранения данных.

7. Время восстановления после сбоев.

8. Полная анонимизация пользователей и сервисов: у каждого сервиса должен быть свой логин, непохожий на другие распространенные.

9. Свой набор логинов контрагентов с непересекающимися связями (чтобы «по внешним связям не отследить идентичность внутреннего пользователя»).

10. Доступ через анонимизирующие прокси типа сети tor.

11. Обязанность провайдера обеспечить взаимодействие с клиентами в случае расследования инцидентов и защита систем в облаке от собственных сотрудников.

12. При смене провайдера – меры по обеспечению сохранности данных, сферы ответственности, параметры восстановления систем и доступа к данным.

13. Быстрый разрыв по инициативе клиента без каких-либо санкций и безусловный возврат всех клиентских данных с гарантией удаления из СХД провайдера.

Источник: *рекомендации экспертов по данным опроса «ИКС»*

структур» в сравнении с крупными коммерческими компаниями, для которых нет таких ограничений. Тем не менее с точки зрения инфобезопасности крупные компании и госструктуры роднят повышенные требования к стабильности, пропускной способности и скорости обработки больших объемов данных. Ф. Гриценко («Ай-Теко») отмечает, что поставщики облачных сервисов, предоставляемых госструктурам и крупному бизнесу, должны иметь сертификаты соответствия в основном оценочным стандартам – ISO 27001, SAS 70, PCI DSS, Cobit. Для ИТ-сервисов, предоставляемых через Интернет с использованием шифровальных средств, в ряде случаев требуются и лицензии ФСБ, сертификация средств защиты ФСТЭК. Аттестация информационных систем на соответствие определенному уровню информационной безопасности обязательна для систем обработки и передачи данных, составляющих коммерческую или государственную тайну.

Надо сказать, что с созданием национального облака О7 госструктуры становятся полноценными участниками рынка: электронное правительство должно базироваться на облачной платформе (будь то приложения, платформа или инфраструктура). По мнению С. Щербины (Esri CIS), многие ключевые направления развития государственных ИТ очень органично ложатся в облако (например, СМЭВ). Кроме того, облака способны существенно приблизить реализацию идей стандартизации подходов и технологий ведомственных ИТ-систем, дать доступ к прикладным сервисам и данным пользователям на всех уровнях (федеральном, региональном, муниципальном), считает эксперт.

Таким образом, специфика безопасности для трех облачных моделей обусловлена уровнем контроля над элементами облачной инфраструктуры (к слову, самой непопулярной, по данным IDC, у нас оказалась модель PaaS с 4% общего объема рынка – против 58% у SaaS и 38% у IaaS). Предложенное Д. Матиевым распределение ответственности выглядит следующим образом:

✓**SaaS:** пользователь – 1% (конфиденциальность аутентификационных данных), провайдер – 99% (обеспечение всех уровней защиты);

✓**PaaS:** пользователь – 20% (защита приложения), провайдер – 80% (защита инфраструктуры и платформ);

✓**IaaS:** пользователь – 80% (защита приложений и платформ), провайдер – 20% (защита инфраструктуры).

Другими словами, в SaaS пользователь несет ответственность только за данные, загружаемые в облако, причем за их сохранность тоже отвечает провайдер. Именно поэтому эксперты, считающие провайдеров наиболее готовыми обеспечить защиту в облаках, полагают, что модель SaaS отличается большим уровнем безопасности, нежели PaaS и IaaS, поскольку практически снимается угроза нарушений со стороны пользователей. Однако сама компания, как правило, не имеет никакой возможности повлиять на перечень мер для обеспечения безопасности платформы – это и отталкивает крупные организации, привыкшие полностью контролировать инфраструктуру. При этом, отмечают эксперты, в модели SaaS обеспечить надежную и гарантированную защиту информации при использовании публичных облачных услуг может сильная посредническая организация, которая берет на себя функции регулятора в отношениях поставщиков и получателей услуг и обеспечивает безопасный информационный обмен. Например, в США такой организацией является Global Service Administration. В России аналогичные функции, будучи оператором электронного правительства, взял на себя «Ростелеком» .

Непопулярность PaaS, которая представляет собой основу для миграции в облака не данных, но приложений, эксперты объясняют сложностью четкого разграничения рисков ИБ, поскольку в такой системе возникает два типа контроля доступа: пользователь – приложение (обеспечивается пользователем) и приложение – сервер приложений (обеспечивается провайдером).

Модель IaaS дает клиенту наибольшую свободу: компания может сама выбирать и контролировать серверы, сетевое оборудование, операционные системы, средства виртуализации, прикладные программы. Но обеспечение безопасности в этом случае также ложится на плечи клиента, точнее, на его ИТ-службу, от профессионализма и грамотности которой и будет зависеть уровень защиты. Провайдер заботится лишь о функционировании, надежности и доступности сервисов, которые пользователь сам себе обеспечивает. При этом оператор, предоставляющий IaaS-услугу, обычно не имеет возможности контролировать даль-

В персональном ракурсе

Моя любимая рубрика – «Персона номера». Встреча с героем – всегда радость и испытание одновременно, ведь заранее не знаешь, о чем человек захочет рассказать побольше, о чем – умолчать, в каком формате потом потребуется делать публикацию (интервью, монолог, авторское повествование, сочетание того, другого, третьего). Но каждый раз такая беседа – открытие: какие же замечательные люди рядом! Яркие, умные, тонкие, глубокие, неординарные – и очень разные.

Эту рубрику мы затеяли в конце 90-х, когда еще не был на слуху слоган «Бизнес – это люди», не было в проекте справочников «Кто есть кто» в телекоме и Интернете… Просто здравый смысл подсказал, что читателям будет интересно и полезно узнать друг о друге побольше – как правило, они пересекаются в профессиональной среде, но вопросы о смысле жизни, кулинарных предпочтениях или ярких впечатлениях детства вряд ли обсуждают. Случалось, что даже члены семей наших «персон номера» передавали редакции благодарность: оказывается, по прочтении по-новому увидели своих домочадцев.

Сейчас в активе рубрики более 150 героев – руководители отрасли разных времен и ученые, бизнес-лидеры и талантливые технари. Одна беда: вечно не хватает журнальной площадки, трудно уложиться в отведенные две полосы, каждая история тянет на книжицу… Но что радует – неиссякаем этот источник!

Лилия ПАВЛОВА,
обозреватель ИКС,
член Союза российских писателей

нейшие действия подписчика, который устанавливает или настраивает дополнительные программные компоненты.

Таким образом, подходы к обеспечению безопасности в разных облачных моделях весьма различны. При этом эксперты подчеркивают: требования безопасности в них не должны отличаться. Как отметил В. Медведев, по сути все три модели описывают лишь разный уровень доступа администраторов клиентов к предоставляемым ресурсам, но кто бы ни отвечал за те или иные части услуги (виртуальную машину, операционную систему, действующий на базе ОС сервис и др.), требования, предъявляемые к безопасности, в общем не отличаются. Разница состоит лишь в том, кто должен реализовывать те или иные меры безопасности.

Вы еще не в облаке?..

Скромность объемов облачного рынка и прогнозы лавинообразного роста говорят о том, что многие компании в ближайшие годы выйдут на это шоссе. «Дорожная карта», составленная усилиями экспертов «ИКС», не претендует на полноту, однако содержит весьма полезные советы. Прежде чем обратиться к облачным сервисам, эксперты рекомендуют оценить все риски, понять степень важности информации, вложенной в облако, и создать модель угроз, которая будет отражать объективное положение дел. Исходя уже из этих компонентов, следует принимать решение о составе системы защиты.

Разумеется, задачи обеспечения безопасности облачных сервисов сильно разнятся в зависимости от того, какова их модель облачных вычислений. Как отмечает Д. Безкоровайный, рисков безопасности огромное количество, причем множество из них не являются техническими – привязка к инфраструктуре провайдера и невозможность перехода к другому в случае изменения условий, риск перепродажи (oversell) провайдером своих мощностей и, как следствие, ухудшение качества услуг и влияние на доступность сервиса, невыполнение требований законодательства по защите данных и многое другое. Эти и другие риски хорошо описаны в таких документах, как Cloud Computing Security Risk Assessment от ENISA и Top Threats to Cloud Computing от Cloud Security Alliance, к которым советует обратиться эксперт. Кроме того, в рамках CSA сформирована рабочая группа по вопросам SLA (Service Level Agreement), и в ближайшее время ожидается выпуск рекомендаций для клиентов и на эту тему.

Наши эксперты, со своей стороны, предлагают рекомендации не только по составлению SLA, но и по переходу на облачные модели, а также по миграции сервисов в облако. Конечно, следует учесть, что разные модели облака предусматривают и разные подходы к миграции. Например, при формировании частного облака с моделью IaaS основной уклон сделан в сторону формирования высокодоступного, отказоустойчивого и производительного ЦОДа. В этом случае переносятся в первую очередь информационные сервисы организации (почта, бухгалтерия и пр.). Важно также провести аудит информационных ресурсов организации на предмет необходимости (целесообразности) миграции унаследованных приложений в облако. Кроме того, во многом очередность зависит от отрасли. Тем не менее опыт экспертов позволяет сформулировать рекомендации, применимые для разных компаний, независимо от отраслей и объемов их деятельности.

Хочется верить, что общие усилия пригодятся в деле сдвигания «бетонной плиты». ИКС

Практикум облачной безопасности

Илья ТРИФАЛЕНКОВ, начальник отдела информационной безопасности «Ростелекома»

О специфике облачной безопасности. В дополнительной защите, связанной со спецификой облачных вычислений, нуждаются, несомненно, системы управления. С нашей точки зрения, к ним должны предъявляться наиболее жесткие требования и применяться полный набор механизмов защиты в соответствии с моделью угроз.

Из трех моделей предоставления облачных сервисов наиболее высокий уровень безопасности – в SaaS, поскольку именно в этой модели реализовано разделение администрирования на прикладном и инфраструктурном уровне, возможность предоставления услуги заданного SLA, разделение зон ответственности оператора и пользователя.

О защите виртуальных сред. Легкость разворачивания виртуальных ресурсов часто приводит к тому, что с ними обращаются гораздо менее ответственно, чем с реальными. Это касается, например, размещения резервных копий виртуальных машин в открытом виде и в доступных местах. Специфические риски виртуализации, связанные с атакой на гипервизор, рассматриваются скорее теоретически, реальных случаев ущерба от таких атак не зафиксировано. Тут такая же ситуация, что и с криптографией: проверки идут на устойчивость алгоритмов, а потери – от элементарной кражи ключей.

О специфике спроса. Крупные коммерческие компании и госструктуры не работают в публичных облаках, скорее – в гибридных. Специфика в том, что коммерческие компании прежде всего защищают коммерческую тайну, а государственные – персональные данные. Из этого следуют несколько разные подходы к этапности работ и набору механизмов защиты.

О специфике рисков. Что касается рисков облачной модели, то это риски, связанные с оператором, и риски, связанные с другими пользователями облачных услуг. Необходимо заметить, что наличие дополнительных типов рисков не обязательно ведет к усилению интегральных рисков, поскольку в облачной архитектуре типовые риски могут быть существенно снижены. Условием этого является четкое распределение зон ответственности оператора и пользователя, отражение в SLA максимально конкретных требований и метрик безопасности.

Об использовании облачных сервисов от разных провайдеров. Целесообразность работы с несколькими провайдерами сомнительна и требует обоснования – ведь при построении корпоративных систем никто, как правило, не стремится использовать конкурирующие решения одной и той же задачи. Провайдеры таких сложных услуг по определению должны быть достаточно крупными организациями с опытом работы на рынке, так что риск, связанный с неспособностью оператора обеспечить услугу, минимален. А проблемы при использовании нескольких провайдеров велики.

О миграции сервисов. Начинать нужно с тех сервисов, применение которых обеспечивает больший экономический эффект. При этом основная проблема – договориться с оператором о параметрах SLA, особенно если до этого они в корпоративной среде не специфицировались, а воспринимались умозрительно, в терминах «чтобы все работало».

Об ответственности и рисках потребителя. Есть элементы, которые в любом варианте остаются на стороне пользователя. Это терминалы в том или ином виде. Можно организовать мощный набор механизмов защиты, который будет бесполезен, если на клиентской стороне не контролируется, кто и как получает доступ к терминальным устройствам.

О балансе между инфобезопасностью и комфортом пользования. Разумный баланс обеспечивается на основе анализа рисков. Общих рекомендаций тут не существует, поскольку все сильно зависит от того, какая информация и в каких целях обрабатывается. Средства защиты мобильных приложений быстро развиваются, и уже сейчас есть вполне эффективный инструментарий. Хотелось бы при этом заметить, что далеко не со всеми приложениями удобно работать с мобильных устройств, так что проблема хотя и актуальная для ряда случаев, но вряд ли определяющая.

О готовности рынка. На сегодняшний день есть набор вендорских решений инфобезопасности как отечественного, так и неотечественного производства. И даже есть сертифицированные решения. Роль системных интеграторов в связи с распространением облачных технологий сейчас не меняется: они выполняют привычные для них функции. Единственно, при широком внедрении облачных технологий количество заказчиков падает, поэтому заинтересованность интеграторов невелика. Операторы за прошлый год сделали огромный шаг к созданию реальных облачных сервисов, а пользователи начали осознавать свою выгоду. Тем не менее этот путь и тем и другим еще предстоит пройти. ИКС

Движение на трех уровнях

Основой для облачной инфобезопасности должны стать документы трех уровней: международные стандарты, национальные нормативно-правовые акты, низкоуровневые рекомендации для компаний. В какой стадии их разработка?

Дмитрий КОСТРОВ,
главный эксперт
КЦ компании МТС,
ассоциированный
репортер ИК 17 МСЭ-Т

Дорога открыта

Все решения по безопасности облачных вычислений опираются в основном на международный опыт – специальной группы ИК 17 МСЭ-Т, американского института стандартов NIST, объединения Cloud Security Alliance. В этих организациях схожий подход к разработке стандартов и рекомендаций – открытость, привлечение широкого круга специалистов. NIST выложил драфт документов на сайт – и любой специалист может ознакомиться с проектом, внести свои предложения.

В Cloud Security Alliance эксперты со всего мира на добровольных началах работают над проектами рекомендаций по обеспечению безопасности при использовании облачных вычислений – и более того, по использованию облачных вычислений

За синергию!

В двадцать лет человек смотрит на мир жадным взглядом первооткрывателя, ему кажется, что все самое лучшее, что может и должно с ним случиться: встречи, открытия и обретения, – впереди.

Двадцатилетие для журнала – возраст зрелости, повод оглянуться назад, на пройденный путь и вспомнить все его крутые повороты и наводящие на раздумья развилки. На всем его протяжении курс ИКСа полностью совпадал с вектором, определяющим направление движения молодого и растущего рынка связи: со сменой технологий или лидеров рынка, с формированием его новых сегментов, с поиском новых источников доходов и переоценкой уже имеющихся.

На пороге двадцатилетия ИКСа его небольшой творческий редакционный коллектив по-юношески пытливо и пристрастно вглядывается в будущее расширяющей свои границы отрасли, с азартом комментирует возникновение и столкновение тенденций, тщательно анализирует позитивные и негативные факторы, словом, разворачивает перед читателем многокрасочную картину ее развития.

Хочется верить в то, что так будет и впредь, как и в то, что вопреки мировым пессимистическим прогнозам читательская аудитория журнала ИКС будет прирастать тысячами посетителей портала www.iksmedia.ru, и синергии «бумажной» и «электронной» версий хватит еще не на один юбилей.

Александра КРЫЛОВА, обозреватель ИКС

при обеспечении безопасности. Каждая отдельная классическая система защиты (управление устройствами, шифрование, IDPS, межсетевое экранирование, антивирус) разворачивается под облачную проблематику, и над каждой системой работают эксперты.

МСЭ активно работает с ISO с целью расширения более общих стандартов управления безопасностью серии 2700x и включения в них вопросов, касающихся безопасности в облаке, а также отраслевой специфики. В этом процессе участвуют все члены союза. К примеру, опираясь на ISO 2700x, Япония разработала специальный стандарт для телекоммуникационных компаний – на мой взгляд, очень адекватный документ.

Видимость нулевая

Нормативно-техническая база облачной безопасности создается с привлечением широких кругов профессиональной общественности, чего не скажешь о базе нормативно-правовой. Сейчас российские регуляторы в области информационной безопасности разрабатывают документ для облачных вычислений. Но проект его закрыт для обсуждения профессиональным сообществом. Если есть драфт – почему бы не разослать его министерствам, научным институтам, различным компаниям отрасли безопасности и тем, кто будет эти облака создавать (ИТ-компаниям, телеком-операторам), почему бы не собрать и не проанализировать предложения, чтобы принять работающий документ? Но этого нет. Зато есть опасение, что результат окажется «для галочки» – слишком общим, который нельзя будет применять в работе. К слову, у нас и так очень много документов, которые либо мешают работать, либо существуют «для галочки». Я не верю, что замкнутая группа даже хороших специалистов может подготовить документ, пригодный для работы всех участников рынка. Даже если дельные предложения от них не были бы приняты (как произошло с поправками в ФЗ-152), участники рынка хотя бы понимали, к чему им готовиться. Сейчас можно лишь предполагать, что документ разрабатывается под облако «Ростелекома».

ПДД пишем сами

Что касается провайдеров облачных услуг, то, поскольку они работают непосредственно с клиентами, им требуются низкоуровневые рекомендации по процедурам, которые необходимо внедрять в компании. МТС пока не предоставляет облачные услуги безопасности, однако наработки в рамках подхода MSSP ведутся и в этом направлении. К слову, например вышла рекомендация Банка России, по которому банковский сектор начал предъявлять новые требования к операторам связи, начиная с представления документов о внешнем и внутреннем аудите безопасности при заключении договора на предоставление доступа в сеть для ДБО. Мы продумали наши риски и готовы предложить банкам не только наши линии защиты, но даже услуги безопасности. Раньше банки воспринимали оператора исключительно как «трубу». Теперь мы должны защищать их от фишинга, от DDoS-атак, от взломов, вирусов и спама при ДБО. Это для нас совершенно новый тренд, новые риски. Совмещение этого тренда с облаками потребует проработать еще целый ряд сложных вопросов – от составления SLA с участием трех сторон «цепочки стоимости» до сложнореализуемых задач, связанных с выполнением требований ФЗ-152, нового закона о «черных списках», с защитой от DDoS-атак и др.

Если говорить о телеком-специфике безопасности для частного пользователя, то здесь можно выделить два направления. Во-первых, это BYOD, «продвинутость» сотрудников, их присутствие в социальных сетях (а это ведь всё облака). Это явление можно патронировать, но запретить нельзя (в отличие, скажем, от банковской сферы). Поэтому для защиты корпоративных данных в новые устройства сотрудников встраивается «песочница безопасности», в корпоративном магазине приложений размещены только проверенные программы. Сейчас рассматриваются и планируются к внедрению специализированные продукты, в рамках MDM, и это новая услуга внутри корпорации. В случае потери устройства корпоративные данные не будут утеряны, а само устройство можно без труда найти, даже если оно будет перепродано.

Второе направление – услуги безопасности для сторонних пользователей. Защиту данных на устройстве и контроль устройства как услугу внедрили компании Vodafon, Orange, T-Mobile, и она хорошо востребована предприятиями SMB, которые не имеют возможности, в отличие от Enterprise, обеспечить такое управление самостоятельно. ИКС

Приглашение к ревизии

Александр САНИН,
коммерческий директор
Avanpost

С точки зрения ИТ-процессов тенденция перехода в облака оправдана и понятна, однако в ракурсе информационной безопасности далеко не все так однозначно. Облачные вычисления ведут к пересмотру привычных для нее понятий и представлений о процессах.

Что осталось на корабле современности

Очень важное обстоятельство, которое до сих пор мешает большинству специалистов по информационной безопасности принять облака как данность, как что-то потенциально хорошее и нужное, – изменение понятия «периметр защиты». Именно периметр защиты традиционно считался базовым понятием с четким определением, и именно отталкиваясь от него большинство компаний выстраивали свои системы защиты информации. В облаках же классическое определение неприменимо: периметр защиты размыт и, что еще более важно, он контролируем лишь частично. Это сразу вызывает настороженность у специалистов по инфобезопасности. Но, несомненно, со временем придется пересматривать сложившиеся взгляды, включая даже такие привычные термины. К слову, в новой парадигме физические границы периметра все же поддаются описанию, ведь у каждого облака есть свой «облачный периметр» – он начинается в той точке, где в ЦОД приходит кабель интернет-провайдера.

Понятие «информационная безопасность» подразумевает множество процессов. Если же говорить только о технической составляющей – средствах и системах, которые обеспечивают безопасность в ИТ-среде, – то для любой среднестатистической службы информационной безопасности основные процессы – это управление доступом, антивирусная и антиспам-защита, защита от внешних угроз и вторжений, межсетевое экранирование и резервирование. Можно перечислить еще ряд элементов, но эти шесть ключевых процессов применимы абсолютно во всех организациях, и переход в облако должен в первую очередь обеспечить специалисту по инфобезопасности их приемлемый уровень. Облако должно иметь технические компоненты защиты от вирусов, троянов и прочих подобных угроз; оно должно быть надежно защищено от внешних атак, таких как DDoS; должно иметь средства межсетевой защиты и средства резервирования и восстановления после аварий. И мы видим, что все эти процессы в современных облаках уже давно перестали быть чем-то новым, все перечисленные системы существуют и успешно функционируют, и заказчику при выборе того или иного облачного сервиса наверняка предложат подписать соответствующий SLA, где будут указаны подробности о каждом из компонентов. Но что современное облако может предложить нам с точки зрения управления доступом? Тут мы видим некоторый вакуум...

Доступ насущный

Из связанных с защитой элементов инфраструктуры вопросов, которые сейчас «стоят ребром», в первую очередь всех очень волнует вопрос управления доступом. Кто кроме меня имеет доступ к сервису? Кто обслуживает его работу? Есть ли возможность получить доступ к моим данным у других участников облака? Другими словами, необходимо продумать такие модели этой подсистемы безопасности, которые вызывали бы у заказчиков доверие. Сейчас очень активно прибегают к различным принципам разделения виртуальной инфраструктуры, но они применимы далеко не всегда, и далеко не каждый провайдер идет на это.

Между тем любой современный и эффективный процесс управления доступом неразрывно связан с решениями IDM (Identity Management). Именно IDM-решения в настоящее время способны автоматизировать большую часть ручной работы в рамках управления доступом. Любое такое решение за счет интеграции с кадровой базой данных организации делает процедуру согласования и предоставления доступа тому или иному лицу полностью автоматизированной и прозрачной. Более того, по результатам тестов, проведенных компанией Avanpost, процесс предоставления доступа ускоряется на порядок, т. е. время предоставления доступа, а также время отзыва прав доступа сокращается минимум в 10–15 раз. Как же процесс управления доступом должен видоизмениться с учетом текущих тенденций «облачности»?

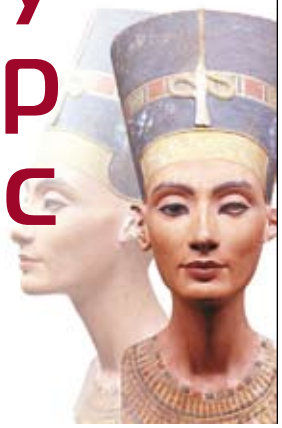
Управление доступом ...aaS

В принципе даже классическое представление процесса управления доступом отчасти вписывается в облачную модель. Например, при использовании IaaS

(Infrastructure as a Service) заказчик может, как и раньше, самостоятельно контролировать и предоставлять доступ даже в облачной среде, с одной лишь оговоркой: он не может достоверно сказать, что список лиц, которым предоставлен доступ, – это окончательный вариант, поскольку существует еще обслуживающий персонал самого облака (тут уже вопрос доверия к провайдеру и тоже, к слову, переосмысления основных понятий ИБ), могут появиться внутренние нарушители и т.п. В целом же процессом управления доступом полностью распоряжается заказчик. Варианты появляются в других моделях. В модели PaaS (Platform as a Service) или SaaS (Software as a Service) говорить о классической схеме уже не приходится. Чтобы автоматизировать управление доступом в облачном сервисе, построенном по такому принципу, нужно искать новые подходы.

Один из новых вариантов – автоматизация процесса управления доступом таким образом, чтобы его можно было предоставлять пользователям тоже в виде сервиса, эдакого IDMaaS. При этом подходе пользователь фактически будет иметь доступ к IDM-решению, которое, в свою очередь, будет настроено на управление доступом ко всем нужным ему бизнес-приложениям, и платить за такой сервис нужно будет по принципу модели SaaS. Технологически такой сервис уже сегодня вполне можно запустить, вопрос лишь в согласовании с провайдерами облаков. Более того, технологически можно добиться интеграции сервиса с облаком до такой степени, чтобы пользователь мог управлять доступом даже к тем бизнес-приложениям, которые находятся вне этого облака (например, у него в офисе или даже в другом облаке). ИКС

ракурс



Разрушение мифа

По данным опроса, проведенного «Лабораторией Касперского»*, 59% компаний-респондентов уже используют или планируют в ближайшие 12 месяцев внедрить серверную виртуализацию. При этом 53% опрошенных считают, что риски ИТ-безопасности для виртуальной среды ниже, чем для физической. Однако на практике повышенная устойчивость виртуальных машин к вредоносному воздействию – не более чем миф.

Владимир УДАЛОВ, руководитель направления корпоративных продуктов в странах развивающихся рынков «Лаборатории Касперского»

Виртуальная среда, как и физические машины, подвержена большинству традиционных киберугроз. Более того, появляются дополнительные риски, поскольку заражение одной виртуальной машины (ВМ) представляет собой угрозу для всей виртуальной среды. А значит, инциденты безопасности могут обернуться куда более серьезными последствиями. Например, одна зараженная

Специфика рисков в виртуальных средах

- Возможность несанкционированного доступа к гипервизору
- Невозможность защиты средствами ОС от угроз уровня гипервизора
- Крайне ограниченный набор средств защиты в виртуальной среде, сертифицированных по требованиям ФСБ и ФСТЭК
- Возможность потери виртуальной машины
- Отсутствие механизмов физической защиты данных при доступе к серверам
- Отсутствие защиты и фильтрации передачи данных между виртуальными машинами в локальной сети и в рамках одного физического сервера, на котором они работают.

Источник: *опрос «ИКС»*

* Опрос проводился в 2012 г. среди компаний, компьютерные сети которых насчитывают 100 и более рабочих станций.

Проблема или возможность развития бизнеса?

Виртуализация десктопов и приложений обеспечивает централизованное хранение и управление приложениями и данными. Сейчас это направление дополняется комплексными сетевыми решениями, повышающими уровень информационной безопасности виртуальной инфраструктуры заказчика. Однако сегодня все больше приложений разрабатывается на основе web, облаков и мобильных платформ – и у бизнеса возникает потребность в контроле за этими разнообразными программными продуктами.

Частные и гибридные облака по умолчанию обладают более высоким уровнем безопасности, чем публичные (и мы считаем, что подавляющее большинство инвестиций в облака в течение ближайших пяти лет пойдет именно туда). Но публичные сервисы, в том числе мобильные, будут распространяться среди пользователей, которые станут требовать от своих ИТ-служб использования этих сервисов и на работе. Это непростая задача – создать в гибридных и частных облаках хотя бы примерно такое же удобство услуг, такой же их ассортимент, что и в публичных облаках, сохранив при этом уровень безопасности.

Для ИТ-служб это проблема, для вендоров – возможность развития бизнеса. А локомотивом процесса, который будет вести нас к развитию облачного рынка в целом, выступят конечные пользователи.

Том ФЛИНК, вице-президент по глобальному сотрудничеству с партнерами и расширению рынка, Citrix

виртуальная машина может использоваться для распространения вредоносных программ и перехвата трафика других машин.

Подходов к обеспечению защиты виртуальных сред несколько, и здесь важно сделать правильный выбор, трезво оценивая не только их преимущества, но и подводные камни. Например, во многих организациях внедряют традиционные защитные решения, требующие установки антивирусных агентов, что означает установку полной копии антивирусного ПО на каждую ВМ. Хотя такое решение обеспечивает надежную защиту, развертывание на хост-сервере избыточных средств для обеспечения безопасности обходится дорого. Установка антивирусного ядра и сигнатурных баз на каждую машину требует избыточных ресурсов памяти, дискового пространства и процессора хост-сервера. Как следствие, снижается производительность. Таким образом, практически сводится на

Хранение данных: курс на централизацию

Переход к облачным сервисам – это элемент стратегии консолидации хранения и обработки корпоративных данных. В этой стратегии особую роль играет виртуализация рабочих мест.

Александр ГЕРАСИМОВ, директор по маркетингу компании «Ай Ко»

По самым скромным оценкам, хранимая и обрабатываемая локально слабоструктурированная информация составляет не менее 80% объема всех корпоративных данных. Но точный ее объем просто невозможно оценить; пожалуй, в реальности это все 90–95%. А ведь это данные, критически важные для деятельности предприятия или организации.

Эта ситуация напрямую определяет низкую степень защищенности корпоративных данных, ведь при прочих равных обеспечить защиту централизованных (консолидированных) данных намного проще и дешевле, нежели хранимых локально на рабочих местах. Очевидно, что сейчас от 80 до 95% корпоративных данных либо недостаточно защищены, либо вообще не имеют защиты. Более того, «локальная» информация привязана не просто к конкретному сотруднику (недоступна для других), но к конкретному пользовательскому оборудованию сотрудника (недоступна для него же с других устройств).

С организационной точки зрения для решения этой проблемы необходимо отказаться от локального хранения и обработки всех видов корпоративных данных и изменить подход к организации труда персонала. А технологически решение заключается в виртуализации рабочих мест по технологии «нулевой клиент» (ультратонкий клиент).

Нулевой клиент – это устройство, работающее по протоколу PCoverIP, используемое только для подключения устройств отображения и ввода (монитор, клавиатура, мышь) и лишенное локального хранилища (жесткий диск, флеш-накопитель и т.п.). На нем также отсутствует операционная система и не исполняется ПО. В отличие от тонкого клиента нулевой клиент позволяет реализовать 100%-ную виртуализацию рабочего места. На физическом рабочем месте необходимы только средства отображения и ввода, системный блок заменяет «коробочка» нулевого клиента. Данные вообще не покидают пределов ЦОДа, по сети передаются только сжатые и зашифрованные описания пикселов.

Поскольку консолидация локально хранимых данных потребует радикального увеличения емкости систем хранения ЦОДа, необходимо также использование гибких и масштабируемых СХД, позволяющих оптимальным образом хранить очень большие объемы слабоструктурированных данных различных видов.

12 правил защиты в виртуальной среде

1. **Определите угрозы и соответствующие им механизмы защиты** на следующих уровнях виртуальной среды: аппаратная платформа, системное ПО виртуализации (гипервизор), система управления виртуальной средой, виртуальные машины, СХД с размещаемыми образами виртуальных машин и данными.
2. **Применяйте специализированные системы защиты** виртуальных рабочих станций и серверов, учитывающие модель потребления ресурсов.
3. **Используйте средства контроля доступа к системе управления** виртуальной инфраструктурой и к конфигурациям.
4. **Применяйте двухфакторную аутентификацию,** интегрированную с имеющимися службами каталогов.
5. **Установите и поддерживайте разделение прав и зон ответственности** администраторов виртуальной среды.
6. Тщательно **выберите и поддерживайте перечень прав,** которые предоставляются администраторам гипервизоров, особенно тем, кто имеет физический доступ к системам.
7. **Используйте возможности повышения защиты,** которые предоставляет вендор (или вендоры) вашей виртуальной среды в части доступа к разделяемым физическим ресурсам, особенно сетевым портам.
8. **Реализуйте сервисный подход к инфраструктурной защите с использованием безагентских технологий** (антивирусная защита, контроль сетевых взаимодействий и обнаружение вторжений, контроль целостности).
9. **Управляйте событиями ИБ** в виртуальной среде и отслеживайте их корреляцию с событиями в общей инфраструктуре.
10. Тщательно **отслеживайте все события в сети,** которые могут привести к нарушениям защиты (например, появление нового узла или клиента). Ведите подробные журналы событий и используйте средства автоматизированного анализа для выявления событий, содержащих потенциальные угрозы инфобезопасности.
11. **Используйте виртуальные шлюзы безопасности,** анализирующие трафик между виртуальными машинами внутри одного гипервизора.
12. **Следите, чтобы уровень защиты информации сохранялся** при внесении изменений (модернизация системы, переход на новые версии гипервизора и средств виртуализации, перенос виртуальной машины на новый физический сервер, перенос приложения на новую виртуальную машину). Для этого необходимы внутренний процесс, регламентирующий конфигурирование и изменения виртуальной среды, а также внутренний или внешний аудит безопасности эксплуатируемой виртуальной среды.

Источник: *рекомендации экспертов по данным опроса «ИКС»*

нет одно из основных преимуществ виртуализации (ради которого компании на нее и переходят) – эффективное использование аппаратных ресурсов. Кроме того, такие явления, как «шквальное сканирование» или «шквальное обновление» (одновременный запуск проверки или обновления сигнатурных баз сразу на нескольких ВМ, расположенных на одном физическом хост-сервере), могут не только существенно замедлить работу хост-сервера, но и привести к его аварийной остановке.

Существуют и решения, пока еще немногочисленные, созданные специально для защиты виртуальных сред. Это так называемые virtual appliances – виртуальные устройства безопасности. Такое устройство обеспечивает антивирусной защитой несколько ВМ; другими словами, антивирус работает на уровне гипервизора. Перенос функции антивирусной защиты с отдельных ВМ на специально выделенное устройство безопасности существенно снижает расходование системных ресурсов, повышает производительность аппаратного обеспечения и увеличивает плотность ВМ на хост-сервере.

Но наряду с неоспоримыми преимуществами такие решения имеют и ряд недостатков. Во-первых, многие из них обеспечивают только базовую защиту. Используемое в таком случае антивирусное ядро должно быть лучшим из доступных на рынке, чтобы компенсировать отсутствие средств многоуровневой защиты. Во-вторых, ИТ-специалисты компаний, внедривших виртуализацию, должны будут впредь поддерживать защиту как физической, так и виртуальной инфраструктуры. И порой для этого приходится использовать несколько консолей управления, что удваивает нагрузку на администраторов и увеличивает расходы.

Вместе с тем на рынке уже появляются современные специализированные решения, избавленные от этих недостатков. Они обеспечивают надежную защиту, не снижая рентабельность виртуализации и не приводя к потере ее преимуществ. Например, создатели нового решения Kaspersky Security для виртуальных сред целенаправленно работали над тем, чтобы обеспечить оптимальный баланс безопасности и производительности ВМ и дать возможность управлять защитой виртуальных и физических сред посредством единой консоли.

Возвращаясь к исследованию, приходится констатировать: к сожалению, пока только 11% из опрошенных компаний используют специализированные решения для защиты виртуальных сред. Но хорошая новость состоит в том, что 25% уже планируют начать их использовать. Миф рушится. ИКС

проекты

Теперь нет классического подхода к информационной безопасности

Артем ПЛЕТНЕВ

Так считает Артем ПЛЕТНЕВ, операционный директор по ИТ ГК «Рольф», завершившей «ровно в половине двенадцатого» (в конце июня 2012 г.) перенос в гибридное облако HP приложений, ранее работавших на 200 серверах в корпоративном ЦОДе холдинга.

– Как повлиял на выбор облачной модели размер компании? И в чем специфика обеспечения инфобезопасности для этой модели?

– Наша компания пошла по пути гибридного облака именно потому, что размер уже не позволяет нам пользоваться стандартными услугами публичного облака – необходим точечный, система за системой, подход к построению облачных сервисов. Отсюда гибридное сочетание моделей SaaS, PaaS, IaaS. Перенос нашей ИТ-инфраструктуры в гибридное облако HP стал первым и пока что единственным успешно завершенным проектом такого масштаба во всей России. Процесс миграции приложений и услуг занял около шести месяцев, и сейчас система безопасности HP и внутренние процессы работают безупречно. С точки зрения ИБ мы руководствовались корпоративными требованиями: прежде всего важно понимать, что защищать и от кого, а также максимально соответствовать требованиям российского законодательства.

– Основными сдерживающими факторами при переходе предприятий на публичные облачные сервисы аналитики называют сомнения в надежности хранения персональной и финансовой информации, нежелание впасть в зависимость от провайдера облачных услуг, опасения снижения доступности сервисов или нарушения функциональности, необходимость внесения изменений в корпоративные инструкции... Оказались ли какие-то из этих страхов мифами, развеять которые поможет опыт вашей компании?

– Согласен, что при использовании публичных облаков непонимание того, где находятся ваши данные, порождает сомнение в их безопасности. Поэтому в нашем случае идею публичных облаков сразу отвергли. Если говорить про опасения, связанные с доступностью, функциональностью и т.д., то, на мой взгляд, 2/3 времени непосредственно перед запуском проекта необходимо потратить на проверку и тестирование систем в облаке всеми имеющимися средствами, потому что потом, уже в боевом режиме, очень трудно, а порой и невозможно в разумное время вернуть все назад. В этом смысле есть определенная зависимость от провайдера, но опять-таки все должно быть тщательно проверено до промышленного запуска. Все остальное регулируется договорными отношениями и вашим профессионализмом. Доверяйте компаниям не по лозунгам, а по реальному опыту и отзывам, тогда не будет зависимости и опасений.

– Как вы считаете, с каких сервисов лучше начинать переход в публичное облако и на каком этапе перехода неизбежно участие системного интегратора?

– Я бы предложил начать с самого «простого», например с электронной почты. Это классический пример об-

лачного SaaS-сервиса, тем более что рынок по этому сервису уже стал конкурентным, а это позволяет попробовать разные решения и сравнить их. Для обслуживания нашего холдинга в ЦОДе HP применяются и физические серверы, на которых работают «тяжелые» приложения (такие как SAP, Oracle), и виртуальные серверы, используемые для остальных приложений и для тестирования. Отказоустойчивая архитектура каналов данных обеспечила бесперебойный доступ к услугам и приложениям, перенесенным в облако. Среди них система Microsoft Exchange, услуги которой сейчас предоставляются по модели SaaS, а также ERP-системы SAP и «1С». Дальнейшие планы развития этого проекта предполагают перевод на модель PaaS баз данных Microsoft SQL Server, Oracle и некоторых других приложений.

К системным же интеграторам я пока отношусь осторожно и рекомендовал бы начать с компаний, которые непосредственно разрабатывают такие технологии и инструменты. Российский рынок в этом вопросе еще молод, и интеграторам надо накопить опыт.

> «Классический» подход к безопасности, когда мы закрываем внешний периметр и считаем, что компания защищена, сегодня уже не действует

– Какие участки должен обезопасить сам пользователь облачных сервисов?

– Прежде всего это разделение ответственности. Сегодня «классический» подход к безопасности, когда мы закрываем внешний периметр и считаем, что компания защищена, уже не действует. Убедившись в полной безопасности, которую гарантирует облачный провайдер, поняв механизмы защиты каналов связи провайдера, можно полностью сконцентрироваться на конечных рабочих местах, с которых выполняется ввод данных, получение отчетности, печать, и эффективно построить их защиту – это должен сделать сам пользователь облачных сервисов.

– Как минимизировать риски при использовании облачных приложений от разных провайдеров? Каковы ваши пожелания вендорам решений инфобезопасности, системным интеграторам, провайдерам?

– На мой взгляд, облачный провайдер должен быть один, и он максимально полно настраивает системы безопасности под себя. Защитить все и вся невозможно, здесь нужен подход, при котором максимальное количество проблем вы можете устранить минимальными усилиями. Не надо стараться объять необъятное, важно понять, провести всесторонний анализ и действовать направленно, только это дает эффект. Самая лучшая система безопасности – та, которую знают досконально. Есть реальные примеры, когда хорошая система безопасности негативно влияла на производительность бизнеса только по причине неквалифицированной настройки и тестирования.

– Каких «подводных камней» при переходе к облачной модели предоставления услуг можно избежать, какие есть «пути отступления» в случае нарушения трех правил ИБ (конфиденциальность, целостность, доступность)? Какие пункты необходимо отразить в SLA? Что бы вы порекомендовали компаниям, идущим «в облака» вслед за вами?

– Прежде всего надо понимать нормы законодательства, потому что это первое препятствие на пути к облакам (взять хотя бы требования по защите персональных данных). Второе: три правила нарушать нельзя ни при каких условиях, исключений быть не должно, нужно сделать все, чтобы конфиденциальность была соблюдена, целостность контролировалась, а доступность была подтверждена процедурами по работе с информацией. Сделать это несложно, но надо понимать, что кроется за этими терминами, у каждой компании свои подходы и требования. В нашем случае зоны ответственности HP и «Рольф» разграничены, права доступа к приложениям и данным жестко определены, а получившаяся инфраструктура соответствует требованиям текущей редакции 152-ФЗ. В конце каждого отчетного периода «Рольф» получает детализированные счета за использованные ИТ-ресурсы гибридного облака с указанием всех задействованных систем, емкости систем хранения и резервного копирования, а также количества почтовых ящиков. Кроме того, провайдер каждый месяц предоставляет нам отчет по выполнению SLA. Кстати, благодаря этому проекту мы смогли вывести из эксплуатации устаревшее оборудование серверов и систем хранения и освободить помещение, которое прежде занимал корпоративный ЦОД, для расширения бизнеса.

– Доступность ИТ-приложений везде, где есть подключение к Интернету, в том числе с мобильных устройств сотрудников – это и безусловное удобство, и дополнительные риски публичных облачных услуг. Как найти разумный баланс между безопасностью и комфортом пользования?

– Доступность приложений из Интернета существовала и до облаков, и здесь ничего не изменилось. Есть проверенные средства защиты и разумный подход: а нужен ли этот доступ извне? То же самое касается и мобильных устройств. Но сегодня я не готов широко использовать мобильный доступ, так что баланса пока нет, есть крен в сторону безопасности: на мой взгляд, открывать корпоративную сеть для доступа со всех мобильных устройств пока рано! ИКС

Чего не впишешь в документ

Эксперты «ИКС» предлагают свои рекомендации по переходу в облака.

Вдумчиво и очень тщательно выбирайте поставщика облачного сервиса.

«Проработав какое-то время с определенным сервис-провайдером, вам будет очень сложно его сменить; информацию не всегда легко переконвертировать в формат другого сервис-провайдера (как правило, это просто невозможно). Идеально, если сервис-провайдер предоставляет возможность выгрузки/бэкапирования всей информации, а также возможность развертывания собственной локальной версии – по сути, частного облака» (*А. Бондаренко, LETA*).

Если поставщик услуг предоставляет выбор между обычным подключением к сервису и **использованием защищенных каналов связи** (VPN, SSL), выбирать следует второй вариант. Если в локальной сети зачастую достаточно шифровать пароли, но не сами данные, то при удаленных подключениях шифровать необходимо практически все.

«Разумеется, обеспечение надежности, отказоустойчивости, сохранности данных – это ответственность поставщика, однако многие системы дают возможность пользователям, к примеру, экспортировать базу клиентов. Поэтому дополнительные меры для создания резервных копий, которые пользователь может принять самостоятельно, будут совсем не лишними» (*А. Разумов, Check Point Software Technologies*).

30

Если вы планируете использовать сервис для обработки данных кредитных карт, необходимо предварительно убедиться, что **сервис-провайдер соответствует требованиям международных стандартов PCI DSS и PA DSS**. Если мы говорим об отечественном законодательстве, в первую очередь о законе «О персональных данных», то здесь все еще сложнее, так как по формальным признакам практически ни один облачный сервис сегодня не может полностью отвечать требованиям законодательства в силу их чрезмерной жесткости.

«Некоторые провайдеры заявляют, что они соответствуют, но это, мягко говоря, лукавство» (*А. Бондаренко, LETA*).

В случае облачных сервисов в SLA зачастую **действуют три стороны:** заказчик, поставщик облачных сервисов и интернет-провайдер.

«Банальное отключение Интернета по вине магистрального оператора может сделать работу с облачными ресурсами невозможной в принципе, поэтому жесткие условия ответственности в соглашениях с поставщиками — обязательные элементы безопасности в облаках (*Н. Никитович, Группа Optima*).

При переносе части ИТ-сервисов в облако можно рекомендовать те же дополнительные действия, которые необходимы для обеспечения безопасности при открытии удаленных офисов, подключаемых через Интернет: **защита сетевого периметра, контроль за правами доступа к локальным и удаленным ресурсам, сегментация локальной вычислительной сети**. Если в процессе использования облачного сервиса обнаруживается его небезопасность, то следует немедленно прекратить работу с ним и потребовать от провайдера вернуть хранимые данные.

«Наиболее распространенные облачные сервисы могут быть развернуты локально за сравнительно короткое время. Ограничивающим фактором в этом случае является наличие бюджета для приобретения оборудования, лицензий на ПО и, возможно, найма дополнительного персонала. К такому повороту событий нужно быть готовым как финансово, так и юридически» (*В. Алеев, «Ситроникс»*). ИКС

Обратной дороги нет

Алексей ЛУКАЦКИЙ,
бизнес-консультант по безопасности Cisco Systems

Если компания перешла в облака, обратного пути уже нет, – это подтверждает опыт компании Cisco, переведшей функционирование офиса в облачную среду.

До прихода в Cisco я работал в российской компании – интеграторе информационной безопасности, где был запрещен удаленный (тем более мобильный) доступ к информации и приложениям, размещенным внутри локальной сети. Об облаках тогда никто не думал (да и сейчас мало кто из российских ИБ-компаний пользуется облачными сервисами). Придя в Cisco, я поразился тому, что у сотрудников не было стационарного компьютера, только лэптопы, и никто не заставлял приходить в офис и сидеть за столом с 9 до 6. Принцип «офис там, где работа, а не работа там, где офис» здесь был реализован чуть ли не с самого основания компании.

Уже давно в Cisco был заложен подход Web 2.0 – все построено на интернет-технологиях. Компания никогда не называла его частным облаком, хотя в современной терминологии это оно и есть, только появилось больше десяти лет назад. И безопасность подстраивалась под такие условия труда, оснащая лэптопы сотрудников соответствующими техническими решениями, прозрачными для пользователей, но обеспечивающими нужный уровень безопасности (заметим, что 70% этих решений было разработано здесь же).

Потом компания перешла на доступ с мобильных устройств, а спустя всего год или два разрешила сотрудникам использовать собственные устройства – задолго до появления термина BYOD. Как это удалось? Основной акцент был сделан не на технологиях (их на рынке в избытке), а на работе с пользователями. Регулярное обучение, пилотные проекты, тестирование на продвинутых пользователях, выслушивание мнений сотрудников, приоритет бизнеса над безопасностью... Все это позволило не только найти баланс между комфортом и безопасностью использования мобильного доступа, но и тесно интегрировать первое со вторым.

Сейчас некоторые сервисы переданы на аутсорсинг внешнему облачному провайдеру, но это не повлекло за собой серьезных проблем – культура работы с такими сервисами в компании внедрена уже давно. Риски снижения доступности мы, конечно, оценивали, но этот риск не сильно отличается от того, что было ранее. При этом мы проработали соответствующий SLA и договор с облачными провайдерами, а также разработали целый ряд контролирующих мер, которые позволяют надеяться, что эти риски никогда для нас не наступят.

Компаниям, которые еще только собираются в дорогу, советую твердо усвоить: никакого отступления после перехода к облакам быть не может. Облака и выбирают для того, чтобы сэкономить на инфраструктуре, приложениях, оборудовании. Если пользователь от всего этого отказывается и переносит свои данные и приложения в облака, то вернуться обратно очень затруднительно, это похоже на построение новой инфраструктуры. И хотя пользователь услуг публичного облака ничего не может в нем обезопасить (если он не пользуется IaaS или PaaS, где у него есть некоторая свобода действий), он может и должен контролировать облачного провайдера. Для этого надо полностью пересмотреть деятельность своей службы инфобезопасности, которая должна уже не сама что-то защищать, а следить, как это делает другая компания. Это требует не просто пересмотра всех принципов, но и выбора новых технических решений, а также привлечения юристов, которые будут прорабатывать договоры с облачными провайдерами именно в контексте ответственности и гарантий по вопросам безопасности. ИКС

Лицо-голос вместо логина-пароля

Михаил ГОТАЛЬСКИЙ,
руководитель TrueConf

В контексте движения Интернета от текстового к мультимедийному формату – с использованием облачных технологий – меняются, порой на грани фантастики, и формы защиты от угроз.

С самого рождения Интернет прошел долгий путь от сугубо текстового средства общения до царства мультимедийных технологий. Сегодня он снова меняется – рождается новое лицо компьютерной связи. Его характерная черта – мультимедийные технологии, технологии видеоконференцсвязи, и во многом – облачные. А это обуславливает ИБ-специфику нового этапа.

Развитие технологий унифицированных коммуникаций ведет к тому, что уже скоро мы сможем использовать в качестве ВКС-терминала любое устройство, находящееся под рукой и обладающее достаточной производительностью и выходом в сеть. На смену распространенным touch-интерфейсам для управления мобильными устройствами придет эпоха управления жестами и голо-

сом. Корпоративный клиент откажется от «тяжеловесного» аппаратного оборудования и обратится к арендной практике, одалживая мощности из облака, позволяющего связать пользователей любых ВКС-систем.

Очевидно, отойдут в прошлое и «логины с паролями». Сейчас любого пользователя компьютер идентифицирует по «текстовой метке» – логин при входе в компьютер, адрес при доступе к электронной почте и т. д., а пароль просто подтверждает компьютеру, что по ту сторону экрана находится именно тот пользователь, за которого он себя выдает. Но для ВКС совершенно естественным идентификатором вместо логина могут стать лицо и голос – гораздо более уникальные признаки, чем логин или ник, помогающие идентифицировать человека в реальной жизни.

Безопасность и ВКС

Проблема уязвимостей, связанных со способом доступа к ресурсу, упирается в финансирование: чем лучше канал связи, тем больше проверок и защит он «потянет», однако проблема целесообразности трат часто приводит к использованию «старых добрых» текстовых шифров и протоколов, по сути своей «дырявых». Это сугубо технологическая угроза, которая есть и будет, она не зависит от сервиса или места его размещения. Если протокол дыряв и уязвим, то уязвим он и в облаках, и в корпоративной сети, и в персональном использовании.

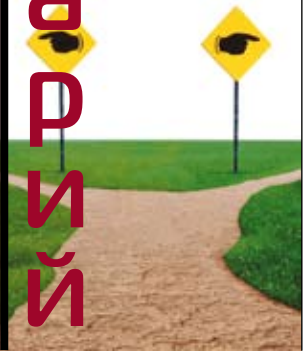
Даже в защищенных корпоративных сетях сложность полноценной интеграции систем ВКС вынуждает специалистов и интеграторов выносить их за защищенный периметр. Многим известен эксперимент г-на Мура, начальника службы безопасности в Rapid7, который решил проверить на прочность корпоративную защиту и с помощью системы ВКС смог заглянуть в офисы, конференц-залы и переговорные комнаты более десятка компаний. Причина возникновения «дыры» в системе безопасности заключалась, конечно, и в небрежности пользователей, оставивших включенной функцию автоответа и автотрансляции видео, но и в осознанном выносе используемой ВКС-системы за пределы безопасного периметра.

Аналогичная ситуация бывает и у частных пользователей облачных ВКС. Когда клиентское приложение начинает «тормозить», многие закрывают «ненужные» программы: отключают антивирус и протокол шифрования данных.

В отличие от корпоративных сетей, в которых существуют «доверенные соединения из локальной сети», в облаках отсутствует локальная сеть, потому любые соединения внутри системы остаются недоверенными. В тот момент, когда пользователь подключается к облачному серверу, на том же сервере вполне может находиться злоумышленник, взламывающий доступ администратора, а следом – и всех пользователей сервера.

Облачный сервис – всегда коллективный, и уязвимости одного пользователя могут распространиться и на всех остальных. К примеру, если в видеоконференции, осуществляемой через облако, из пятерых участников двое используют суперзащищенный канал, двое – обычный, а один – очень слабый и совсем без защиты (допустим, тот же 3G с телефона), то характеристика «очень слабый и совсем без защиты» относится ко всем пятерым участникам. В чем-то облачные сервисы подобны проходному двору, и во избежание неприятных последствий, пока для авторизации используются не индивидуальные особенности пользователя (лицо и речь), а логин – пароль – ключ шифрования, стоит менять их почаще. ИКС

Сценарий



Цепочка доверия

Чтобы защитить информационное облако, необходимо доверять каждому компоненту и каждой связи, фактически создать цепочку доверия. Выстроить такую систему безопасности в глобальном масштабе сложно, но в национальном – вполне реально, уверен Ренат ЮСУПОВ, старший вице-президент Kraftway.

Ренат ЮСУПОВ

– Согласны ли Вы с утверждением, что вопросы безопасности в частном облаке в принципе решены?

– С точки зрения защиты ЦОДа – согласен. Но гарантий защиты клиента нет ни в частном, ни в гибридном, ни в публичном облаке. Включая компьютер, пользователь обычно не задумывается о процессах, которые запускаются в этот момент: стартовые микропрограммы-загрузчики инициализируют устройства, пространство памяти, запускают необходимые драйверы, а после передают управление операционной системе. Эту работу традиционно выполняет микрокод BIOS (basic input/output system – базовая система ввода-вывода). Физически BIOS расположен в энергонезависимой памяти клиента. А клиент, как известно, самый незащищенный

Люди-генераторы

Во главе любого дела – люди, которые сначала генерируют идею, потом ее воплощают и впоследствии развивают. Может случиться, что основными участниками трех этапов окажутся разные люди, такова жизнь.

Генераторами идеи ИКСа стали Юрий Борисович Зубарев и Галина Монина. Идею создать издание для зарождающегося в 1992 г. рынка связи удалось воплотить как благодаря личным качествам организаторов, так и в силу сформировавшейся в отрасли потребности в таком СМИ. Тогда были затеяны рубрики, которые впоследствии трансформировались в тематические подборки.

А сегодняшнее лицо журнала, а теперь и портала, Наталия Кий, создала блестящий прецедент преемственности: под ее руководством ИКС стал не только информационным рупором, но и уважаемой аналитической площадкой отрасли. Сама Н. Кий – удивительная личность. Уже стало традицией, открывая журнал, первым делом читать ее мудрую передовицу.

И еще одно лицо, воплощающее и развивающее идеи, – мой давний редактор и обозреватель этого журнала Лилия Павлова. Пользуясь случаем, хочу выразить ей глубокую благодарность за поддержку и квалифицированную помощь.

Поздравляю с юбилеем журнал! С его коллективом работать мне нравится.

Марк КРИВОШЕЕВ, почетный председатель ИК-6 МСЭ-Р, главный научный сотрудник ФГУП НИИР, докт. техн. наук

субъект потребительского рынка вообще и его ИТ-сегмента в частности, включая и облачную инфраструктуру. Свидетельство тому – появление в спектре вредоносных программ нового класса, который способен взять контроль над устройством через уровень BIOS. Угрозы подобного типа практически неуловимы и, что самое печальное, неизлечимы. Переломить ситуацию удастся только при системном подходе к безопасности облаков, не ограничиваясь защитой ЦОДов, но обеспечивая защиту клиентов через доверенный BIOS. Концептуально это выражается в выстраивании цепочки доверия без выпадающих звеньев.

– Принцип создания доверенных систем существует достаточно давно. Что нового в цепочке доверия?

– Все построенные раньше средства безопасности обеспечивали лишь фрагментарную защиту отдельных компонентов и звеньев системы. В традиционной парадигме доверенных систем либо каждое средство безопасности работало на поиск и уничтожение уже реализованных угроз, либо всегда существовала возможность обхода этой системы. Цепочка же доверия обеспечивает превентивную защиту. Если все участки системы доверенные, если существует внутренняя система подтверждения каждого этапа и компонента на соответствие, то никакие угрозы в рамках модели внедрения вредоносного кода в систему не страшны. Крупные ИТ-компании сейчас выстраивают свои системы безопасности на этой новой модели защиты. Однако превентивная модель требует серьезных вложений и усилий, ведь каждое звено цепочки доверия должно разрабатываться, производиться и эксплуатироваться доверенной организацией. Иначе говоря, разработчикам приложений надо договориться об участии в цепочке с производителями операционных систем, а тем, в свою очередь, с производителями средств вычислительной техники, далее по цепочке – с разработчиками BIOS, с производителями процессоров, чипсетов, микроконтроллеров, и всем вместе взятым – с разработчиками средств безопасности. Когда это удастся, можно будет говорить если не о промышленной революции, то о коренном изменении принципов работы всемирной ИТ-индустрии – о переходе от простой стыковки интерфейсов обмена к стыковке интерфейсов безопасности.

– С кем из потенциальных участников цепочки доверия труднее всего договориться?

– Сейчас большая часть материнских плат выпускается в Китае, Тайване и т.п., где типовые BIOS адаптируются под конкретные платы, и никто, кроме их производителей, не знает, какой конкретно микрокод имплементирован в их базовую систему ввода-вывода. Исходные коды эти многочисленные компании вряд ли захотят открыть. Недавно в России была введена процедура проверки BIOS в лабораториях, аккредитованных ФСБ, но, не зная исходных кодов, проверить в двоичном коде, даже после декомпиляции, программу объемом 2 Мбайт, тесно связанную с аппаратным обеспечением, еще можно, а вот в 256 Мбайт (новый стандарт BIOS, стартующий в 2013 г.) – жизни не хватит. А в запасе остается еще возможность маскировки микрокода BIOS под безобидные функции, проверки теряют свою эффективность.

– Выход есть?

– Мы решили, что для России единственный способ создать доверенный BIOS – разрабатывать его здесь. Что мы и начали делать, лицензировав типовые исходные коды у компании AMI. С другой стороны, поскольку это аппаратно-зависимое ПО, создать доверенный BIOS практически невозможно, не будучи разработчиком аппаратуры. Соответственно, мы занимаемся разработкой материнских плат, в которые встраивается базовая система ввода-вывода собственной же разработки.

Следующий шаг – создание «оболочки безопасности» Secure Shell, позволяющей решить проблему контроля бинарных модулей различных контроллеров, присутствующих в прошивке. Собирая исходный код BIOS, мы обеспечиваем контроль их работы. BIOS де-факто получается доверенный, поскольку модули других производителей повредить ему уже не могут. «Оболочка безопасности» BIOS обладает еще одним важным свойством – в нее можно интегрировать модули защиты информации других компаний: всевозможные модули доверенной загрузки, модули шифрования, межсетевые экраны, антивирусы и даже доверенные гипервизоры. Мы сотрудничаем уже почти с десятком крупных компаний, работающих в сфере ИБ, по интеграции их продуктов в нашу оболочку. Таким образом, мы создали несколько

звеньев цепочки доверия нижнего уровня. На процессоры не замахиваемся, но до кремния мы пока дошли. В результате удалось на порядок увеличить безопасность и защищенность клиентских рабочих мест. Положа руку на сердце, могу сказать, что создана устойчивая безопасная система, способная блокировать угрозы нового поколения, которые еще называют кибероружием.

– Национальная цепочка доверия программно-аппаратного уровня уже находит практическое применение?

– Первое решение этой серии сейчас реализуется в медицинских проектах. В наш BIOS встроен модуль доверенной загрузки – электронный замок одного из наших партнеров. Пока он не взломан (профессионалы из ИБ-лаборатории «Бауманки» полтора-два месяца пытались взломать – не смогли). Если при аутентификации пользователя произойдет некоторое заданное количество неправильных вводов кода, система блокируется. Восстановить систему сможет администратор безопасности. Если же такую ошибку совершит администратор, то единственный способ восстановить работу – привозить машину к нам на завод, выпаивать микросхему, «прошивать» ее заново. С одной стороны, это плохо: возникают дополнительные трудности. С другой – хорошо, взломать систему невозможно.

Это решение внедрено и технологически отрабатывается в 11 регионах в рамках проектов модернизации здравоохранения. Часть действующих в регионе лечебных учреждений оснащается клиентскими рабочими местами с нашими решениями. Средства идентификации и аутентификации, встроенные в BIOS, пока гарантируют 100%-ную невзламываемость системы «электронной регистратуры» и «электронной истории болезни» нарушителем со стороны клиентских рабочих мест. Но система безопасности, эксплуатирующаяся в медицинских проектах, – это еще не «оболочка безопасности». Собственно «оболочка» сейчас проходит процедуру сертификации.

– Что мешает силовикам, госорганам, бизнесу внедрять решение уже сейчас?

– У первых и вторых существует действующая нормативная база. Но она устарела; модели угроз, на которые она рассчитана, не предусматривают угроз уровня BIOS и низкоуровневых гипервизоров. А если нет нормативного документа, то нет формального обоснования, чтобы приобретать средства защиты от непредусмотренных угроз. Они должны сначала принять новую модель угроз и нарушителя, потом под нее разработать концепцию безопасности, под концепцию безопасности создать пакет нормативных документов, под нормативные документы – новые регламенты. Это длительный процесс, но судя по косвенным признакам, он уже пошел.

Что касается госсектора, то проблема связана с конкурсным законодательством: нужны аналоги, а их пока нет! Соответственно, механизм приобретения такой продукции осложняется, поскольку отсутствует конкуренция. Наконец, есть проблема искажения информации. Все что-то слышали про опасности, про кибероружие – но лишь ограниченный круг специалистов отчетливо понимает, о чем речь. Цельной концепции противодействия таким угрозам в голове у людей, принимающих решения, нет, они ориентируются на общие векторы. Свое решение мы сделали с большим опережением, но, думаю, очень скоро «оболочка безопасности» станет общим вектором. ИКС

Особое мнение

Не по дороге с облаками

Продавцы облачных сервисов убеждают нас, что корпоративные заказчики уже просто-таки рвутся в облака... Но до сих пор нет ни одного внятного, обоснованного и убедительного ответа на крайне простые, очевидные вопросы.

Михаил ЕМЕЛЬЯННИКОВ,
консалтинговое агентство «Емельянников, Попова и партнеры»

Все эти годы вдвижения новых сервисов в умы и деньги заказчиков вместо ответов мы получаем то, что классик мировой революции называл эклектической похлебкой, – общие слова про колоссальный опыт и ответственность разработчиков, про неизбежность научно-технического прогресса и светлое будущее аутсорсинга... Все эти слова останутся лишь общими словами, пока не станет ясно:

1. Что происходит с данными, загруженными в облако, после выполнения действий, назначенных заказчиком (обработки, проведения вычислений, нажатия клавиши Delete на ПК пользователя, работающего с облачной инфраструктурой)?
2. Какими конкретно механизмами обеспечивается разграничение доступа к информации в облаке между пользователями всех этих SaaS/IaaS/

PaaS и вообще XaaS, кто и как подтвердил их надежность?

3. Как обеспечивается безопасность виртуальной архитектуры внутри облака, нейтрализуются атаки на гипервизор, ограничиваются права суперпользователя, и почему бы не продать нашу информацию конкурентам, которые получают всё по запросу в том же облаке?

4. Кто и как управляет ключами шифрования при закрытии канала передачи данных в облако? Почему это не АНБ/ЦРУ/«Моссад»/BND/MI5-MI6 (список продолжите сами)?

Перечень вопросов не исчерпывающий, и касается он только конфиденциальности. Но, как только вы поднимаете глаза вверх и смотрите на белогривых лошадок, у любого ИТ- или ИБ- директора в здравом уме и твердой памяти появляются нехорошие мысли про доступность и целостность. Перечень вопросов стремительно растет:

5. Кто конкретно и как отвечает за неизменность ваших данных в облаке? Чем это подтверждается?

6. Что вы будете делать, когда у вас не окажется доступа к Интернету?

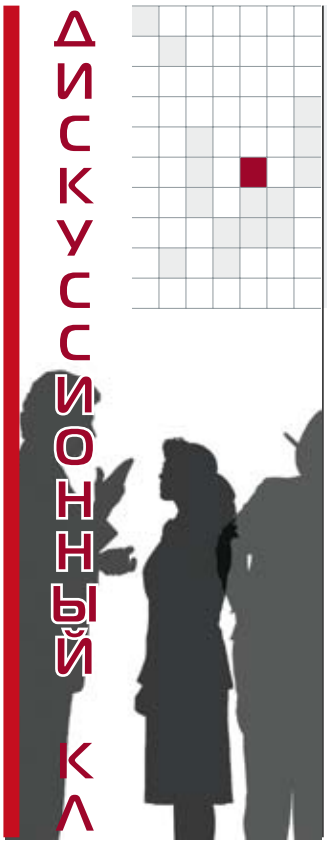
7. Что вы будете делать, когда провайдер откажет вам в услуге?

8. Что вы будете делать, когда ваши данные бесследно исчезнут?

9. Что вы будете делать, когда решите «найти себе другого провайдера, честного» и мигрировать к нему? Как вы перенесете свои данные и перенесете ли вообще?

Отсутствие внятных ответов на все выше поставленные вопросы заставило меня вернуться к соображениям годичной давности, изложенным на одной из профильных конференций. Я не нашел не только тридцать три, но и три отличия от того, что происходит сегодня. Для информационных технологий и информационной безопасности с точки зрения нейтрализации возникающих угроз год – период огромный. И если за это время на технологические вызовы нет соответствующей реакции, зато заметен рост агрессивности маркетинга, это неспроста. И у меня, как у специалиста по безопасности, появился новый вопрос к провайдерам облачных услуг: а как и где заказчик может познакомиться с логами событий безопасности, связанными с его конкретно данными? Они вообще-то есть? И как там с таргетированными атаками, всякими новыми Stuxnet, Flame, Gauss? Ведь красть с колхозного поля всегда легче, чем с личной делянки.

Боюсь, что до получения не просто ответов, а обязательств, закрепленных в договорах с провайдерами, публичные облака останутся областью применения для почтовых сервисов и личных файлов, а про международные корпорации, перенесшие в них свою информационную инфраструктуру (названия, по понятным причинам, не раскрываются), нам придется верить продавцам ~~воздуха~~ облаков на слово. ИКС



Без периметра

Вендоры идут в провайдеры облачных сервисов и выступают в качестве заказчиков таких услуг от других провайдеров, системные интеграторы становятся провайдерами и наоборот – «бизнес-периметр» размыт облаками не меньше, чем само базовое понятие информационной безопасности, признают участники дискуссионного клуба «ИКС», они же эксперты нашего «дорожного картирования».

Специфика движения

«ИКС»: Большинство решений инфобезопасности перекочевало в облака из корпоративных сетей. Какие элементы инфраструктуры нуждаются в дополнительной защите, связанной с облачной спецификой?

Юрий СЕРГЕЕВ, системный архитектор Центра информационной безопасности, «Инфосистемы Джет» : Традиционно наиболее уязви-


Ю. СЕРГЕЕВ

мы сервисы, к которым возможен доступ из внешних сетей. Это особенно критично в случае недостаточности функционала ИБ при реализации API взаимодействия с облаком. В «зону риска» попадают также сервисы, обеспечивающие изоляцию между данными отдельных подписчиков услуг облака: сервер приложений для SaaS, платформа, являющаяся средой разработки приложений в модели PaaS, а для IaaS это зачастую гипервизор и другие компоненты виртуальной инфраструктуры. Нельзя забывать и о системах, обеспечивающих работу в инфраструктуре, – коммутаторах, системах хранения данных, средствах управления, которые также несут в себе угрозы нарушения конфиденциальности доверенной оператору информации.

Джабраил МАТИЕВ, руководитель группы информационной безопасности, IBS Platformix: В облачной среде появляются новые элементы: подсистема управления и подсистема самообслуживания. Обе эти подсистемы требуют особого внимания с точки зрения защиты. Другие вопросы безопасности тесно перекликаются с защитой виртуализации.

Дмитрий МИТРОФАНОВ, заместитель директора СЦ по производству, «Ай-Теко»: Усиленная защита всегда будет нужна элементам вычислительных сетей и сетей передачи данных. При любом уровне развития технологий защиты данных эти информационные активы критически важны для бизнеса.


А. ФИЛАТЕНКОВ

Алексей ФИЛАТЕНКОВ, начальник отдела ИБ, «Открытые Технологии»: Особое внимание следует уделить системе мониторинга на предмет соответствия данных об облаке реальной картине. Решения для обеспечения безопасности облачных инфраструктур, по всей видимости, должны учитывать изменения самой вычислительной платформы, наличие систем виртуализации.


Н. НИКИТОВИЧ

Неманья НИКИТОВИЧ, управляющий директор, Optima Infosecurity (Группа Optima): В зависимости от требований бизнеса все сетевые компоненты должны быть соответствующим образом защищены, но большинство компаний сегодня более всего сосредоточены на хранении данных и, следовательно, на защите и шифровании внутренних коммуникаций.


А. ХРИПУНОВ

Антон ХРИПУНОВ, руководитель направления центров обработки данных, CTI: На первое место надо ставить физическую безопасность, при недостаточности которой никакие программные методы не помогут. Одно из интересных и перспективных решений для тех, кто решился на использование публичных облаков, – создание механизма динамического перемещения ресурсов между ними облачными провайдерами (liquid cloud). Это не панацея в плане обеспечения физической безопасности, но позволит значительно сократить риски за счет того, что даже сам провайдер облака не сможет спрогнозировать наличие у него ресурсов клиента в обозримом будущем. Единственной точкой проникновения к бизнес-данным и приложениям в таком случае становится обслуживающий ИТ-персонал клиента, который контролирует перемещение ресурсов от одного облачного провайдера к другому.


М. ГОТАЛЬСКИЙ

Михаил ГОТАЛЬСКИЙ, руководитель TrueConf: В облачные сервисы будут перекочевывать все корпоративные системы безопасности, а также добавятся сервисы защиты каналов. Основа корпоративной безопасности – безусловное доверие внутренней локальной сети при полном недоверии внешним коннектам. Поэтому максимальный уровень контроля – доступу извне, шифростойкости каналов, аутентификации, авторизации, получению и повышению привилегий. Правило хорошего тона при обеспечении безопасности в облачных вычислениях – полное разделение сред и средств различных сеансов: «персональные песочницы» в java, chroot в linux, jail в freebsd.

Вячеслав МЕДВЕДЕВ, аналитик, «Доктор Веб»: Даже в случае полного перевода всех сервисов компании в облако сложно представить, что машины сотрудников будут подсоединяться к облаку непосредственно. Как минимум в локальной сети должен остаться интернет-шлюз. Должна быть система защиты от атак и брандмауэр: несмотря на вынос сервисов наружу (а во многом и благодаря этому) «остаток» локальной сети, рабочие станции пользователей – это лакомый кусок для хакеров. По тем же причинам должны быть защищены рабочие станции – требование наличия на них антивируса, системы ограничения доступа и брандмауэра отменить невозможно. Другой вопрос, что управляться эти системы могут из облака. Для минимизации рисков на случай недоступности Интернета или плановых ремонтов на стороне провайдера услуг желательно наличие резервного почтового сервера, сервера Active

Directory и др. Защита облака сама по себе не представляет ничего особенного, но при переходе в облако нужно обратить особое внимание на гарантии поставщика в области обеспечения непрерывности работы и процедуры, связанные с хранением, обработкой и уничтожением данных клиента, в том числе в резервных копиях.


А. ГАРУСЕВ

Артем ГАРУСЕВ, исполнительный директор, CDNvideo: Есть очевидные вещи, например, защита гипервизора или системы биллинга. Но есть и важные темы, которым почему-то уделяется меньше внимания. Например, это вопросы безопасности микрокода процессора, который, собственно, выполняет все гостевые ОС. Если процессор (микрокод) разделяется между несколькими клиентами, он может послужить причиной утечек данных между облаками. Еще я бы отметил, что объектом нападения могут становиться сами подсистемы ИБ, причем не только те, которые использует провайдер, но и те, которыми его сервис дополняет заказчик. Нарушив работу системы управления правами доступа или, например, системы аутентификации, киберпреступник может добраться до информации под видом легального пользователя, без каких-то сложнейших «инновационных» разработок. Похоже, это самый экономичный способ, а значит им будут активно пользоваться.


А. САНИН

Александр САНИН, коммерческий директор, Avanpost: Представьте: работаете вы в облаке, ничего не нарушаете, а параллельно с вами работает какая-то другая компания, у которой случаются проблемы с надзорными органами. Приходит ФСБ или кто-то еще, например БСТМ (бюро специальных технических мероприятий), и изымает серверы из ЦОДа… А ведь на этих серверах вполне может быть часть и вашей инфраструктуры и информации. Вопрос, конечно, крайне специфичный, но все-таки его надо как-то решать.

Водительские риски

?→ «ИКС»: Как соотносятся затраты провайдера облачных услуг на внедрение решений ИБ и окупаемость таких проектов? Как минимизировать его риски?


А. ИВАНОВ

Алексей ИВАНОВ, руководитель проектов, департамент инфраструктурных решений, Digital Design: Перемещение вектора ответственности за безопасность облака на провайдера – правильная тенденция. Иначе облачными сервисами так и будут пользоваться только ради интереса, не перенося в них ничего серьезного. Конечно, построение хорошей системы защиты требует покупки и внедрения множества продуктов, что приведет к увеличению стоимости подписки для потребителя. Но иначе никак, качество услуги должно быть соразмерно ее стоимости. С другой стороны, риск потери или компрометации информации заказчика висит «дамокловым мечом» над провайдером. Чтобы облегчить его участь, можно посоветовать разделение ответственности между провайдером и вендорами средств безопасности.

А. ГАРУСЕВ: Один из способов минимизировать риски – передать существенную часть защиты (вместе с ответственностью за результаты) в руки самих пользователей. Скажем, сервис синхронизации файлов Dropbox позволяет помещать в облачное хранилище зашифрованные пользователем файлы. «Заметочный» сервис Evernote проводит синхронизацию облачной и локальной баз данных на более детальном «субфайловом» уровне, поэтому здесь разработчики рекомендуют помещать всю БД на шифруемый диск (например, TrueCrypt).

Денис БЕЗКОРОВАЙНЫЙ, технический консультант, Trend Micro в России и СНГ: К затратам провайдера следует также отнести расходы на прохождение аудита и различных сертификаций, на квалифицированный ИБ-персонал, который в дефиците на рынке. Снизить затраты и риски провайдера поможет использование схемы pay-as-you-grow для оплаты решений ИБ. Это относительно новая система отношений с вендорами, при которой провайдер облачных услуг может начать предоставлять своим клиентам решения для защиты облачной инфраструктуры с нулевыми затратами. По мере роста клиентской базы провайдера растет количество защищаемых объектов, и только после этого происходит оплата фактически потребленных провайдером лицензий на средства ИБ.


Д. БЕЗКОРОВАЙНЫЙ

Д. МАТИЕВ: Затраты на внедрение решений информационной безопасности для провайдера более высоки в случае с SaaS, но, как правило, услуга может быть эксклюзивной и высокомаржинальной.

Внедрения систем безопасности окупаются очень быстро, затраты невысоки (не более 5% от стоимости облака), при этом надежная защита всегда привлечет больше потребителей. Минимизация рисков достигается за счет комплексного подхода к обеспечению инфобезопасности, основанного на лучших мировых практиках. Безусловно, при этом необходимо внедрить рабочую систему оценки и управления рисками.


Д. МАТИЕВ

Владимир ТКАЧЕВ, технический директор, VMware Россия и СНГ: Риски нельзя минимизировать, рисками надо управлять. Минимизировать риски можно, только отказавшись от ответственности по рискованным статьям, что приведет к сокращению перечня предоставляемых услуг или оттоку заказчиков из-за снижения качества услуг.

Путеукладчики за рулем

«ИКС»: Роль системных интеграторов на рынке безопасности публичных облачных услуг: в каких случаях привлечение «третьей стороны» неизбежно и почему?


С. ЩЕРБИНА

Сергей ЩЕРБИНА, заместитель генерального директора, Esri CIS: Роль системных интеграторов в создании облаков и обеспечении их безопасности в целом аналогична их роли в других ИТ-проектах. Однако в данном случае в силу относительной новизны технологий и особых опасений относительно безопасности заказчикам имеет смысл подумать о проведении независимого аудита степени защиты своих данных и приложений.

А. ИВАНОВ: Наверное, ситуаций, в которых привлечение «третьей стороны» было бы неизбежно, нет. Однако привлечение системного интегратора может снизить риск ошибок в принятии решений, обеспечить переход в облака с минимальными трудностями. Системный интегратор может стать тем «третейским судьей», который поможет потребителю, с одной стороны, не испугаться новых решений, с другой – не «повестись» на завлекательные речи провайдеров, доходчиво разъяснит все плюсы и минусы.


А. КОЛЫБЕЛЬНИКОВ

Александр КОЛЫБЕЛЬНИКОВ, эксперт по информационной безопасности, «Микротест»: Системный интегратор на этом рынке выполняет ровно свою функцию. Передача каких-либо технологий, ПО, информации в облако – это акт доверия со стороны пользователя провайдеру. В этих отношениях системный интегратор играет роль третьей стороны не только в процессе внедрения технологий, но и в процессе аудита безопасности облаков, выдавая некое заключение о безопасности облака, которое позволит провайдеру демонстрировать потенциальным заказчикам определенную степень защищенности, побуждая доверять им больше. По сути это способ продвижения на рынке.

Д. БЕЗКОРОВАЙНЫЙ: На западном рынке уже сформировалась ниша для компаний – «облачных брокеров». Это компании, предоставляющие услуги интеграции сервисов от различных облачных провайдеров и их совместного использования клиентами. Основные плюсы облачного брокера для заказчиков – возможность переключения от одного провайдера к другому в случае сбоев, оптимизация расходов и упрощение биллинга. В России можно ожидать появления облачных брокеров, если провайдеры будут готовы открывать интерфейсы интеграции для сторонних сервисов.


В. АНДРЕЕВ

Валерий АНДРЕЕВ, заместитель директора по науке и развитию, ИВК: Все зависит от модели облака. Если вопросы ИБ будет решать пользователь, то интеграторам есть место, а если провайдер – то нет.

Д. МИТРОФАНОВ: Если говорить о российской специфике, то у нас по закону ФЗ-152 обеспечивать законодательное соответствие предлагаемых клиентам решений должны локальные поставщики. Это как раз задача интеграторов. Можно сказать, что интегратор – это глаза и руки вендора, работающие на рынке и позволяющие объединить интересы всех сторон. Системные интеграторы играют роль инжиниринговых компаний по разработке и развертыванию облачных сервисов для сервис-провайдеров.


А. РАЗУМОВ

Антон РАЗУМОВ, руководитель группы консультантов по безопасности, Check Point Software Technologies: Чем сложнее система, тем больший опыт необходимо иметь для грамотного ее проектирования и внедрения. Именно опыт, просто теоретиче-

ских знаний будет недостаточно. Кроме того, у новичка часто разбегаются глаза от многообразия решений, и для грамотного сравнения, выбора стратегии нужно изучить множество вариантов, в том числе и те, которые ему вовсе не пригодятся. Поэтому помощь системных интеграторов, имеющих опыт разнообразных проектов, позволяет сэкономить значительные средства, время и избежать критичных ошибок.


М. БАШЛЫКОВ

Михаил БАШЛЫКОВ, руководитель направления информационной безопасности, КРОК: Системный интегратор может сам выступать в роли провайдера публичного облака, обеспечивая безопасность облака в целом или опционально, в зависимости от вида услуг.

Впереди – поворот

«ИКС»: Насколько реальна перспектива появления на рынке продуктов, способных безопасно интегрировать в облаках множество ИТ-приложений от разных поставщиков и провайдеров?

В. АНДРЕЕВ: Пока что совершенно нереальна. Даже на уровне функционала, не говоря уже о проблемах инфобезопасности. Отсутствие облачных стандартов не дает возможности интеграции, но все впереди.


А. ТРОШИН

Александр ТРОШИН, технический директор, «Манго Телеком»: Я пока не вижу таких продуктов на рынке. Но в то же время ничего нереального в их создании нет. И когда-нибудь их появление станет очень актуальным, так как множество различных нестандартизованных инструментов управления виртуальными средами могут однажды загнать пользователя в тупик. Думаю, лет через пять на рынок выйдут некие продукты, которые смогут определенным образом (например, с помощью API) взаимодействовать с разными провайдерами и управлять всеми разрозненными виртуальными продуктами.


В. МЕДВЕДЕВ

В. МЕДВЕДЕВ: Необходимо создание резервных локальных сервисов на время недоступности облачных. Появление таких предложений вполне реально, но вот использование их не может быть рекомендовано. Например, антивирусы, использующие сторонние антивирусные ядра, даже при их высоком качестве в тестах на активные заражения показывают во многих случаях не самые высокие результаты.

А. КОЛЫБЕЛЬНИКОВ: На рынке такие продукты уже есть, и они давно и успешно используются. Например, системы сбора и анализа данных журналов событий работают с разными приложениями.


В. АЛЕЕВ

Владимир АЛЕЕВ, главный архитектор бизнес-решений: центры обработки данных, «Ситроникс»: Необходимо заранее проверить возможность обмена данными между различными облачными приложениями, но лучше если этой задачей озаботятся операторы облачных услуг, которые предлагают несколько SaaS-приложений от разных разработчиков. Спрос на такие платформы интеграции есть, предложение начинает формироваться.

В. ТКАЧЕВ: Модель потребления приложений от разных поставщиков из облака пока только развивается. Тем не менее уже очевидно, что точечные сервисы, решающие узкие задачи, будут набирать обороты. Программное обеспечение становится очень «динамичным» с точки зрения сроков разработки и времени жизни отдельных версий. Как следствие, в арсенале бизнес-пользователя будет широкий спектр программных продуктов, потребляемых по различным моделям, от локальных до внутренних облаков или публичных поставщиков. В этой связи ИТ- и ИБ-подразделения столкнутся с пока еще новыми задачами, от управления доступом к широкому спектру внешних услуг до сохранности данных, необходимых для работы этих сервисов.


В. ТКАЧЕВ

ПОЛНЫЙ ТЕКСТ
Дискуссионного клуба читайте на
www.iksmedia.ru

Производительность шлюзов безопасности: «кот в мешке» или разумный расчет

При передаче данных через недоверенные сети технология IPSec VPN обеспечивает их конфиденциальность и целостность. Однако шифрование и контроль целостности – ресурсоемкие операции, при неправильном построении системы передачи данных именно они становятся узким местом. Чтобы не создавать проблем в работе ИТ-сервисов, следует уже на этапе проектирования учитывать производительность шифрующих средств.

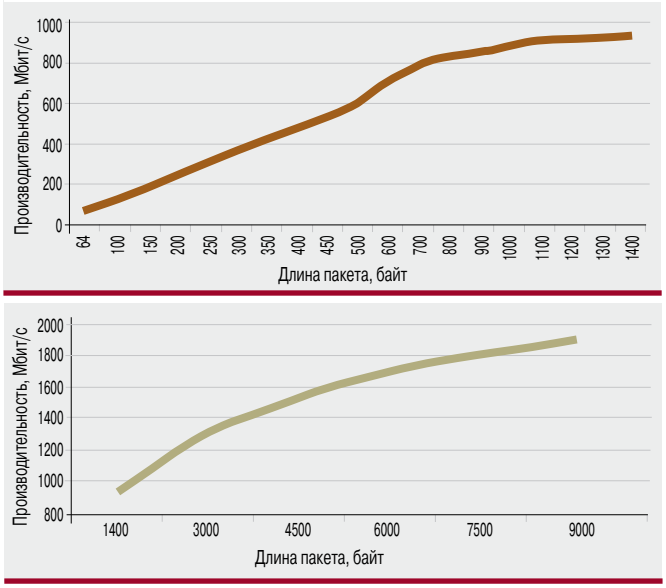
Владимир ВОРОТНИКОВ, руководитель департамента перспективных исследований и проектов, «С-Терра СиЭсПи»

Существует распространенное заблуждение, что производительность – это простое понятие, характеризуемое одним числом. На самом деле **производительность – комплексная величина, зависящая от множества факторов.** Для сетевых устройств безопасности она будет включать в себя как сетевую производительность, так и производительность шифрования. Все значения, речь о которых пойдет ниже, получены при использовании алгоритмов, описанных в ГОСТ 28147-89 и ГОСТ Р 34.11-94.

Ресурсы шлюза безопасности тратятся приблизительно в равной степени на шифрование и на дешифрование трафика. Поэтому если указана, например, производительность шифрования 500 Мбит/с, это значит, что либо шлюз шифрует поток 500 Мбит/с «в одну сторону», либо шифрует 250 Мбит/с и расшифровывает 250 Мбит/с. В любом случае перед выбором оборудования следует уточнить у вендора, какая именно производительность имеется в виду.

Еще один фактор, влияющий на производительность, – профиль трафика или, проще говоря, частота встречаемости пакетов разной длины. Это наиболее существенный параметр: **одно и то же устройство на разных профилях трафика может показывать производительность, различающуюся в десятки раз.** Например, топовые шлюзы компании «С-Терра СиЭсПи» (CSP VPN Gate 7000 HighPerformance) показывают производительность 3,5 Гбит/с на UDP-трафике с пакетами длиной 1400 байт и 150 Мбит/с на UDP-трафике с пакетами в 64 байт. Понятно, что в случае коротких пакетов узким местом становится не шифрование, а сетевая подсистема.

Производительность шлюза безопасности в зависимости от длины пакета



Измерения производительности шлюза безопасности в зависимости от длины пакета (см. рисунок) проводились на шлюзе средней производительности CSP VPN Gate 3000 от «С-Терра СиЭсПи».

Здесь важно отметить: тесты на пакетах фиксированной длины являются синтетическими. В реальной сети такой профиль трафика практически никогда не встречается. **Для того, чтобы при моделировании максимально приблизиться к условиям работы шлюзов безопасности в реальных сетях, используют смешанный трафик (IMIX).** Он неплохо соответствует среднестатистическому трафику магистральных каналов. Статистика измерений производительности шлюзов безопасности «С-Терра СиЭсПи» свидетельствует, что производительность на IMIX и на трафике UDP с пакетами длиной 450 байт примерно одинакова.

Еще один параметр, который может повлиять на производительность, – количество потоков трафика. Распространено мнение, что чем больше IPSec-туннелей, тем сложнее их обрабатывать. Это не так (по крайней мере для шлюзов безопасности «С-Терра СиЭсПи»). Плюс большого количества IPSec-туннелей в том, что обработку множества потоков легче распараллелить на многопроцессорных устройствах. Есть, конечно, верхний предел, начиная с которого производительность будет снижаться, но он обычно составляет сотни и тысячи туннелей, в зависимости от аппаратной платформы и структуры сети.

Итак, производительность – многогранное понятие, и при разных условиях у одного и того же оборудования она может отличаться на порядок. **Выбирая шлюз безопасности по производительности, старайтесь получить полную информацию:** что понимает вендор под производительностью, какова она на коротких и длинных пакетах, какова на смешанном трафике (IMIX) и что произойдет, если количество туннелей будет возрастать. Только так можно быть уверенными, что внедрение решения для защиты каналов связи пройдет прозрачно для ИТ-инфраструктуры и конечный пользователь не заметит включения шлюза безопасности в существующую сеть.