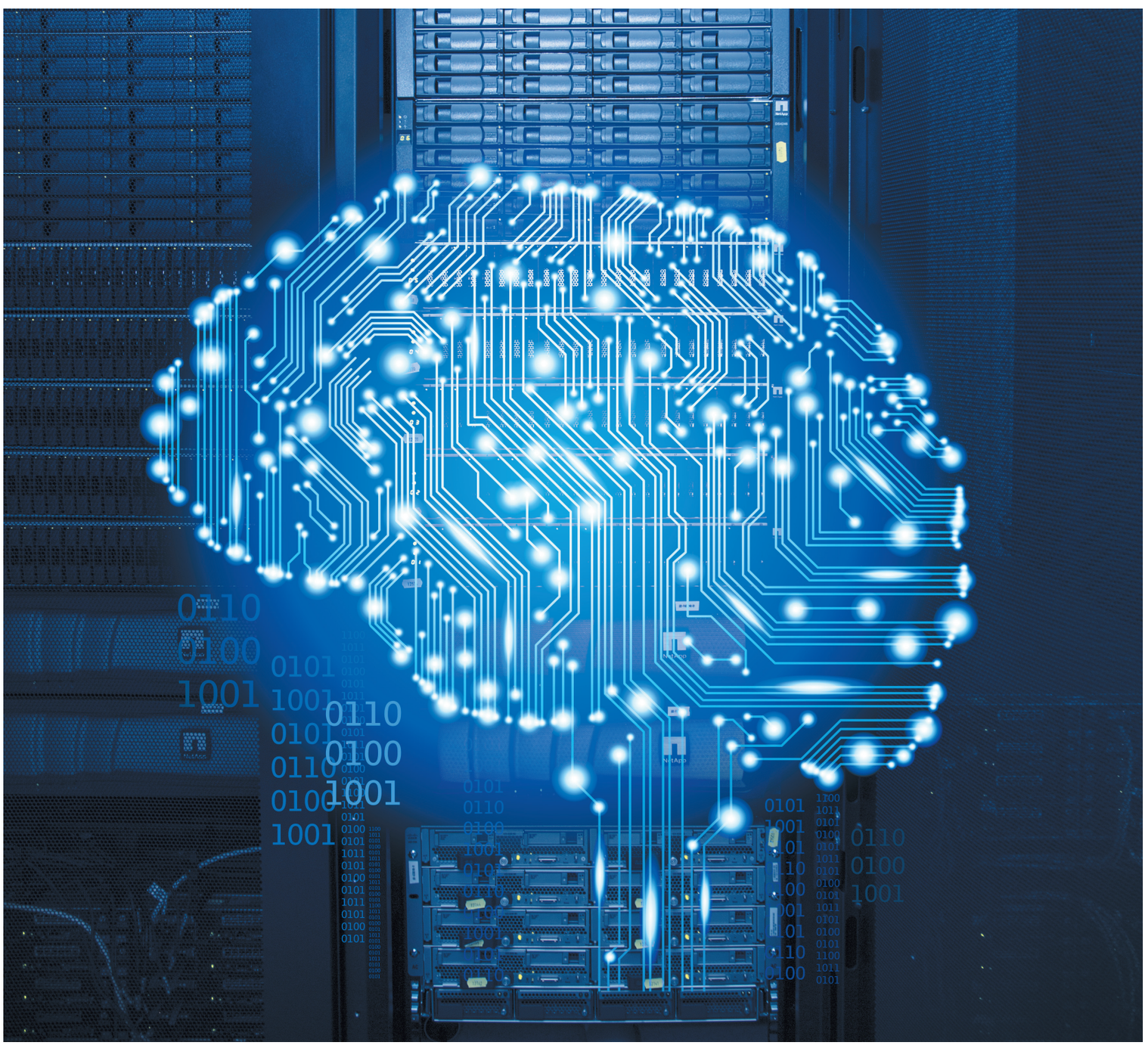
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№10 (255)/2014

ИТ-СЕРВИСЫ. КАК ПОЛУЧИТЬ ВСЕ И СРАЗУ?



Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Редакция:
Дмитриев В.Ю.
vlad@jet.msk.su

Некрасова Н.А.
nekrasova@jet.msk.su

Шедова Е.Л.

Дискина А.Л.
ashklyaeva@jet.msk.su

Дизайн и верстка:
Саблина М.А.

Корректура:
Макеева Е.И.

Над номером работали:
Дрюков В.В.
Кошкин И.М.
Панченко Ю.В.
Учамприн А.В.

Издатель:
Компания
«Инфосистемы Джет»

Контакты:
тел.: (495) 411-76-01
www.jetinfo.ru

ИЛЬЯ КОШКИН,
менеджер по развитию бизнеса Центра проектирования вычислительных комплексов компании «Инфосистемы Джет»

«Налево пойдешь... направо пойдешь... прямо пойдешь...». Примерно так можно охарактеризовать процесс принятия решения CIO относительно формата получения и использования необходимых ИТ-ресурсов. Что будет наиболее оптимально — построить свой ЦОД, воспользоваться услугами colocation-провайдера или арендовать готовые ИТ-сервисы? В нашем номере мы рассматриваем все три подхода на реальных кейсах, более подробно останавливаясь на последнем варианте и его конкретной реализации — нашем виртуальном центре обработки данных. Что и кто «живет» в нашем ВЦОД, в каких случаях его использование целесообразно, какие бизнес-выгоды он может дать компании? На последующих страницах наши эксперты дают ответы на эти и многие другие сопутствующие вопросы.

СОДЕРЖАНИЕ

12 ВНЕШНИЕ ИТ-РЕСУРСЫ – НЕЛЬЗЯ (,) ОТКАЗАТЬСЯ!
ИЛЬЯ КОШКИН, ЮРИЙ ПАНЧЕНКО

17 МАСС-МАРКЕТ VS ИНДИВИДУАЛЬНЫЙ ПОШИВ
ИЛЬЯ КОШКИН, АЛЕКСЕЙ УЧАМПРИН

3 От редакции

5 Новости

9 Наши проекты

30 В тему номера

23 НА ЧЕМ СТОИМ
ИЛЬЯ КОШКИН

26 ВНЕШНЯЯ ПОДУШКА БЕЗОПАСНОСТИ
ВЛАДИМИР ДРЮКОВ

СЕМИНАР «ДИНАМИЧЕСКАЯ ИНФРАСТРУКТУРА: ВОПРОСЫ ЭКСПЛУАТАЦИИ»

16–17 октября в Подмосковье прошел традиционный ежегодный семинар для заказчиков Сервисного центра компании «Инфосистемы Джет», собравший более 170 участников.

В этом году деловая программа получилась насыщенной. Пленарное заседание и 6 секций не смогли вместить всех актуальных тематик, поэтому часть докладов в виде мини-презентаций можно было послушать на демонстрационных стендах, работавших на протяжении всего семинара.

Одной из центральных тем стала практика применения аутсорсинга. Были рассмотрены различные этапы перехода к аутсорсингу: от принятия решения и проработки стратегии до непосредственного взаимодействия заказчика и исполнителя в ходе проекта. Также обсуждались практические аспекты эксплуатации систем: на что необходимо обратить внимание службам поддержки, какие технологические новинки можно применять и для каких целей и т.д.

Специально организованный мастер-класс был посвящен вопросам составления аутсорсинговых договоров: специалисты компании «Инфосистемы Джет» рассказали, как правильно их составлять и читать, что необходимо учесть и ни в коем случае нельзя забывать, а также поделились своими наработками. Заказчики задавали вопросы и приводили примеры из своей практики – получилась живая и по-настоящему интересная дискуссия.

Среди других горячих тем, которые нашли отражение в программе, – вопросы внешнеполитических рисков и инструменты оптимизации затрат на инфраструктуру. Эксперты рассказали о продуктах, которые могут стать заменой традиционным решениям, и представили результаты проведенных тестов.

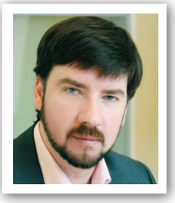
В ходе семинара работал инструмент Jet Toolbar – собственная программная разработка компании «Инфосистемы Джет» – приложение для тонкой настройки и персонализации операторских услуг. По Wi-Fi сети посетители получали на свои мобильные устройства оповещения о программе и демонстрациях на стендах и даже меню кофе-брейков. Также на круглом столе, посвященном эффективному использованию Wi-Fi сети, можно было поподробнее узнать о возможностях Jet Toolbar и посмотреть его работу в режиме реального времени.

На стендах партнеров семинара были представлены такие продукты, как:

- Cisco Systems и NetApp – интегрированная инфраструктура FlexPod;
- Hitachi Data Systems – интерфейс управления и пользовательский портал HCP AnyWhere;
- Huawei – коммутатор 12700;
- IBM – Smart Cloud Orchestrator.

ДЕМОНСТРАЦИЯ ИБ-КОМПЕТЕНЦИЙ

«Инфосистемы Джет» приняла участие в XI Международной выставке-конференции«InfoSecurity Russia». В деловой программе мероприятия эксперты компании поделились собственным взглядом на самые актуальные сегодня задачи в области ИБ, основанным на проектном опыте.



Игорь Ляпунов, директор Центра информационной безопасности компании «Инфосистемы Джет», рассказал о том, что можно и что нельзя отдавать на аутсорсинг, как выработать стратегию перехода на аутсорсинговую модель, каков зарубежный опыт есть и насколько он применим к отечественной практике. В качестве практических примеров для изучения участникам секции были представлены кейсы, которые решались командой собственного коммерческого центра мониторинга и реагирования на инциденты ИБ компании «Инфосистемы Джет» (JSOC) в течение 2013–2014 г.г.

В последующем открытом диспуте слушатели секции и приглашенные эксперты обсудили вопросы, связанные с определением места аутсорсинга в сфере ИБ, аргументацией защитников и противников этой идеи, передачей функций ИБ на аутсорсинг, подводными камнями процесса передачи и т.п.

Эксперты компании приняли участие в секции, посвященной теме DLP (контроля утечек информации), сконцентрировавшись при этом на тенденции к функциональному слиянию информационной и экономической безопасности. На примере развития собственного DLP-продукта компании (комплекса «Дозор-Джет») **Дмитрий Михеев, ведущий архи-**

тектор Центра информационной безопасности, рассказал о том, куда и почему движутся современные системы класса DLP и о новых возможностях в расследовании инцидентов безопасности.

Еще одна актуальная тема, которую эксперты компании «Инфосистемы Джет» также не обошли своим вниманием на конференции – уязвимость мобильных приложений и защита содержащихся в них данных от НСД: эксперты компании познакомили аудиторию с ТОП 10 наиболее популярных уязвимостей, примерами их применения и методами исправления кода.

Посетители выставки также ознакомились с «живым» опытом экспертов компании в таких направлениях, как защита АСУ ТП, борьба с мошенничеством и гарантирование доходов.

VMWARE NSX ДЛЯ ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ ЦОД

Dell и VMware предложат серию новых сетевых решений и референсную архитектуру для среднего бизнеса, крупных предприятий и провайдеров услуг. В частности партнеры совместно с компанией Cumulus Networks выпустили платформу виртуализации сетей VMware NSX с операционной системой Cumulus Linux для коммутаторов Dell Networking. В дополнение к этому Dell предложит конвергентное решение с предустановленной платформой VMware NSX для среднего бизнеса.

По расчетам Dell, VMware и Cumulus Networks, сконфигурированное решение, сочетающее платформу VMware NSX с ОС Cumulus Linux для Dell Networking, поможет предприятиям и провайдерам услуг получить готовую сетевую среду для центров обработки данных, физическую и виртуальную, обеспечить централизованное управление, упростить ИТ-операции и сократить время на запуск новых приложений.

Как известно, компании с ограниченным ИТ-штатом и бюджетом нуждаются в простых, интегрированных и проверенных архитектурах. Конвергентное решение Dell и VMware призвано удовлетворить такие потребности. Решение включает платформу виртуализации сетей VMware NSX, запущенную на инфраструктуре Dell, состоящей из серверов, сетевого оборудования и системы хранения данных. Конвергентная инфраструктура Dell включает блейд-систему Dell PowerEdge M1000e, блейд-коммутатор Dell Networking 10/40GbE MXL, надстоечный коммутатор S4810, коммутаторы S6000 и массивы Dell Storage iSCSI.

НОВАЯ ПЛАТФОРМА NEXUS 2300

Прошло уже более пяти лет с тех пор, как Cisco вывела на рынок свой первый расширитель коммутационной матрицы (Fabric Extender, FEX) семейства Nexus 2000. Теперь линейка пополнилась новой платформой Nexus 2300, т.е. третьим поколением расширителей Fabric Extender. Решение открывает новые возможности:

- увеличен объем буферной памяти для сглаживания всплесков трафика при выполнении многоадресной рассылки, передачи голоса и видео.
- Унифицированные порты позволяют гибко разворачивать LAN и SAN благодаря поддержке подключений Ethernet, FC и FCoE.
- Обеспечена поддержка 40-гигабитных оптических трансиверов Cisco BiDi с двунаправленной передачей, что упрощает переход с 10 на 40 Gigabit Ethernet, позволяя при этом использовать существующее 10-гигабитное кабельное хозяйство.
- Дополнительная память TCAM.

К вышеупомянутому следует добавить такие реализованные во всех устройствах Nexus 2000 функции, как централизованное управление и применение политик, автоматическую настройку при установке и автоматическое конфигурирование. Это дает дополнительные преимущества благодаря уменьшению сложности и повышению гибкости сети. В результате ускоряется монтаж и демонтаж серверных стоек, упрощается эксплуатация, обеспечивается поддержка изменяющихся требований разнообразных систем.

КОМПЬЮТЕРНЫЙ МОЗГ ПРИБЛИЖАЕТСЯ К ЧЕЛОВЕЧЕСКОМУ

Как известно, нервная система работает благодаря колоссальному количеству нервных клеток, образующих контакты друг с другом — синапсы. Один и тот же нейрон образует связи со многими другими нейронами, учитывает при передаче сигналов «мнение» соседей, участвует сразу в нескольких нейронных контурах, рвёт старые синапсы, формирует новые и т.д. Несколько миллиардов нервных клеток как будто постоянно «дышат», образуя, усиливая, ослабляя и разрывая множество соединений-синапсов. Обрабатывая изображение, мозг работает параллельно, то есть разные нейроны занимаются различными фрагментами картинки, вместо того чтобы последовательно, пиксель за пикселем, её прочёсывать, как это делает процессор. То же самое касается и других задач, не только визуальных.

Одна из успешных попыток воплощения мозга в железе сделана в исследовательской лаборатории IBM в рамках проекта SyNAPSE (Systems of Neuromorphic Adaptive Plastic Scalable Electronics). Суть его сводится к созданию вычислительных ядер с чистого листа, которые смогли бы имитировать работу мозга. Каждое из них содержит «синапс» (память), «тело нейрона» (вычислительный блок) и «аксон» (коммуникационный канал). Работая параллельно, большой массив таких ядер сможет обеспечить принципиально новые возможности вроде мгновенного распознавания сложных изображений, выявления связей между объектами, прогнозирования событий и т.д.

Если описать задачу очень грубо и с большим количеством при-

ближений и допущений, то суть её в том, чтобы создать сверхмногоядерный процессор, в котором каждое ядро будет работать как нейрон. Собранный в IBM чип TrueNorth состоит из 4000 ядер, у каждого из них есть 256 каналов ввода и 256 каналов вывода информации. Причём электрический сигнал покидает ядро только в том случае, если он превышает какое-то пороговое значение, подобно тому, как это происходит в живых нейронах. В целом на изготовление чипа ушло 5,4 млрд транзисторов, которые вместе имитируют 1 млн нервных клеток и 256 млн межклеточных соединений. Соединения ядер внутри чипа имитируют нервные контуры мозга. Компьютер с таким чипом, к примеру, быстро и корректно отличает по фото просто человека от человека на велосипеде, а легковую машину от других транспортных средств. Мозгоподобный чип оказался не только более эффективным, чем стандартные процессоры, но и меньше нагревался при работе.

В дальнейшем конструкторы собираются и дальше начинять свой процессор транзисторами, чтобы сделать его ещё более похожим на мозг — напомним, что на данном этапе он имитирует работу 1 млн нейронов, тогда как в мозге их порядка 100 млрд. К слову, предпринимались попытки симулировать работу головного мозга с помощью традиционных микросхемных технологий, и самая масштабная из таких попыток воспроизводила 1,6 млрд нейронов и 8,87 трлн синапсов, что соответствует коре мозга кошки. Для этого понадобился суперкомпьютер Blue Gene/P Dawn, насчитывающий 147 456 процессоров и 144 Тб основной памяти. Иными словами, пока даже самым мощным вычислительным комплексам в мире не под силу воспроизвести тот потенциал, который в нас заложила природа. Но, возможно, с появлением «нейронных процессоров» ситуация начнёт меняться. JI

ПЕРЕКЛЮЧАЮЩИЕСЯ МАТЕРИАЛЫ ЗАМЕНЯТ КРЕМНИЙ В КОМПЬЮТЕРАХ

Ученые из Массачусетского технологического института (США) и Университета Бата (Великобритания) разработали наноматериалы, способные переключаться между двумя структурными фазами с различными электрическими состояниями — одним кристаллическим и проводящим, а другим стекловидным и изолирующим, причем они делают это за миллиардные доли секунды. В результате обработка данных может выполняться в энергонезависимых ячейках памяти с помощью конкретных сочетаний ультракоротких импульсов напряжения, которые невозможно осуществить в устройствах на основе кремния.

Как показывают исследования, наноматериалы с такими способностями могут в конечном итоге сделать скорость обработки в тысячу раз быстрее, чем среднестатистический портативный компьютер, используя при этом меньше энергии. JI

Исследование на языке оригинала доступно здесь:

УЧЕНЫЕ ИСПЫТАЛИ «ЯДЕРНЫЙ» ЖК-ДИСПЛЕЙ

Физики Университета Юты (США) изучили субатомные спины ядер изотопов водорода и использовали полученные данные для управления питанием ЖК-дисплея при комнатной температуре и без сильных магнитных полей.

Это исследование делает физику на шаг ближе к так называемым «спинтронным» устройствам: сверхбыстрым квантовым компьютерам, а также компактным устройствам хранения данных и органическим светодиодам, которые будут гораздо эффективнее используемых сегодня.

Ученые пока не называют сроков широкого распространения «спинтронных» устройств, тем не менее появление жестких дисков объемом более терабайта стало возможно именно благодаря «спинтронным» считывающим головкам, таким маленьким, что данные могут храниться гораздо более плотно. JI

Исследование на языке оригинала доступно здесь:

ОПТИМИЗАЦИЯ РАБОТЫ КОРПОРАТИВНЫХ ПРИЛОЖЕНИЙ ХОЛДИНГА ВГТРК

ВГТРК — крупнейшая государственная медиакорпорация России, имеющая более восьмидесяти региональных представительств на территории РФ. Территориально распределенный медиабизнес предполагает активное использование корпоративных ИС. Поэтому эффективность и непрерывность их работы имеют ключевое значение для телерадиокомпании.

Партнером проекта по созданию системы контроля и управления нагрузкой на корпоративные приложения телерадиокомпании стала компания «Инфосистемы Джет».

Для автоматического перераспределения нагрузки между почтовыми серверами в соответствии с загруженностью каждого из них был построен отказоустойчивый кластер балансировщиков Brocade.

Компания «Инфосистемы Джет» более 10 лет является аккредитованным партнером Brocade и имеет значительный опыт проектирования, внедрения и поддержки решений Brocade в России и СНГ.

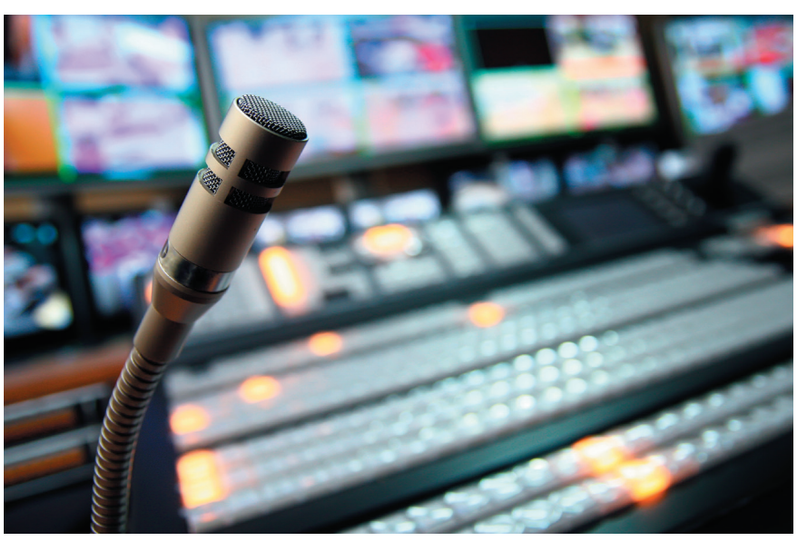
Также обеспечен постоянный мониторинг работоспособности системы балансировки и наращивание ее производительности без установки дополнительного оборудования.

«Сбои в работе корпоративных информационных систем крайне негативно сказываются на бизнес-процессах компании. Использование проверенных временем решений позволило минимизировать вероятность сбоя ИТ-сервиса по причине проблем с системами балансировки трафика. Автоматизация процессов перераспределения нагрузки позволила нам свести этот показатель практически к нулю, существенно увеличив надежность и отказоустойчивость корпоративных приложений», — рассказывает **Евгений Кукушкин, начальник управления сетевых и серверных технологий ДИТ ДРЦТ ВГТРК.**

«Установку оборудования, его настройку и тестирование мы выполняли "на ходу" в часы наименьшей нагрузки, — рассказывает

Игорь Грибанов, менеджер по работе с корпоративными клиентами компании "Инфосистемы Джет". — Весь процесс был поэтапно описан и спланирован совместно с командой специалистов ВГТРК. Благодаря слаженной работе всех участников процесса мы смогли встроить оборудование в чувствительную инфраструктуру совершенно незаметно для конечных пользователей».

«Балансировщики нагрузки приложений Brocade ADX являются одним из самых популярных и востребованных направлений Brocade с момента выхода компании на сетевой рынок России и СНГ в 2009 году, — комментирует **Иван Иашагашвили, генеральный управляющий Brocade**



в России и СНГ. — Компания "Инфосистемы Джет" обладает очень высокой технической квалификацией по всем продуктовым линейкам Brocade и является партнером Brocade в России и СНГ с 2003 года. Более 30 технических специалистов компании сертифицированы по направлениям Brocade SAN и IP. Сотрудники ВГТРК и компании "Инфосистемы Джет" блестяще справились с задачей разработки и реализации решения. Мы благодарны им за выбор Brocade в качестве платформы балансировки нагрузки».

В результате обеспечено бесперебойное распределение нагрузки на корпоративный почтовый сервис (общее число его пользователей в моменты пиковой нагрузки превышает несколько тысяч человек) и корпоративные информационные системы ВГТРК, в которых в пиковые часы работают несколько сотен пользователей единовременно.

ПОСТРОЕНИЕ ЕДИНОГО АНАЛИТИЧЕСКОГО ХРАНИЛИЩА ДАННЫХ О КЛИЕНТАХ ДЛЯ ГРУППЫ «АЛЬФАСТРАХОВАНИЕ»

«АльфаСтрахование» — один из крупнейших российских страховщиков, имеющих более 400 региональных представительств в России. Компания использует около 20 информационных систем, в которых в разном объеме ведется учет сведений о контрагентах. Отсутствие единого аналитического хранилища данных о клиентах затрудняло анализ имеющейся информации, а также решение задач по сопровождению процессов продаж, урегулированию убытков и др. В связи с этим «АльфаСтрахование» объявило открытый тендер, по результатам которого проект был доверен компании «Инфосистемы Джет».

Проект выполнялся поэтапно. В первую очередь была создана единая база полной и непротиворечивой информации о клиентах. Следующий крупный блок работ был связан с реализацией BI-отчетности, а также доработкой компонентов хранилища.

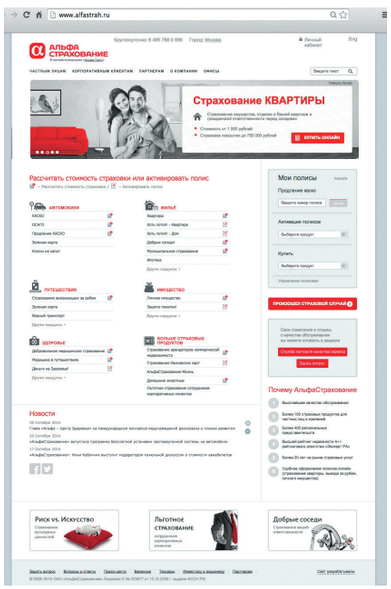
Было разработано несколько аналитических инструментов для различных целей: пролонгации клиентских договоров, поддержки кросс-продаж, а также получения разноплановой статистики (по видам продуктов, каналам продаж, клиентам и др.). BI-решение извлекает информацию о страхователе (из единой клиентской базы), его договорах и убытках (из учетных систем) и строит отчеты с требуемым составом полей. При этом права доступа к данным разграничены в соответствии с политиками информационной безопасности Группы «АльфаСтрахование», что снижает риски утечек информации.

Дополнительные данные для аналитики система также получает с сайта Группы, предназначенного для онлайн-продаж и активации полисов, и из системы обработки вызовов колл-центра. Это позволяет обогащать и актуализировать информацию о страхователях. В то же время клиенты имеют возможность просматривать все свои договоры и полисы из систем Группы «АльфаСтрахование» в личном кабинете страхователя на сайте alfastrah.ru.

Сегодня аналитическое хранилище активно используется для работы с физическими лицами. Процент актуальных контактных данных увеличился в среднем в 1,4 раза. В ближайших планах — развитие функционала для возможности обслуживания корпоративного сектора.

«За множеством разрозненных систем и договоров мы четко видим своего клиента, его потребности и возможности. Теперь мы можем эффективно персонализировать наши продукты и услуги. Это, пожалуй, главное достижение проекта, — отмечает **Андрей Педоренко, директор**

> Аналитическое хранилище включает единую базу страхователей, основные учетные системы (в том числе веб-портал и систему колл-центра) и BI-решение. Специалисты Группы получают в одном окне полную информацию о клиенте, его договорах и убытках, также они могут создавать аналитические отчеты со сложной комбинацией условий. Хранилище обеспечивает работу сотрудников фронт-офисов «АльфаСтрахование», аналитиков, менеджеров по контролю качества, маркетологов и других представителей компании в нескольких регионах России.



Департамента информационных технологий ОАО "Альфастрахование". — Другой плюс — снижение временных и трудовых затрат. Выборки клиентов, которые создавались по данным разных источников вручную, теперь формируются буквально в несколько кликов. Кроме того, у нас появился удобный инструмент для построения клиентской аналитики в разрезе учетных систем — раньше мы не могли этого сделать».

«Со стороны Группы "АльфаСтрахование" в проект были вовлечены как руководители, так и ключевые специалисты, поэтому сотрудничество получилось по-настоящему интересным и плодотворным. На каждом этапе бизнес четко обозначал требуемые KPI, например, в части повышения качества данных, и мы их достигали, — рассказывает **руководитель Центра компетенции по индустрии торговли и страхования компании "Инфосистемы Джет" Геннадий Махов.** — В конечном итоге решение крайне востребовано и приносит реальную выгоду бизнесу нашего партнера». JI

РЕСЕРТИФИКАЦИЯ ООО «МУЛЬТИКАРТА» НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

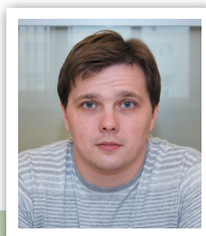
Проект затронул все основные системы и процессы, обеспечивающие безопасность хранения, обработки и передачи данных платежных карт. В ходе его реализации были учтены не только новые, более строгие требования стандарта PCI DSS, но и актуальные потребности «МультиКарты», связанные с необходимостью обеспечения непрерывности бизнеса и завершением работ по объединению с «ТрансКредитКард».

Основным партнером проекта стала компания «Инфосистемы Джет», обладающая статусами Qualified Security Assessor (QSA) и Approved Scanning Vendor (ASV). Эксперты компании провели комплексное обследование архитектуры и взаимодействия всех системных компонентов, входящих в состав сложной ИТ-инфраструктуры «МультиКарты». Она включает более 60 серверов, расположенных на двух площадках — в Москве и Санкт-Петербурге. Следующим шагом стали работы по совершенствованию и оптимизации существующих процессов в соответствии с новыми требованиями стандарта PCI DSS, которые осуществлялись с участием специалистов компании «МультиКарта».

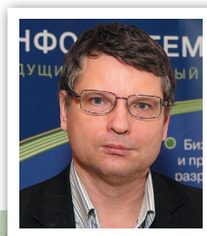
На завершающем этапе отдельная команда специалистов компании «Инфосистемы Джет» провела сертификационный аудит. Проводилась проверка систем, осуществляющих обработку и хранение данных платежных карт, регламентирующих документов и процедур, конфигураций используемых средств защиты. По результатам составлено заключение о полном соответствии процессинговых центров «МультиКарты» требованиям PCI DSS.

«В рамках проекта перед нами стояла задача не только успешной ресертификации компании "МультиКарта", но и наиболее безболезненного перехода к новой версии стандарта PCI DSS — 3.0. Поэтому помимо ежегодных и уже привычных для "МультиКарты" аудиторских проверок довольно весомой частью проекта стало внедрение организационных мер и процедур, а также технических средств обеспечения безопасности», — комментирует **Елена Козлова, руководитель направления Security Compliance Центра информационной безопасности компании «Инфосистемы Джет».** JI

ВНЕШНИЕ ИТ-РЕСУРСЫ – НЕЛЬЗЯ (,) ОТКАЗАТЬСЯ!



ИЛЬЯ КОШКИН,
менеджер по развитию бизнеса Центра проектирования вычислительных комплексов компании «Инфосистемы Джет»



ЮРИЙ ПАНЧЕНКО,
заместитель директора Сервисного центра по организации производства компании «Инфосистемы Джет»

Представим себе ситуацию: компания задумалась о том, чтобы внедрить ERP. На месте этих 3 букв может стоять другая аббревиатура – CRM, CAD, BI, SRM, CMS, EAM, MRM, GIS. С чего все начинается? С определения функциональности и требуемой производительности, причем нужно не только рассчитать ее на текущий момент, но и спрогнозировать перспективное развитие хотя бы на 3 года. Необходимо посмотреть на архитектуру железа, базовое и прикладное программное обеспечение, подумать над тем, как обеспечить RTO/RPO, катастрофоустойчивость, безопасность, привлечь высококвалифицированную проектную команду. Помимо этого, детально проанализировать несколько вариантов решения, предлагаемых производителями. Подумать, во сколько обойдется последующая эксплуатация. И мы еще не сделали самое главное – не убедили инвесторов или владельцев бизнеса в необходимости потратить бюджет именно на эту ИТ-систему.

А что ИТ-директор скажет бизнесу, когда спустя пару лет все так изменится, что нужно будет снова проводить аналогичные мероприятия? Ведь потраченные несколько миллионов уже не вернуть. При этом средства на поддержание решения так или иначе нужно расходовать.

Или другой вариант – ИТ-система нужна компании «еще вчера», а ресурсов под срочные задачи внедрения нет. На проектирование, поставку и монтаж оборудования, внедрение, тестирование решения и его введение в эксплуатацию в совокупности уйдет около полугода, а ждать некогда.

Иногда ИТ-ресурсы необходимы компаниям лишь на определенный срок – полгода, год, после чего они с большой долей вероятности будут висеть на балансе. Безусловно, если в подобных ситуациях идти по классическому пути наращивания инфраструктуры (свой ЦОД/colocation), в будущем это может обернуться существенными проблемами. Есть и другое решение – взять ИТ-ресурсы в аренду.

НАМ ЧУЖОГО НЕ НАДО?

У каждого пути – свой ЦОД, colocation, аренда вычислительных ресурсов – есть свои преимущества, недостатки и подводные камни. Подробнее рассмотрим каждый из них.

Для того чтобы носить звание ЦОДовладельца, для начала необходимо построить дата-центр или переоборудовать под него уже имеющееся помещение/здание. По времени это около полутора лет, по стоимости – приблизительно 2–3 млн долларов (мы рассматриваем ЦОД средних размеров – 100–120 м^2, уровня надежности TIER 3, наш опыт показывает, что каждый квадратный метр в нем стоит порядка 15–20 тыс. долларов). Но к внушительным CAPEX нужно прибавить OPEX – затраты на обслуживание дата-центра (на электроэнергию, воду и др.). Необходимо учитывать расходы на обучение и сертификацию специалистов, поддержание на высоком уровне их теоретических знаний и практических навыков эксплуатации инженерных систем ЦОД. С другой стороны, своя рубашка ближе к

Аренда вычислительных ресурсов наиболее актуальна для банковского сектора, ритейловых компаний и телеком-операторов. Средства, сэкономленные на долгосрочном строительстве ИТ-инфраструктуры, здесь и сейчас вливаются в оборот и начинают работать на бизнес. Другой момент: аренда позволяет компаниям максимально оперативно выводить на рынок новые услуги, опережая конкурентов. Не нужно ждать несколько месяцев, а то и полгода, пока сервис «взлетит», и терять драгоценное время. Например, маркетинг телеком-оператора предлагает запустить новый тариф «Все включено», для этого необходимо изменить биллинговую часть – внедрить отдельное специализированное приложение. Расширение своей ИТ-инфраструктуры проигрывает аутсорсингу вычислительных ресурсов в части оперативности поддержки бизнес-идей.

телу, а свой дата-центр — это гарантия сохранности конфиденциальных данных и полный контроль над ИТ-инфраструктурой в режиме реального времени.

Размещая железо у провайдера, компания снимает вопросы, связанные с построением и эксплуатацией своего дата-центра. При этом ИТ-инфраструктура по-прежнему остается за ней, соответственно, проектирование, закупка оборудования, инсталлирование, запуск, администрирование и т.д. — на ее стороне. Развертывание вычислительного комплекса займет несколько месяцев. Оперативно нарастить ИТ-ресурсы в случае необходимости не удастся, как и отказаться от них.

Аренда вычислительных ресурсов подразумевает, что в твоем распоряжении находятся производственные мощности, на которых ты можешь разворачивать свои бизнес-приложения. В этом случае не потребуются одномоментные серьезные капитальные затраты на покупку оборудования и ПО, которые за время разработки первого релиза продуктивной среды могут устареть и физически, и морально.

Можно заказать архитектуру под конкретные требования прикладной системы, при этом серьезно сэкономить, поскольку на первых этапах разработки ИТ-системы компании может быть предоставлена упрощенная конфигурация инфраструктуры. В случае редкой пиковой загрузки можно пользоваться дополнительными мощностями исключительно в «высокий сезон».

При этом проектная команда партнера, что называется, уже под парами и готова оперативно собрать новый ИТ-комплекс под те или иные задачи. Компания платит только за непосредственный результат. Отсюда же следует «свобода от эксплуатации»: обслуживание ЦОД — как инженерных, так и вычислительных систем — является заботой тех, кто предоставляет услуги. Как и обеспечение требуемой доступности, надежности и безопасности.

При желании можно и поэкспериментировать. Если разработка зашла в тупик и не сходится с требуемой функциональностью, или вообще стало понятно, что внедрение ИТ-системы в текущих условиях не даст экономического эффекта, потери от остановки внедрения будут минимальными. Это дает возможность попробовать то, чего еще нет у конкурентов, и быстро понять, что может обеспечить бизнес-преимущества. А затем оперативно встроить решение в корпоративный ИТ-ландшафт. Сколько времени потребуется на внедрение новой технологии при классическом подходе?

В случае аренды вычислительных ресурсов оборудование и ПО не числится на балансе, соответственно, нет необходимости в инвентаризации и амортизации. Не нужно заботиться о технической вендорской поддержке.

И наконец последнее, но от этого не менее важное преимущество аутсорсинга вычислительных ресурсов — прозрачная и гибкая финансовая модель. Конечно, при условии выбора адекватного партнера. Отсутствуют пики затрат, ты платишь только за то, что получаешь, как только отпала необходимость в таком сервисе, просто отказываешься от него.

Вроде бы, идеальная картина мира. Но вместе с тем есть моменты, о которых нельзя забывать. Аутсорсинг — эта всегда определенная зависимость от поставщика услуг. При его замене могут возникнуть сложности с миграцией сервисов. Если вы только начинаете сотрудничество, имеет смысл проверить партнера на простых продуктивных проектах или на начальной стадии внедрения новых ИТ-услуг.

ПЛАТИТЬ ПО СЧЕТАМ

Как соотносятся между собой расходы в случае традиционного подхода и аренды ИТ-ресурсов? Для наглядности возьмем бизнес-кейс крупной промышленной компании, которая активно развивается и планирует поддерживать заданный темп в течение ближайших 5 лет. По оценке ее ИТ-специалистов, для обеспечения потребностей бизнеса в течение этого срока потребуется увеличение вычислительных мощностей в 5 раз. На данный момент есть 6 стоек оборудования, через год потребуется 11 стоек, через два — 18, через три — 23, через четыре — 27 и через пять лет — 32 стойки. Перед компанией стоит выбор — построить новый ЦОД, воспользоваться услугами colocation-провайдера или арендовать ИТ-сервисы. За основу для расчетов мы взяли стоимость построения и обслуживания имеющегося ИТ-комплекса (6 стоек) и рассчитали условную стоимость одной готовой стойки. Вот что получилось:

Свой ЦОД

Построение ЦОД
~ $3 000 000

Закупка ИТ-оборудования для вычислительного комплекса (ВК)
~ $ 285 000 за стойку с учетом поддержки решений производителей в течение 1 года

Эксплуатация инженерных систем ЦОД
~ $ 150 000 в год

Эксплуатация ВК
~ $ 35 000 за стойку в год

Аренда дата-центра (colocation)

В этом случае две статьи расходов – строительство ЦОД и его обслуживание – входят в стоимость ежемесячного платежа за аренду стоек. Остальное остается неизменным:

Закупка ИТ-оборудования
~ $ 285 000 за стойку

Эксплуатация ВК
~ $ 35 000 за стойку в год

Аренда стоек
~ $ 48 000 за стойку в год (усредненная цифра по рынку)

Аренда готовых ИТ-сервисов на примере нашего ВЦОД

Все статьи расходов входят в один ежемесячный платеж: аренда аналогичного вычислительного комплекса
~ $ 168 000
за стойку в год

Формат	*Млн долларов*
Собственный ЦОД	5
Colocation	2,2
Аренда ИТ-ресурсов	1

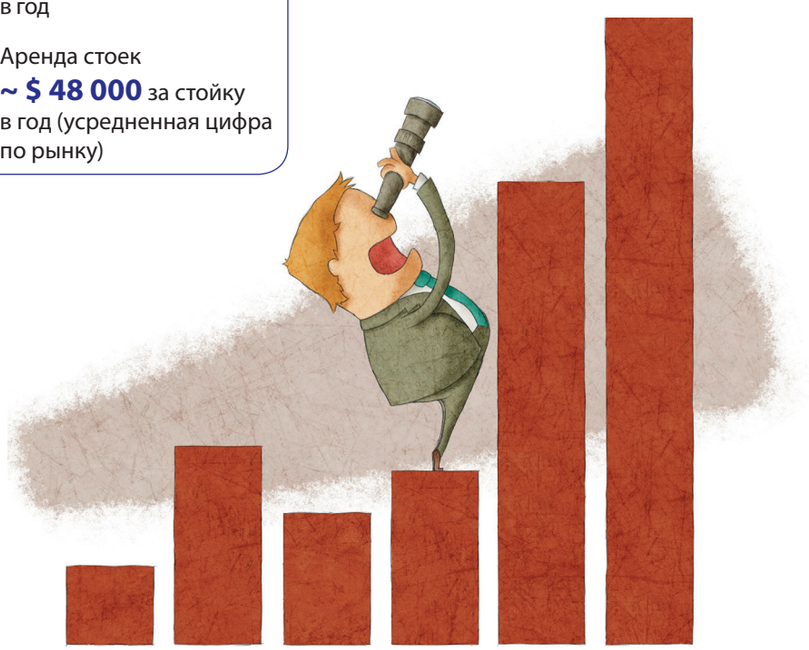


Рис. 1. Суммарные затраты за первый год (6 стоек)

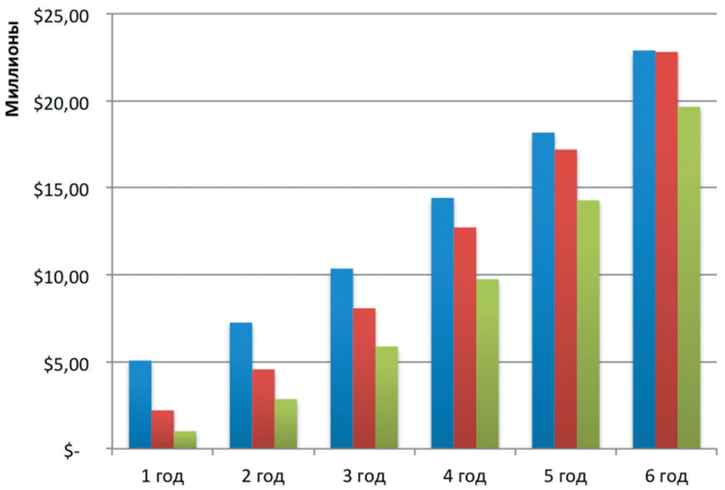


Рис. 2. Затраты на ИТ-ресурсы в течение 5 лет

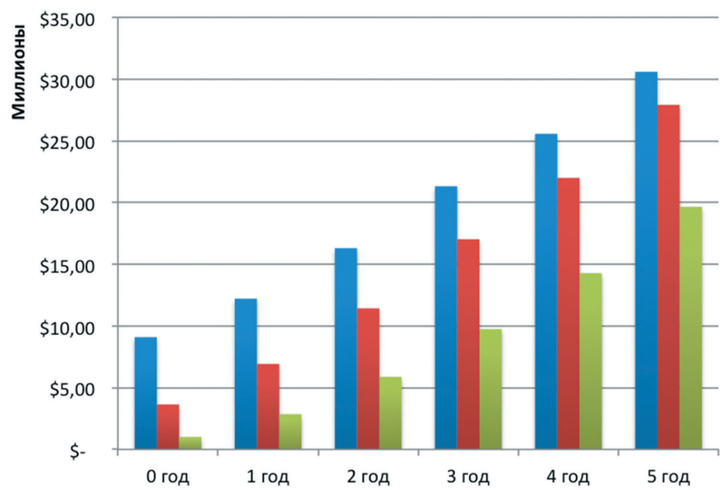


Рис. 3. Затраты на ИТ-ресурсы в течение 5 лет с учетом ставки кредитования (10%)

В последующие годы операционные затраты на свой ЦОД и colocation будут ниже (отпадает CAPEX), чем на аренду ИТ-ресурсов, однако суммарные расходы по-прежнему будут выше (см. рис. 2).

Мы брали усредненную стоимость обслуживания инженерных систем и вычислительного комплекса исходя из своего опыта. Также необходимо учесть, что оборудование с течением времени устаревает и рано или поздно потребуется его модернизация. Можно предположить, что через 3 года эксплуатации вычислительного комплекса потребуется модернизировать 25% существующего оборудования.

При этом мы не учитывали ряд финансовых аспектов, которые имеют высокую значимость при рассмотрении вариантов дальнейшего развития компании. Например, возьмем ставку кредитования: она показывает, что потраченные 5 лет назад 100 долларов сейчас стоят порядка 150. Так как при традиционном подходе существенная часть расходов приходится на капитальные затраты на старте проекта (строительство ЦОД, закупка оборудования), фактически создание своего дата-центра или вариант colocation будут еще более затратными (см. рис. 3).

***

По сравнению с классическим подходом и использованием colocation аутсорсинг вычислительных мощностей в ряде случаев более конкурентоспособен — он дает быстрое, качественное и при этом весьма эффективное по стоимости решение в части внедрения новых ИТ-сервисов. В современном быстро меняющемся мире эти характеристики реализации ИТ-проектов обеспечивают компании конкурентное преимущество. JI

МАСС-МАРКЕТ

ИНДИВИДУАЛЬНЫЙ ПОШИВ

ИЛЬЯ КОШКИН,
менеджер по развитию бизнеса Центра проектирования вычислительных комплексов компании «Инфосистемы Джет»

АЛЕКСЕЙ УЧАМПРИН,
директор по развитию сервисов ВЦОД компании «Инфосистемы Джет»

Арендовать ИТ-ресурсы можно у разных поставщиков — у хостеров, облачных провайдеров, а также у системных интеграторов, предоставляющих услуги формата «ЦОД как сервис». Что получает компания в каждом из этих случаев? Хостеры традиционно предлагают аутсорсинг вычислительных ресурсов (модель IaaS) — выделенные виртуальные или физические серверы, облачные услуги. При этом их специалисты, как правило, не обладают глубокими компетенциями и не могут вести проектную деятельность — сконфигурировать ИТ-комплекс под конкретную компанию.

Облачные провайдеры, особенно гиганты этого рынка — Amazon, Google, ориентируются на SMB-сектор, т.е. на массовое обслуживание непрерывного потока средних и небольших компаний. Качество их услуг может быть достаточно высоким, но при этом отсутствуют серьезные гарантии безопасности и непрерывности предоставления сервисов. Если компанию не устраивают подобные условия, всегда найдется другой, не столь требовательный клиент. Ради специализированных запросов конкретного пользователя услуг провайдер не будет перестраивать весь процесс предоставления сервиса. При этом поставщик облачных услуг способен обеспечить гранулярность учета на уровне минут — компания платит ровно за тот объем услуг, который потребила.

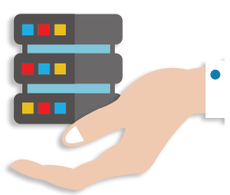
Интеграторы, предоставляющие ИТ-ресурсы в аренду, практически всегда ориентируются на Enterprise-сегмент, соответственно, они индивидуально подходят к задачам компании, не ограничиваясь предоставлением типовых вычислительных ресурсов. Собственно аренду предваряет проектирование ИТ-комплекса, удовлетворяющего конкретным потребностям заказчика. Внутри ЦОД интегратора «под ключ» создается окружение, в котором располагаются все выделенные компании ИТ-ресурсы. Таким образом, партнер обеспечивает проектирование, построение, техподдержку, администрирование и мониторинг ИТ-инфраструктуры/ИТ-сервисов компании (модель IaaS, PaaS или SaaS), при необходимости осуществляет конфигурирование систем. В результате компания получает всё как единый сервис «из коробки», за эффективное функционирование которого полностью отвечает интегратор.

Здесь напрашивается аналогия из далекого от ИТ мира fashion-индустрии. Хостеров и облачных провайдеров можно сравнить с магазинами масс-маркета — колоссальный выбор одежды по готовым лекалам, как следствие, отсутствует возможность выбрать ткань, подогнать модель под себя и т.д. Системные интеграторы же — это индивидуальный пошив под конкретного клиента, посадка точно по фигуре. Те же принципы заложены в основу работы виртуального ЦОД (ВЦОД) нашей компании.

ВЦОД является платформой для целого портфеля наших аутсорсинговых услуг. Помимо распространенных услуг семейства IaaS мы предоставляем PaaS и SaaS. В последнюю категорию, в том числе, входит наш аутсорсинговый центр безопасности JSOC, развернутый на базе ВЦОД. Рассмотрим предоставляемые сервисы более подробно (JSOC в нашем номере посвящена отдельная статья, так что в этом обзоре он принимать участия не будет).

IaaS

Приобретая инфраструктуру как сервис, компания получает ИТ-комплекс, обладающий требуемой производительностью и отвечающий необходимым для бизнеса параметрам доступности (SLA). Главное отличие нашей услуги от аналогичных предложений конкурентов состоит в том, что мы предоставляем не набор элементов инфраструктуры (виртуальные машины + пространство в СХД), а законченную работающую инфраструктуру, полностью отвечающую потребностям компании. При этом и первоначальное «конструирование» ИТ-комплекса, и его дальнейшее расширение происходит за счет элементов, уже размещенных и работающих в нашем ВЦОД. Такой подход позволяет минимизировать время предоставления готовой инфраструктуры —



компания получает ее в свое распоряжение буквально за считанные дни. На нашей стороне:

1) подготовка и предоставление инфраструктуры в соответствии с требованиями бизнеса;

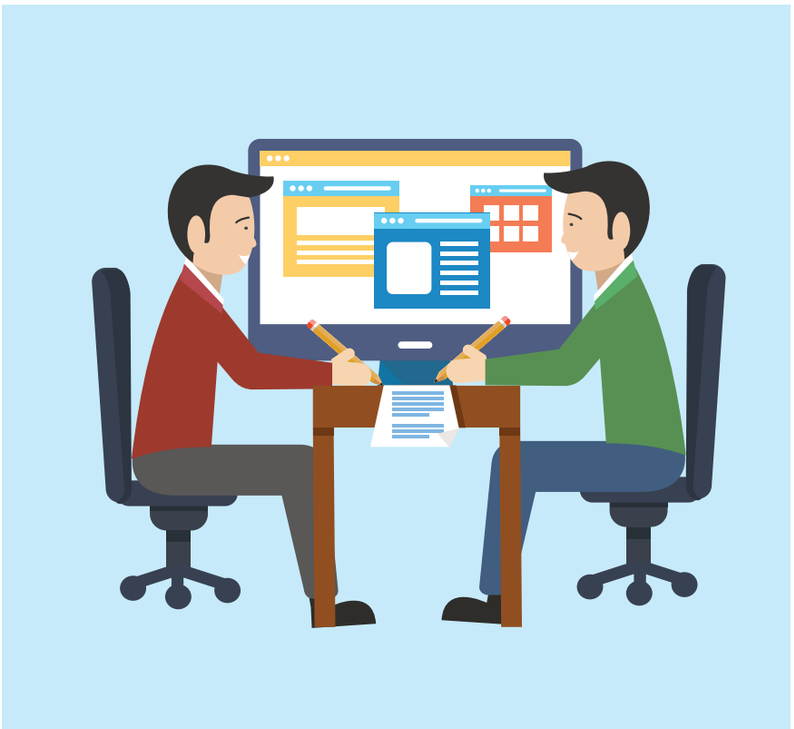
2) эксплуатация инфраструктуры, операционных систем и общесистемного ПО. Она включает:

- ☑ круглосуточный мониторинг состояния здоровья как элементов инфраструктуры, так и операционных систем и общесистемного ПО;
- ☑ оперативное устранение возникающих инцидентов выделенной командой сотрудников;
- ☑ администрирование ОС и общесистемного ПО;
- ☑ оперативное изменение вычислительных мощностей, потребляемых инфраструктурой.

Отметим, что IaaS является своего рода базой для прочих услуг, предоставляемых на платформе ВЦОД. Используя ее, компании получают высоконадежные ИТ-комплексы под продуктивные бизнес-приложения и высокую скорость разворачивания инфраструктур под тестовые среды и среды разработки. Кроме того, возможно создание резервных сред для продуктивных бизнес-приложений.

Характерный пример использования нашего ВЦОД — разворачивание в нем среды разработки для CRM-системы одной из российских транспортных компаний. На момент старта проекта у заказчика отсутствовали необходимые вычислительные мощности, поэтому фактор оперативного предоставления ИТ-ресурсов с нашей стороны стал решающим при выборе партнера. В данный момент разработка подходит к концу, параллельно идет инсталляция оборудования в дата-центре компании.

Крупная ритейловая компания арендовала вычислительные мощности в нашем ВЦОД на время строительства своего второго дата-центра. Дело в том, что в ее первом ЦОД закончилось место в стойках, при этом бизнес требовал расширения ИТ-ландшафта для решения своих задач. Таким образом, ритейлер не ждал появления второй площадки (а это полтора года) и получил необходимые ИТ-ресурсы здесь и сейчас.



Резервное и архивное копирование как сервис

Услуга предназначена для управления резервными копиями (РК) данных, обрабатываемых как на инфраструктуре ВЦОД, так и на собственных площадках компании (причём и на серверах, и на рабочих станциях). Это возможность гарантированного восстановления консистентных данных в полном объеме и в соответствии с заданными параметрами глубины хранения и частоты создания резервных копий. Компании не составит труда восстановить данные по состоянию на любой момент создания РК, при этом сам процесс восстановления происходит в течение гарантированного времени. Работоспособность процесса создания РК гарантируется круглосуточной службой мониторинга и эксплуатации ВЦОД. На нашей стороне:

- ☑ предоставление инфраструктуры из состава оборудования ВЦОД под систему резервного копирования и ее настройка в соответствии с требованиями бизнеса;
- ☑ круглосуточный мониторинг процесса создания РК и оперативное устранение возникающих инцидентов;
- ☑ хранение резервных копий;
- ☑ восстановление данных из РК по требованию компании.

Резервный ЦОД

РЦОД как услуга призван повысить катастрофоустойчивость ИТ-сервисов — обеспечить возможность восстановления их работоспособности на удаленной площадке. В зависимости от требуемых SLA используются различные средства для переноса данных, обеспечения доступности ИТ-сервисов и способы восстановления ИТ-систем.

Мы предоставляем инфраструктуру и ПО из состава оборудования ВЦОД и настраиваем ее в соответствии с требованиями бизнеса, обеспечиваем круглосуточный мониторинг доступности резервного дата-центра. Восстановление работоспособности ИТ-систем в РЦОД происходит по требованию компании или в автоматическом режиме.

PaaS

SAP Hosting

Наш ВЦОД — один из немногих дата-центров в России, официально сертифицированный в соответствии с требованиями SAP Hosting Provider. Приобретая услугу, бизнес получает в свое распоряжение платформу SAP, гарантированно функционирующую с заданными параметрами доступности. По сути, компания может перестать заботиться об администрировании своей ERP и сосредоточиться на реализации в ней непосредственных требований бизнес-подразделений.

Мы производим расчет вычислительных мощностей, необходимых для стабильной работы всех компонент платформы SAP, на основе бизнес-показателей, которые предоставляет компания. Под рассчитанные мощности происходит формирование как виртуальной, так и физической (в случае использования SAP HANA Appliance, например) инфраструктуры.

Далее происходит миграция платформы SAP с существующей инфраструктурной площадки компании в ВЦОД. Миграция продуктивной прикладной системы (а в случае с SAP речь идет, как правило, о системе уровня обслуживания mission critical) всегда является наиболее болезненным процессом в проектах обновления инфраструктурных площадок. В нашем случае планирование и саму миграцию осуществляет команда, обладающая большим опытом выполнения подобных проектов. При этом мы несем 100%-ную ответственность за результаты миграции. Следующий шаг — это установка платформы SAP и внедрение подсистемы SAP Basis.

В тех случаях, когда происходит разворачивание системы «с нуля», мы выполняем установку требуемых компонент платформы и внедрение подсистемы SAP Basis, которое включает:

- установку подсистемы, включая первоначальную базовую настройку;
- разработку и настройку транспортного ландшафта;
- разработку и настройку концепции полномочий;
- подготовку документации по подсистеме.

Отвечая за эксплуатацию платформы, мы выполняем круглосуточный мониторинг состояния не только ее инфраструктурной части, но и самого прикладного ПО. Кроме того, услуга включает устранение возникающих инцидентов (на основании как запросов от компании, так и показателей системы мониторинга) и администрирование SAP Basis, в том числе планирование изменений в конфигурациях ПО, анализ производительности подсистемы, планирование и проведение экспорта данных в тестовую среду по требованию компании и др.

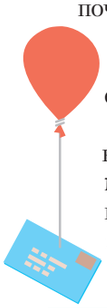
В данный момент платформа SAP, «прописанная» в нашем ВЦОД, решает бизнес-задачи одного из крупнейших российских ритейлеров.

> Безопасность ВЦОД обеспечивается как физически (пропускной режим, выделенная огороженная площадь), так и технологически: современные комплексы организационных и технических мер обеспечивают надежную защиту данных от внутренних и внешних угроз. Для изоляции данных заказчиков в виртуальной среде дата-центра используются архитектурные решения по разделению контекстов — контексты безопасности, VLAN, vRF, vFiler. Доступ к внутренним сегментам сети и весь внешний периметр виртуального ЦОД контролируется межсетевыми экранами. Отдельно стоит сказать о создании в нашем ВЦОД инфраструктуры, сертифицированной по требованиям российского законодательства и международных стандартов защиты персональных данных (№ 152-ФЗ, PCI DSS и др.). Это выделенная часть ВЦОД — периметр, закрытый дополнительными средствами защиты и соответствующий более жестким политикам безопасности.

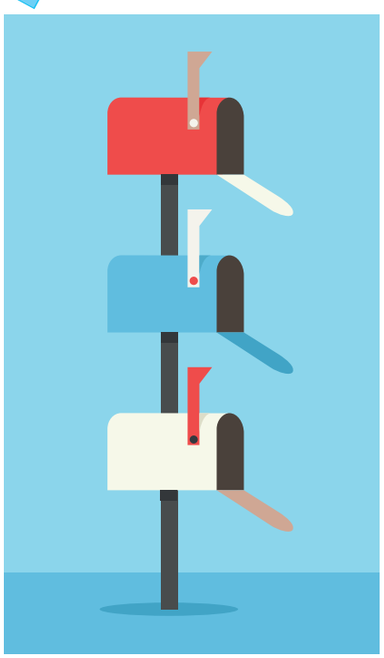
SaaS

Почта как сервис

Компания получает в свое распоряжение почтовую систему на базе MS Exchange, функционирующую с заданными параметрами доступности. Как следствие, не нужно заботиться о настройках анти-спама и антивируса, о заведении новых учетных записей (почтовых ящиков) и удалении неактуальных, об архивировании почтовых баз.



Мы предоставляем инфраструктуру, интегрируем почтовую систему в информационный ландшафт компании и осуществляем миграцию почтовых ящиков из существующего у заказчика приложения.



Система Service Desk как сервис

Компания получает в распоряжение комплексную ITSM-систему, обеспечивающую автоматизацию процессов управления запросами и инцидентами, изменениями, ИТ-активами, качеством предоставления услуг и т.д. Использование системы Service Desk как SaaS гарантирует высокую скорость развертывания решения (срок запуска системы с загрузкой данных и обучением пользователей может составлять 2–4 недели). Кроме того, отсутствуют затраты на ее развертывание и эксплуатацию. На наши плечи ложатся все задачи, связанные с работоспособностью оборудования, его отказоустойчивостью, установкой обновлений и новых версий ПО, резервным копированием. При этом есть четкие и измеряемые показатели качества работы системы, такие как отклик сервера приложений, скорость открытия страниц и пр.

Мы обеспечиваем развертывание контуров разработки и тестирования системы в случае необходимости ее доработки. Выполняем настройку решения под потребности компании. Кроме этого, предоставляем дополнительные вычислительные ресурсы на период обновления версий для обеспечения миграции системы без существенных простоев.

На базе Service Desk также могут быть созданы новые бизнес-ориентированные приложения, обеспечивающие развитие модели предоставления услуг внутри компании в интересах всех подразделений, — система автоматизации заявок в административно-хозяйственных подразделениях, система заказа обучения и пр.

***

Таким образом, использование услуг ВЦОД позволяет оперативно получать необходимые ИТ-сервисы и гибко изменять их с сохранением гарантированных показателей производительности и уровня доступности (SLA). JI

ЗАМЕТКИ НА ПОЛЯХ

ВЦОД КАК АУТСОРСИНГОВАЯ ПЛАТФОРМА

АЛЕКСЕЙ УЧАМПРИН

Идея ИТ-аутсорсинга не нова — только в нашей стране она активно развивается уже, как минимум, лет 10. В то же время само понятие аутсорсинга до сих пор допускает неоднозначное толкование. Под этим порой подразумевают оформление штата ИТ-подразделения в отдельную сервисную компанию и заключение с ней договора на предоставление услуг. Ключевое слово здесь — «услуги», или, как сейчас принято говорить, «сервисы». Можно с уверенностью сказать: для того чтобы появилась сама возможность передачи чего-либо на аутсорсинг, это что-то должно обладать характеристиками услуги.

Другими словами, должно быть однозначное описание того, что получает компания в виде услуги. Заказчик при этом платит ровно за тот объем сервисов, который он «потребил», имеет возможность получить их максимально быстро и просто, так же легко он может изменить их объем. И последнее — услуга должна иметь внятные критерии оценки качества.

Казалось бы, описать продукт деятельности любого интегратора, предоставляющего услуги ИТ-аутсорсинга, в соответствии с приведенными выше критериями, не составляет большого труда. Но реальность с теорией расходятся кардинально. Основные причины, из-за которых зачастую невозможно предоставлять услуги ИТ-аутсорсинга именно в виде сервисов – это:

- **ограниченная гибкость услуг:** компании на практике не всегда могут оперативно управлять объемом предоставляемых им сервисов;
- **ограниченность схем оплаты**: компания зачастую не может платить ровно за потребленный объем услуг. Да и корректно посчитать его порой бывает весьма затруднительно.

Наиболее полно эти проблемы проявляются в части аутсорсинга вычислительных комплексов. Эта область наименее гибкая, но при этом наиболее востребованная на рынке. Отдать на аутсорсинг оборудование и все, что «вокруг» (обслуживание, поддержка и т.п.), – это первое, что приходит на ум практически любому CIO независимо от размера компании, в которой он работает.

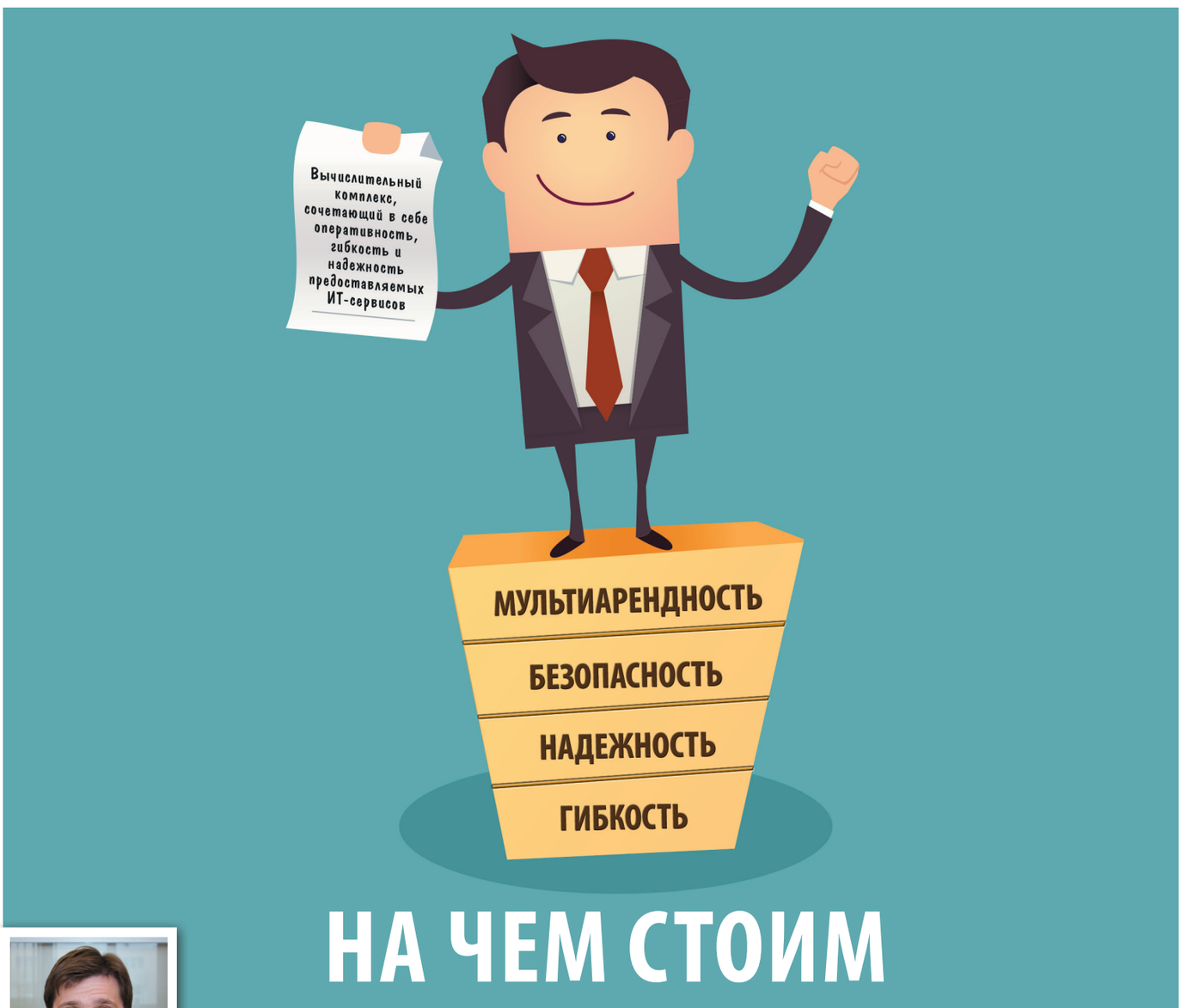
Практически единственный действенный способ, с помощью которого интегратор может устранить проблемы недостаточной гибкости этой услуги, – создание собственного, разделяемого между компаниями-заказчиками пула вычислительных мощностей. При этом «степень атомарности» ресурсов должна быть достаточно высокой – до процессорного ядра и гигабайта сетевого хранилища данных. К этим же «квантам» мощностей должна привязываться и модель оплаты за их потребление (напрашивается давно забытая аналогия – оплата процессорного времени в ГИВЦ того или иного НИИ). Таким образом, чтобы обеспечить реальную гибкость услуги аутсорсинга вычислительных мощностей, интегратору необходимо иметь собственный ЦОД.

Собственно, мы пошли по такому пути. Теперь компании могут оперативно менять объем потребляемых сервисов и платить ровно за используемые вычислительные ресурсы. То есть речь идет о предоставлении услуг семейства IaaS.

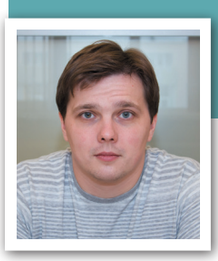
С точки зрения «техники» предоставления услуги мы далеко не первопроходцы – конкуренты относительно давно предлагают вычислительные мощности из облаков.

Наше основное преимущество – в высоком качестве сервисов, чему способствует накопленный опыт предоставления услуг по аутсорсингу ИТ-инфраструктуры. Эти же принципы распространяются на все аутсорсинговые услуги, предоставляемые на платформе ВЦОД. Кроме «пакета» вычислительных мощностей, это выделенная инфраструктура любой сложности, которая также может быстро идти в рост. Один из примеров – предоставление инфраструктуры для разрабатываемой АБС «Лето Банка». Банк воспользовался временной инфраструктурой для проведения разработки, тестирования и отладки перспективной АБС, при этом не инвестировал дополнительные средства в оборудование и никоим образом не затрагивал свой продуктив.

Помимо тестовых и перспективных систем, в нашем ВЦОД «живут» и продуктивные высоконагруженные mission critical системы. JI



НА ЧЕМ СТОИМ



ИЛЬЯ КОШКИН,
менеджер по развитию бизнеса Центра проектирования вычислительных комплексов компании «Инфосистемы Джет»

Реализация вычислительного комплекса, сочетающего в себе оперативность, гибкость и надежность предоставляемых ИТ-сервисов, была непростой задачей. Чтобы построить такую платформу, нам необходимо было учесть несколько моментов.

Первый аспект — это **«мультиарендность»** (multitenancy). Инфраструктура должна предоставлять возможность совместной и в то же время изолированной работы большого количества компаний. Совместное использование единой инфраструктуры обеспечивает существенную экономию

в части приобретаемых ресурсов, при этом данные должны быть разделены на всех уровнях – ПО, виртуализации, систем хранения данных и сети (см. рис. 1)

В нашем ВЦОД для разделения данных на уровнях ПО и виртуализации используются встроенные функции: создание отдельных виртуальных сущностей, которые изолированы друг от друга. В качестве гипервизоров применяются VMware и Oracle VM. Выбор последнего решения обусловлен упрощенной схемой лицензирования для СУБД. Она позволяет лицензировать только виртуальные машины, в которых будет располагаться СУБД, а не весь набор серверов, используемый в пуле виртуализации, при этом все стандартные функции гипервизора присутствуют и работают исправно.

Для разделения данных на уровне СХД мы используем технологии от NetApp – vFilers и IPSpaces. Первая позволяет создавать виртуальные массивы, доступные по разным IP-адресам в различных VLAN (Virtual Local Area Network), через которые каждая компания может получать выделенные только для нее дисковые ресурсы по протоколам NFS/CIFS/iSCSI. Вторая (IPSpaces) дает возможность компаниям иметь одинаковые пространства IP-адресов без конфликтов внутри СХД.

Разделение данных на сетевом уровне происходит стандартными способами: есть VLAN, VRF (Virtual Routing and Forwarding) и виртуальные контексты, позволяющие разделить трафик как на входе, так и внутри ИТ-инфраструктуры.

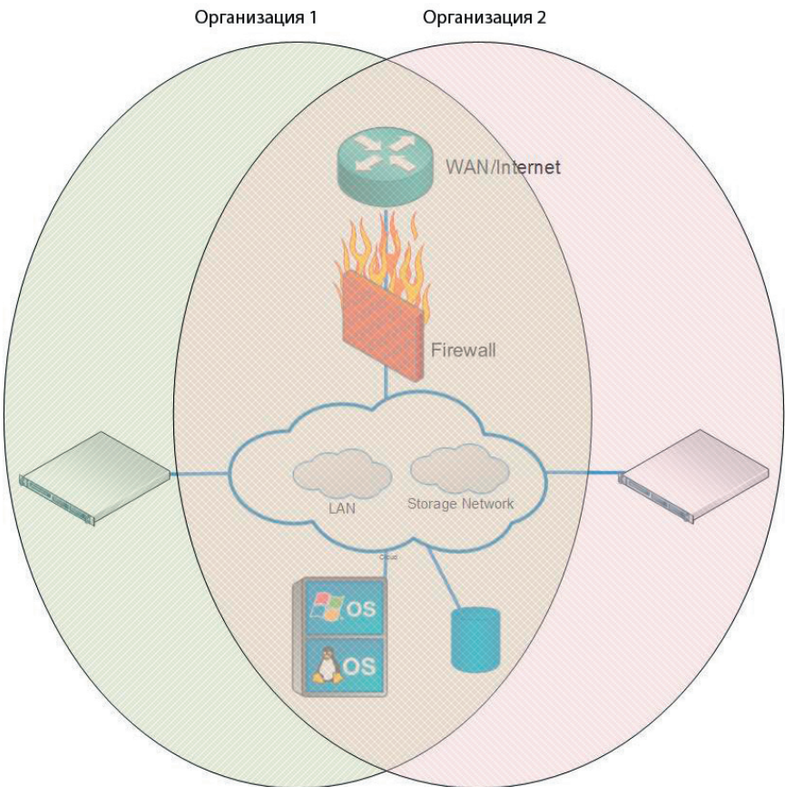


Рис. 1. Общая схема реализации мультиарендности

Второй момент – это **гибкость** использования ИТ-сервисов. Она подразумевает возможность легкого изменения количества потребляемых ресурсов в зависимости от потребностей бизнеса. Для этого всегда должен существовать запас вычислительных ресурсов, т.е. инфраструктура должна иметь возможность горизонтально масштабироваться. Для этого мы используем стандартизованные блоки оборудования – за счет них происходит расширение ИТ-инфраструктуры. Такой подход упрощает и управление.

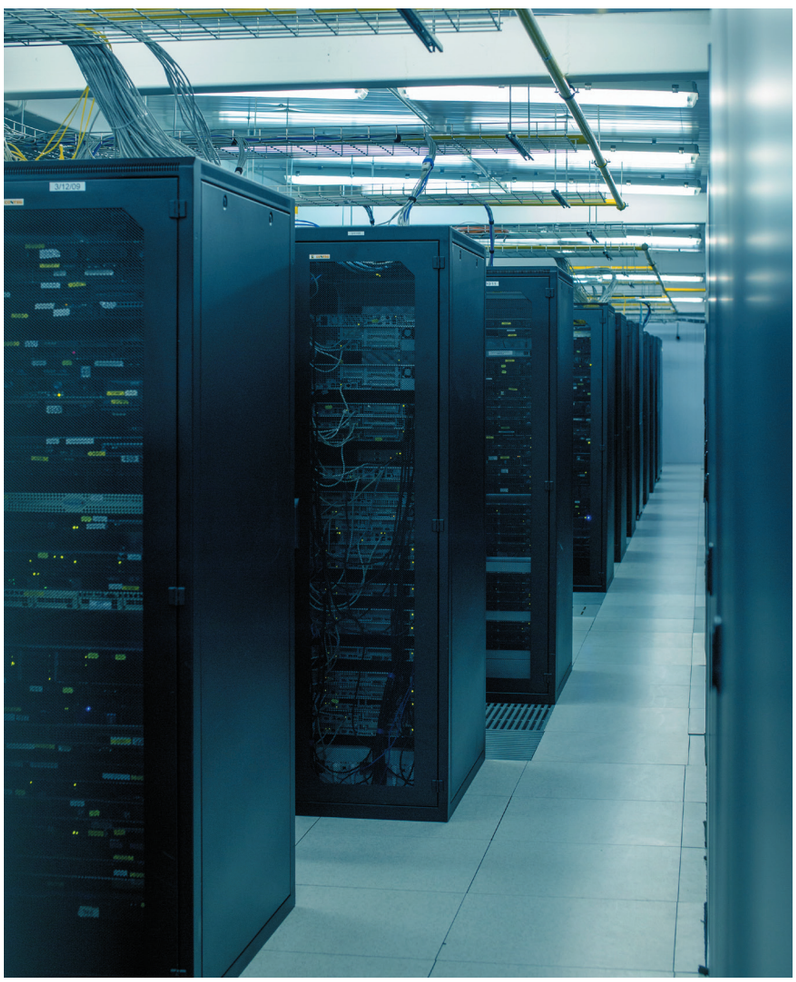
Сеть построена по технологии 10GbE. Это, во-первых, избавило нас от узких мест в сетевом взаимодействии – как между разными виртуальными машинами, так и между ВМ и СХД. Во-вторых, нам не нужен SAN. Нет лишних HBA (Host Bus Adapter) и портов в массивах, дополнительных коммутаторов. Это также облегчает масштабируемость и упрощает управление инфраструктурой, тем самым повышается ее гибкость.

Еще один приоритет – **надежность.** Для обеспечения работоспособности корпоративных бизнес-приложений и ИТ-систем необходимо реализовать инфраструктуру без единых точек отказа, позволяющую проводить любые регламентные работы без прерывания сервиса. Желательно создание ИТ-комплекса на базе нескольких ЦОД для обеспечения катастрофоустойчивости.

Вычислительный комплекс нашего ВЦОД спроектирован таким образом, что все железные компоненты задублированы и не имеют единых точек отказа, а технологии виртуализации и кластеризации позволяют проводить миграцию ИТ-сервисов прозрачно для бизнес-приложений. На данный момент мы предоставляем услуги ВЦОД на базе двух разных дата-центров.

Естественно, нужно помнить и о таком аспекте, как **безопасность.** Помимо того, что данные разных компаний должны быть разделены на всех уровнях, необходимо обеспечить защищенный доступ авторизованных пользователей (и только их) к ресурсам, защиту от возможных взломов и вторжений и своевременную реакцию на возникающие угрозы.

При разработке архитектуры ВЦОД и процессов обеспечения безопасности мы учитывали требования как российского законодательства (№152-ФЗ) и международных стандартов (PCI DSS 2.0), так и лучшие мировые практики в области ИБ (CIS, SANS, NIST). Для обеспечения информационной безопасности в нашем ВЦОД внедрен комплекс технических решений, исключающий несанкционированный доступ к данным. Физические компоненты ВЦОД расположены в дата-центре, который соответствует всем требованиям, предъявляемым к обеспечению физической безопасности. Кроме того, в нашей компании проводятся регулярные внутренние аудиты ИБ, результаты которых используются в процессе улучшения системы обеспечения информационной безопасности ВЦОД. JI



ВНЕШНЯЯ ПОДУШКА БЕЗОПАСНОСТИ

ВЛАДИМИР ДРЮКОВ,
руководитель направления аутсорсинга ИБ Центра информационной безопасности компании «Инфосистемы Джет

Сегодня уже никому не нужно доказывать, зачем крупной российской компании необходим центр по мониторингу и реагированию на инциденты информационной безопасности (SOC). Практически каждую неделю в ИТ-прессе появляются статьи, исследования и мнения экспертов на эту тему. Гораздо интереснее посмотреть на статистику. Так, в компании со штатом от 1 до 5 тысяч сотрудников SOC в течение года фиксирует около 90 млн событий ИБ, более 15 тысяч событий с подозрением на инцидент и около 100 реальных инцидентов ИБ. Есть и другие, еще более негативные данные: общий объем потерь от инцидентов ИБ в 2013 году составил $ 25 млрд. При этом в крупной компании в среднем используется не менее 15 разнородных средств защиты, не более чем в 7 из них проводится активный анализ журналов для выявления инцидентов.

В то же время приходится констатировать, что собственный SOC — это дорогое удовольствие. Необходимо учитывать капитальные финансовые затраты на его построение и расширение штата ИБ-службы для эффективного ведения соответствующих процессов. Имеет смысл рассмотреть вариант использования SOC в формате ИБ-аутсорсинга — наш Jet Security Operation Center.

JSOC как услуга относится к категории SecaaS (Security as a Service) и состоит из нескольких основных компонентов. На площадке компании устанавливаются 1–2 сервера сбора событий аудита с целевых систем. Как правило, это средства защиты (антивирусы, VPN, межсетевые экраны, прокси-серверы), инфраструктурные системы (Active Directory, сетевое оборудование) и наиболее критичные с точки зрения ИБ бизнес-приложения. События обрабатываются и нормализуются, после чего по защищенному каналу передаются в ядро JSOC, располагающееся непосредственно в нашем виртуальном ЦОД.

В ядре все полученные события обрабатываются по большому количеству правил и сценариев, позволяющих нам определять подозрительные и аномальные активности в сети компании и тем самым выявлять инциденты ИБ. По факту выявления инцидента наша круглосуточная дежурная смена самостоятельно проводит его анализ, фильтрацию ложных срабатываний и в короткие сроки (по критичным инцидентам — в течение 30 минут) готовит аналитическую справку для специалистов компании о выявленном инциденте. Она включает информацию о том, какой инцидент произошел, что стало его причиной, какое влияние он может иметь на бизнес-процессы и информационную безопасность, и какие меры необходимо предпринять, для того чтобы заблокировать или хотя бы минимизировать ущерб.

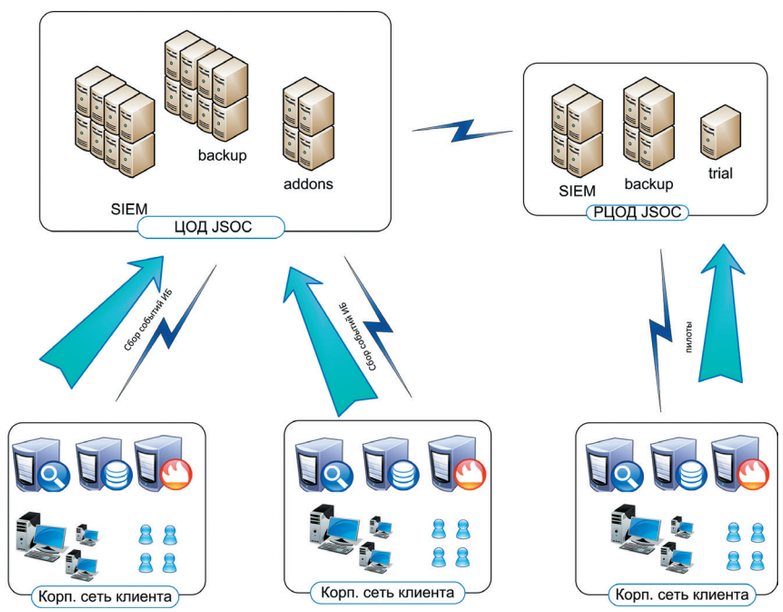


Рис. 1. Верхнеуровневая схема оказания сервиса

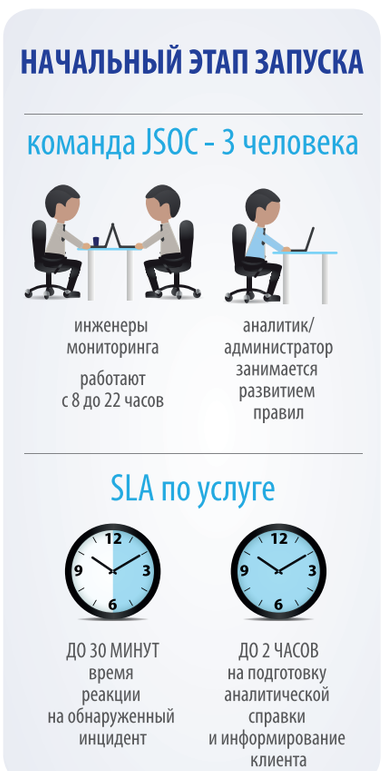
Как уже говорилось, JSOC базируется в нашем ВЦОД. Почему мы поселили его именно там? Опыт наших западных коллег показывает, что целевая доступность архитектуры SOC должна составлять не менее 99,5% (причем с максимальной катаклизмоустойчивостью). При этом принципиален и вопрос географии: colocation возможен только в границах России. Это исключило для нас возможность сотрудничества с популярными западными провайдерами. Одновременно встали вопросы обеспечения информационной безопасности инфраструктуры на всех уровнях доступа, и выбора у нас по большому счету не осталось: мы обратились к команде нашего ВЦОД. Для JSOC специально выделили фрагмент, где мы смогли развернуть свою архитектуру, одновременно ужесточив уже существующие в рамках ВЦОД профили безопасности.

ИТ-инфраструктура развернута в Tier 3 дата-центре нашей компании, и ее показатели доступности составляют 99,8%. В результате мы получили целевые показатели доступности нашего сервиса и существенную свободу действий в работе и адаптации системы под себя.

Объем потребляемых нами вычислительных мощностей сейчас исчисляется несколькими сотнями Гб оперативной памяти и 200 Тб дискового пространства. Архитектура ВЦОД и выстроенная коммуникация с его командой позволяют нам очень спокойно относиться к планированию вычислительных мощностей: процесс масштабирования проходит очень прозрачно и оперативно.

ОХОТНИКИ ЗА ИНЦИДЕНТАМИ ИБ

На начальном этапе запуска услуги команда JSOC состояла из 3 человек: двух инженеров мониторинга, закрывающих временной интервал с 8 до 22 часов, и одного аналитика/администратора, который занимался развитием правил. SLA по услуге, обозначенный компаниям, тоже был достаточно мягким: время реакции на обнаруженный инцидент — до 30 минут, время на разбор, подготовку аналитической справки и информирование клиента — до 2 часов. Но по прошествии первых месяцев работы мы сделали несколько очень существенных выводов.



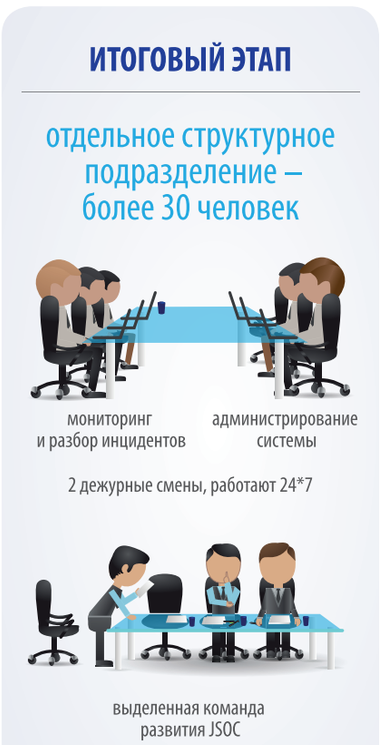
Смена мониторинга должна обязательно работать в режиме 24*7. Несмотря на существенно меньший объем инцидентов в вечерние и ночные часы, самые важные и критичные события (старт DDoS-атак, завершающие фазы таргетированных атак, злонамеренные действия контрагентов и т.п.) происходят все же именно в ночное время и к моменту старта утренней смены уже теряют свою актуальность.

Время разбора критичного инцидента не должно превышать 30 минут. В противном случае шансы на его предотвращение или существенную минимизацию ущерба катастрофически падают.

Для обеспечения требуемого времени разбора под каждый инцидент должен быть подготовлен полноценный инструментарий для его расследования: active channels с отфильтрованными целевыми событиями для разбора, тренды, демонстрирующие статистические изменения в подозрительных активностях и целевые аналитические отчеты, позволяющие быстро анализировать активности и принимать оперативные решения.

Команда администрирования средств защиты наших клиентов должна быть отделена от группы мониторинга и выявления инцидентов. В противном случае риск влияния человеческого фактора в цепочке «выполнил изменения конфигурации — зафиксировал по факту инцидент — отметил ложным срабатыванием» мог существенно сказаться на качестве нашей услуги.

На практике все эти выводы вылились в создание в нашей компании отдельного структурного подразделения, ориентированного на трехуровневую модель обеспечения каждой задачи: как мониторинга и разбора инцидентов, так и администрирования средств защиты. Сейчас подразделение насчитывает уже более 30 человек. Это 2 дежурные смены, которые работают 24*7 (одна занимается мониторингом и разбором инцидентов, другая — администрированием системы) и выделенная команда развития JSOC.

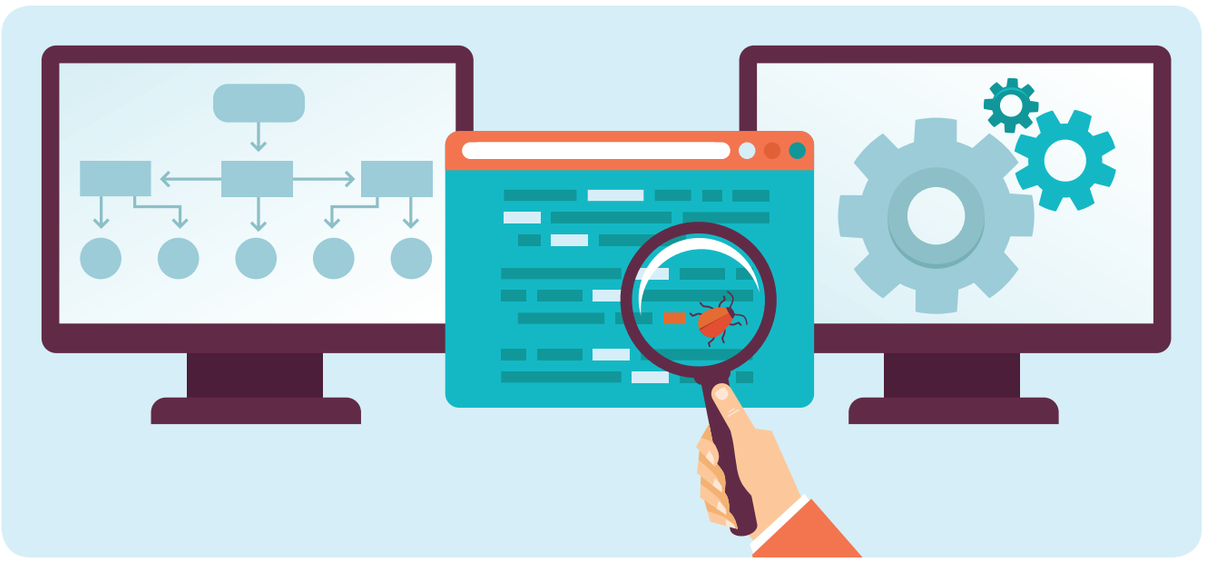


ОТЛОВ ПОШЕЛ

Задачи, которые сейчас закрывает JSOC, можно разделить на три больших класса.

1 Закрытие нормативных или внутренних требований информационной безопасности

Требования многих отраслевых стандартов определяют необходимость выявления и разбора инцидентов ИБ. Самым регулируемым на данный момент является банковский стандарт PCI DSS. В то же время компании зачастую хотят решать задачи, связанные не с внешними нормативными документами, а с собственной внутренней политикой ИБ. Они стремятся контролировать использование



запрещенного ПО (Tor Browser, Skype, торренты), выявлять случаи применения съемных носителей в серверном сегменте или использования служебных учетных записей. Эти задачи достаточно типичны, но все-таки требуют наличия специализированного программного обеспечения. JSOC со своей стороны может служить системой выявления таких инцидентов на основании базовой информации от инфраструктуры. Тем самым компания будет получать оперативную информацию о соблюдении как внешних, так и внутренних политик информационной безопасности.

2 Обеспечение безопасности инфраструктуры

Достаточно большое количество событий, аномалий и инцидентов, происходящих на уровне инфраструктуры, зачастую остается незамеченным. Мы говорим об использовании базовых сервисов — создании временных учетных записей для проведения злонамеренных действий администраторами, несанкционированном использовании удаленного доступа сотрудниками и внешними контрагентами, взаимодействии внутренних систем с подозрительными и вредоносными хостами сети Интернет (как правило, это свидетельствует о скрытых вирусных заражениях). Наш опыт позволил нам сформировать набор сценариев (около 50 различных типов инцидентов), которые позволяют службе ИБ видеть, выявлять и оперативно расследовать инциденты. Дополнительными задачами здесь являются мониторинг и защита внешних веб-сервисов компании от злонамеренных атак или попыток внешнего проникновения.

3 Контроль инцидентов, связанных с нарушением бизнес-процессов и внутренним мошенничеством

Наиболее глубоким уровнем погружения для JSOC является контроль ключевых бизнес-процессов компании. Богатый опыт интеграции JSOC с бизнес-системами, построения аналитики по поиску ключевых и уязвимых точек бизнес-процессов, а также определения потенциальных схем внутреннего мошенничества позволяет нам говорить о задачах обеспечения безопасности не только инфраструктуры, но и бизнеса. Один из наиболее часто встречающихся кейсов последнего времени — это обеспечение безопасности кредитного конвейера и выдачи кредитов, здесь мы за последний год накопили особенно высокий уровень экспертизы.

***

JSOC, входящий в комплекс услуг, предоставляемых на платформе нашего ВЦОД, дает возможность компаниям сосредоточиться на своей профильной деятельности, не привлекая дополнительные материальные и человеческие ресурсы для задач обеспечения ИБ. Наша практика показывает, что этот сервис наиболее интересен банкам, ритейлерам и другим компаниям, для которых одной из ключевых задач является гарантирование высокого уровня защищенности онлайн-сервисов. JSOC позволяет оперативно выявлять, анализировать и расследовать инциденты, обеспечивая круглосуточный контроль состояния безопасности компании. JI

Аутсорсинг ИБ в банковском секторе: потребности и решаемые задачи

АВТОР: ВЛАДИМИР ДРЮКОВ

О том, какова роль ИБ-аутсорсинга в новой реальности (когда атаки злоумышленников на ИС банков становятся все изощреннее) и о результатах подключения банков к сервису JSOC (Jet Security Center, коммерческому центру мониторинга и реагирования на инциденты ИБ), созданному компанией «Инфосистемы Джет», в интервью NBJ рассказывает **руководитель направления аутсорсинга ИБ Центра информационной безопасности компании «Инфосистемы Джет» Владимир Дрюков.**

Источник: Национальный банковский журнал, № 6, июнь 2014 г.

Облачная безопасность, или SOC в аренду

АВТОР: ВЛАДИМИР ДРЮКОВ

В этом году компания «Инфосистемы Джет» запустила первый в России коммерческий центр мониторинга и реагирования на инциденты ИБ – облачный JSOC (Jet Security Operation Center). О том, что же получают компании, подключенные к нему, как изменилось их отношение к обеспечению ИБ и как устроен JSOC изнутри, пишет **Владимир Дрюков, руководитель направления аутсорсинга ИБ Центра информационной безопасности компании «Инфосистемы Джет».**

Источник: Information Security, № 6, декабрь 2013 г.

Jet Info
NEWS-BULLETIN

Главный редактор Дмитриев В. Ю.

Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01 факс (495) 411 76 02
e-mail: Jetinfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати **32555**