

PC WEEK RUSSIAN EDITION

18+

СК ПРЕСС

№ 16 (893) • 29 СЕНТЯБРЯ • 2015 • МОСКВА

<http://www.pcweek.ru>



**Бизнес-форум
1C:ERP
23 октября
Москва**

Регистрация:
www.1c.ru/bf

Inspur готова производить серверы в России

СЕРГЕЙ СВИНАРЕВ

На прошедшей в сентябре первой своей партнерской конференции в России китайская Inspur впервые представила планы работы на российском рынке. В нашей стране имя компании не очень известно, однако

БИЗНЕС в Китае она является крупнейшим производителем серверов с годовым оборотом 8,2 млрд. долл., опережая Dell, Lenovo, Huawei и Sugon. Да и на мировом рынке серверов Inspur занимает весьма почетное пятое место с долей 3,1% (в штучном исчислении). Компания выпускает также системы хранения, программное обеспечение (включая ОС и ERP-системы), а также суперкомпьютеры. Вице-президент по зарубежному маркетингу и продажам Inspur Дэвид Чэнь напомнил, что машина, занимающая сегодня первую строчку в мировом суперкомпьютерном рейтинге Top-500, построена Inspur совместно с национальным НРС-центром в Гуанчжоу.

В 2010 г. было принято решение развивать успех, достигнутый в Китае, и на международном рынке. В настоящее время у компании есть 8 тыс. парт-

неров в 85 странах, в 26 из них открыты ее представительства и в 10 — выставочные демоцентры. Первые контакты Inspur в нашей стране начались в 2011 г. и велись они с учреждениями Академии наук, занимающимися разработкой суперкомпьютеров, а в 2014-м было открыто полноценное представительство Inspur Russia. Как заявил Дэвид Чэнь, в рамках программы интернационализации компания рассматривает российский рынок в качестве ключевого. Об этом свидетельствуют и состоявшиеся в прошлом году контакты на достаточно высоком государственном уровне. “Российская Федерация заинтересована в более широком использовании китайских серверов, систем хранения и телекоммуникационного обо-



Дэвид Чэнь

рудования”, — заявил тогда в рамках рабочей встречи с министром промышленности и информатизации КНР Мяо Веем министр связи и массовых коммуникаций РФ Николай Никифоров.

Напомним, что Inspur наряду с линейкой серверов на платформе x86 (от 1 до 8 процессоров) выпускает 32-процессорный high-end Unix-сервер собствен-

ПРОДОЛЖЕНИЕ НА С. 2 ▶

Finnopolis 2015: на пути к дигитализации

СЕРГЕЙ КОСТЯКОВ

Всем известно, сколь важную роль технологии автоматизации играют в различных компаниях электронного бизнеса, существующего, как известно, в самых разнообразных формах. Современный банковский бизнес, или,

ФОРУМЫ если употреблять более общий термин, финансовый сектор, играет в деятельности индустрий e-бизнеса особую системообразующую роль. Большинство инноваций, связанных с ИКТ и направленных на совершенствование обслуживания конечных пользователей, становятся возможными, только если в разрабатываемые продукты можно встроить соответствующую уровню инновации банковскую услугу. Иными словами, отрасль оказания финансовых услуг по определению становится основным локомотивом (или в случае негативного сценария развития основным блокирующим фактором) на пути к созданию инновационных механизмов взаимодействия бизнеса со своими клиентами.

Первый Форум инновационных финансовых технологий Finnopolis 2015, состоявшийся в сентябре в Казани, под

разными ракурсами обсуждал именно эту группу вопросов.

Тон задавала первая панельная дискуссия под названием “Дигитализация финансовых рынков: взгляд в будущее”, в которой участвовали первые лица банковской отрасли со стороны государства и бизнеса, а также министр связи и массовых комму-

никаций РФ Николай Никифоров. По словам президента и председателя правления Сбербанка Германа Грефа, банковская индустрия сегодня входит в пятерку ведущих в отношении объемов венчурного финансирования, получаемого отраслевыми стартапами. Далее, по его мнению, очень существенной особенностью нынешнего состояния отрасли является приход на рынок оказания финансовых сервисов новых игроков из других

отраслей. В качестве примера он привел развитие двусторонних (peer-to-peer) договоров кредитования при посредничестве специализированных интернет-площадок, а также продажу финансовых услуг через классические интернет-магазины. Также в группу популярных небанковских финансовых сервисов на сегодня можно

ПРОДОЛЖЕНИЕ НА С. 14 ▶



Вань Бяо

В НОМЕРЕ:

- Инфраструктура цифрового бизнеса **6**
- ASUS ZenPad – новые планшеты премиального класса **6**
- Отечественный IT-рынок в исторической перспективе **8**
- Перспективы автоматизации банковского сектора **11**
- О внешних и внутренних ИБ-угрозах **12**



RECS'2015: куда двинется российский рынок ЕСМ

СЕРГЕЙ СВИНАРЕВ

Вряд ли следует удивляться, что в фокусе очередной, третьей конференции Russian Enterprise Content Summit'2015 (RECS), проведенной в середине сентября еженедельником PC Week/RE, оказались задачи в области

ЕСМ электронного документооборота (ЭДО) и управления контентом (ЕСМ), стоящие перед государственными организациями самого разного масштаба. Подобные задачи всегда имели высокий приоритет в корпоративном и государственном секторах, но сегодня, в условиях экономического кризиса и политического давления, они стали еще более актуальными. Следует учитывать и то, что российский рынок ЕСМ, столкнувшийся с урезанием ИТ-бюджетов в коммерческих компаниях, сохраняет неплохую динамику благодаря стабильности бюджетов в госсекторе. Ряд ведущих там проектов имеет самое непосредственное отношение к жизни граждан и потому оценивается специалистами не только по чисто технологическим параметрам, но и с позиций реальной пользы, удобства, целесообразности и т. д.



Рубен Энфиаджан

Особенно ярко это проявилось на панельной дискуссии “Электронное взаимодействие государства с организациями и гражданами: стратегия и практика”. Заведомо провокационный вопрос модератора дискуссии — нашего обозревателя Станислава Макарова: “Кто больше выиграет от реализации электронного взаимодействия, государство или граждане?” — заставил лишний раз вдуматься в смысл слов, которыми мы похода оперируем. Первым обратился на это внимание руководитель продаж IBM EE/A по направлению ЕСМ Алексей Гостев: “А почему, собственно, полезность системы для граждан и для государства мы рассматриваем в отрыве друг от друга? В электронном правительстве множество субъектов, и упрощение взаимодействия для каждого из них выгодно и важно”.

По мнению же начальника департамента управления инфраструктурой автоматизированной информационной системы Пенсионного фонда России Рубена Энфиаджана, свои выгоды получают и граждане, и государство: для первых это дополнительный комфорт, для вторых — механизмы контроля и обеспечения дисциплины. В силу этого оценивать выгоду в деньгах

не имеет смысла. Речь идет не о формальном возврате инвестиций, ведь электронный документооборот сегодня — насущная необходимость. Региональный директор Forrester Research в России Максим Тамбиев предложил оценивать экономический эффект в терминах времени, а не денег: “Например, в электронном правительстве Эстонии на регистрацию нового бизнеса уходит два часа. В освободившееся время можно сделать много чего полезного”.

А что же мешает переходить к электронному взаимодействию? Рубен Энфиаджан, ведомство которого (ПФР) имеет подразделения в 84 субъектах федерации, видит одну из причин в преодолении психологического барьера сотрудников, в связи с тем, что они привыкли работать с документами на бумажных носителях и им сложно перейти к использованию нового инструмента. Он отметил, что большую роль при внедрении электронного документооборота играет решение руководителя подразделения, например, о том, что с завтрашнего дня он не подпишет ни одного документа в бумажном варианте, а только в электронном виде. По мнению ведущего эксперта по управлению документацией компании ЭОС Наталья Храмовской, в условиях нынешней “многоукладности” (сочетания бумажного и электронного документооборота) существующая нормативная

ПРОДОЛЖЕНИЕ НА С. 2 ▶

SAP продвигает свои облачные решения в России

АНДРЕЙ КОЛЕСОВ

SAP объявила о развертывании двух своих флагманских облачных решений Arriba (управление закупками) и SuccessFactors (управление персоналом) на мощностях собственного московского ЦОДа, запущенного в конце прошлого года в кооперации с «Ростелекомом», и об их доступности для российских заказчиков. Генеральный директор «SAP СНГ» Вячеслав Орехов подчеркнул, что данный проект еще раз демонстрирует намерения компании продолжать развивать свой бизнес в России, продвигая здесь свои новейшие продукты и сервисы, которые реально могут помочь предприятиям и организациям страны повышать эффективность своей работы даже в условиях непростой экономической ситуации. Он отметил также, что облачные модели использования ИТ, как это обычно бывает с любыми инновациями, наряду с важными технологическими преимуществами создают и определенные новые проблемы и вызовы, на которые рынок должен находить оптимальные ответы совместными усилиями поставщиков, заказчиков и регулятора.

ОБЛАКА



Вячеслав Орехов

Одной из таких проблем, о которой на первой фазе продвижения облаков (изучение возможностей и опробование) фактически не упоминалось, но которая за последние пару лет стала выходить на первый план, являются вопросы трансграничности. Здесь возникает целый ряд вопросов, связанных с различной юрисдикцией поставщика и потребителя, необходимостью соответствия меняющимся нормативно-законодательным требованиям, обеспечением безопасности ИТ-систем и данных, а также с чисто техническими аспектами, такими как пропускная способность каналов связи, время задержки при обработке запросов и пр. Принципиальным решением этих вопросов является создание глобальными поставщиками собственных локальных дата-центров с размещаемыми в них прикладными решениями, что позволяет в полной мере учесть положения национального законодательства и специфику требований местных заказчиков, а кроме того, оптимизировать затраты самого провайдера на поддержку своей глобальной инфраструктуры вычислительных мощностей.

Именно такой стратегии придерживается SAP при работе на российском рынке. «Мы готовы поддержать всех наших российских заказчиков в плане соответствия новым законодательным требованиям и возможности максимально эффективно использовать преимущества современных облачных решений», — заявил Вячеслав Орехов. Он пояснил, что развернутые компанией в России решения полностью соответствуют введенным в действие с 1 сентября положениям закона 242-ФЗ о необходимости хранения персональных данных граждан России на территории страны. Более того,

возникает целый ряд вопросов, связанных с различной юрисдикцией поставщика и потребителя, необходимостью соответствия меняющимся нормативно-законодательным требованиям, обеспечением безопасности ИТ-систем и данных, а также с чисто техническими аспектами, такими как пропускная способность каналов связи, время задержки при обработке запросов и пр. Принципиальным решением этих вопросов является создание глобальными поставщиками собственных локальных дата-центров с размещаемыми в них прикладными решениями, что позволяет в полной мере учесть положения национального законодательства и специфику требований местных заказчиков, а кроме того, оптимизировать затраты самого провайдера на поддержку своей глобальной инфраструктуры вычислительных мощностей.

в российском ЦОДе развернуты все необходимые программно-аппаратные средства, которые работают полностью автономно и не зависят от каких-то зарубежных ресурсов. Оператором сервисов является российская дочерняя структура SAP — ООО «САП СНГ», которая находится полностью в местной юрисдикции и уже зарегистрирована Роскомнадзором в качестве оператора персональных данных. Для всех информационных систем, функционирующих в московском ЦОДе, уже получены аттестаты соответствия 2-му уровню защищенности персональных данных в системе сертификации ФСТЭК России.

Локализация облачных сервисов, уверены в SAP, сделает их более доступными для российских заказчиков, это, свою очередь, позволит предприятиям более решительно продвигаться в сторону использования эффективных облачных ИТ-моделей в целом. Хотя, конечно, понятно, процесс этот будет эволюционным, поэтапным, именно поэтому сейчас в России развернуты именно те средства, которые, по мнению SAP, могут быть наиболее востребованы в нашей стране.

Руководитель отдела по оказанию консультационных услуг по управлению персоналом компании PwC Карина Худенко отметила, что облачные сервисы позволяют не только получить сугубо ИТ-эффект (затраты, масштабируемость, надежность и пр.), но и, что, с точки зрения заказчика, может быть намного важнее, — повысить эффективность самого бизнеса за счет ис-

пользования новых возможностей, реализация которых в онпремис-решениях является сложной или почти невозможной. Например, речь может идти о различных форматах удаленного взаимодействия менеджеров по персоналу с сотрудниками и кандидатами на работу, о проведении онлайн-обучения и пр.

Именно необходимость решения задач обучения и переподготовки персонала подвигла сотового оператора МТС взять на вооружение облачное решение SuccessFactors Employee Central. Представитель оператора Юлия Цапкова сообщила, что уже первый опыт освоения сервиса показал, что он достаточно просто интегрируется с используемыми в компании системами обучения, до конца года к новому сервису будет подключен ряд подразделений МТС и начнется его промышленная эксплуатация. Но все же в полной мере оценить эффективность использования облачного решения SAP можно будет только спустя два-три года, считает она.

Другой пример использования облачного сервиса SuccessFactors привел член правления ГК АКИГ Алексей Шипов — в его организации он используется для проведения в масштабах всей страны разного рода молодежных олимпиад и конкурсов. В группе компаний пилотное развертывание системы на основе этого решения была проведена еще в начале текущего года за три месяца. Помимо экономии средств собственно на ИТ-проект подобного масштаба (от Калининграда до Владивостока) это позволило выйти на возможность реализации новых задач без увеличения штата сотрудников, отметил он.

RECS'2015...

◀ ПРОДОЛЖЕНИЕ СО С. 1

база иногда не помогает, а мешает его реализации.

В ряде выступлений из зала участники конференции отмечали существенные недостатки действующих электронных госуслуг, а иногда указывали даже на то, что услуги, вполне сносно функционировавшие прежде, сегодня не выдерживают никакой критики. В качестве одной из возможных причин этого руководитель практики Alfresco компании «Логика бизнеса» Олег Бейлезон назвал регулярные изменения в нормативной базе, которые налагаются на успешно реализованные ранее функции обработки документов и создают в них проблемы. Кроме того, он обратил внимание на то, что пропагандируемый сегодня безусловный приоритет электронной записи таит в себе большие опасности. Если такие записи обновляются медленно, то вполне добропорядочный гражданин может неожиданно для себя стать невыездыным, узнав об этом уже на паспортном контроле. Наталья Храмцовская подчеркнула в этой связи также огромную опасность недостаточно выверенных, «грязных» данных. Подобные случаи уже неоднократно фиксировались, и, как убежден Олег Бейлезон, переход на электронный документооборот должен сопровождаться какими-то реальными гарантиями со стороны государства.



Алексей Гостев

госучреждений. На предварительно отобранных платформах-кандидатах строятся прототипы искомого решения, которые затем тестируются на реальных данных и оцениваются экспертами по тем или иным параметрам. В результате каждая платформа (оценивались четыре отечественные системы) получает некий сводный балл, руководствуясь которым вроде бы и следует делать окончательный выбор. Впрочем, Анатолий Карпенко отметил, что их методика выявляет не лучшую СЭД, а систему, лучше соответствующую решаемой задаче.

И действительно, в проекте по созданию системы электронного документооборота для Пенсионного фонда РФ, о которой рассказал Рубен Энфиаджян, не использовалась ни одна из упомянутых четырех платформ: решение строится на заказной разработке, выполненной компанией R-Style на базе ряда Open Source-продуктов (PostgreSQL, Jboss, Apache Tomcat). В то же время она способна функционировать и на проприетарных платформах (Oracle DB, IBM DB2, WebSphere и WebLogic). Система должна охватить 2700 территориальных органов ПФР, в которых трудится более 100 тыс. человек, и призвана обеспечить юридически значимый документооборот широкого спектра типов документов (внутренняя корреспонденция, нормативно-правовые акты, протоколы, проекты конкурсной документации, обращения граждан, финансовый документооборот и т. д.) и интеграцию с системами межведомственного электронного документооборота.



Олег Бейлезон

Еще две темы постоянно затрагивались на конференции, и обе они особенно актуальны для госсектора. Это импортозамещение и применение свободного ПО. Так, заместитель начальника управления ИТ Аналитического центра при правительстве РФ Анатолий Карпенко описал предлагаемую методику выбора и внедрения корпоративной СЭД для

лированием бизнес-процессов на этапе постановки задачи. Это привело, в частности, к тому, что в ходе пилотного тестирования после изменения изначально спроектированной логики движения документов выявились «нестыковки» процессов их обработки и снизилась производительность базы данных.

Что касается применения СПО на российском рынке ЕСМ, то компания «Логика бизнеса», предлагающая своим заказчикам решения как на проприетарных (IBM FileNet и Notes/Domino), так и на опенсорсных (JBoss и Alfresco) платформах, провела специальное исследование, в ходе которого опрашивались представители организаций и компаний из разных сфер деятельности. Выяснилось, что



Максим Тамбиев

уже применяют указанные СПО-решения лишь 15% опрошенных. Остальные разделились на две одинаковые по размерам группы: одна планирует переход

на подобные решения, другая не имеет таких намерений. Причем в качестве главных причин своего выбора первые называют экономию средств и снижение политических рисков, а вторые — отсутствие готовых решений и сведений об успешных проектах. Представляя результаты исследования, Олег Бейлезон отметил, что ему известен ряд компаний, которые уже начали перенос своих ЕСМ-систем

с проприетарной платформы на опенсорсную. Впрочем, как признал докладчик, среди клиентов самой «Логика бизнеса» таковых пока нет.

Inspur...

◀ ПРОДОЛЖЕНИЕ СО С. 1

ной разработки Tianshuo K1 на платформе Itanium. На ее производственных мощностях выпускаются микросхемы, системные платы и корпуса.

Рассказывая о стратегии Inspur в нашей стране, президент Inspur Russia Чи Чунанью сообщил, что компания намерена не только продавать здесь решения, произведенные в Китае, но и создать совместное производство изделий под локальным брендом с не названной пока российской компанией. Кроме того, планируется организовать полную техподдержку и сервис, продолжить сотрудничество с российскими разработчиками суперкомпьютеров. В Россию будут также поставляться модульные и мобильные ЦОДы. Не исключено, что со временем будет принято решение о создании в России производственной площадки для выпуска ПК и ноутбуков. У компании уже есть опыт построения подобных производств в Венесуэле, Кении и на Кубе.

По словам генерального директора Inspur Russia Андрея Ковалева, сейчас российское представительство активно

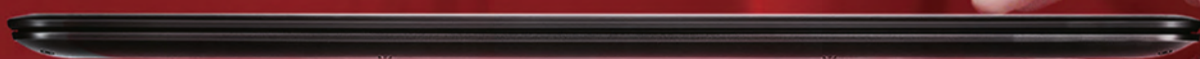
развивает партнерскую программу, в которой будут участвовать местные дистрибьюторы, системные интеграторы, сервис-провайдеры и научные учреждения. В России у компании уже есть 10 партнеров, из которых названы были только «Ай-Теко» и НИИ «Восход». Впрочем ранее в СМИ сообщалось о подписании партнерских соглашений еще и с компаниями СФЕРА, Merlion и MICS. Андрей Ковалев пообещал, что с учетом сложной экономической обстановкой в нашей стране Inspur готова предоставить отдельным заказчикам специальные финансовые программы, позволяющие получать отсрочку платежей за поставленные решения на 9—12 месяцев.

Среди первых проектов, выполненных в России, Андрей Ковалев упомянул тестирование банковских приложений «Диасофт» на серверах Inspur с целью проверки масштабируемости, производительности и отказоустойчивости, а также создание средств доверенной загрузки набора ОС, включая и специализированные системы российского производства. Последнее приобретает особую важность в свете известного курса российского правительства на импортозамещение.

ASUS[®]
В ПОИСКАХ НЕВЕРОЯТНОГО

ASUS рекомендует Windows.

от 46 990 руб



ASUS ZenBook™ UX305 Быстрый. Тонкий. Красивый.

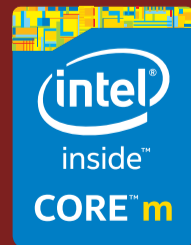
- Новейший процессор Intel® Core™ M 5Y10
- Операционная система Windows 8.1
- Ошелмляющий 13,3" IPS-дисплей с разрешением QHD+ (3200x1800)* или Full HD (1920x1080) и матовым покрытием
- Абсолютно бесшумный благодаря пассивной системе охлаждения

Ультрабуки серии Zenbook становятся еще компактнее благодаря революционным процессорам Intel® Core™ M, сочетающим высокую производительность и беспрецедентно низкое потребление энергии, что позволило сделать ультрабук совершенно бесшумным. Новый Zenbook в стильном корпусе из анодированного алюминия в черном или белом исполнении имеет толщину всего 12,3 мм, вес 1,2 кг и работает от батареи до 10 часов.

Intel Inside® , значит исключительная производительность.

* спецификации отличаются в зависимости от модели

Реклама. Intel, логотип Intel, Intel Inside, Intel Core и Core Inside являются товарными знаками корпорации Intel на территории США и других стран.



ПРИСОЕДИНЯЙТЕСЬ К НАМ В СОЦИАЛЬНЫХ СЕТЯХ:

B [VK.COM/ASUS](https://vk.com/asus)

f [FACEBOOK.COM/ASUS.RU](https://facebook.com/asus.ru)

T [TWITTER.COM/ASUS_RUSSIA](https://twitter.com/asus_russia)

I [INSTAGRAM.COM/ASUS_RUSSIA](https://instagram.com/asus_russia)

СОДЕРЖАНИЕ

№ 16 (893) • 29 СЕНТЯБРЯ, 2015 • Страница 4

НОВОСТИ

- 1 **На своей первой** партнерской конференции в России китайская Inspur впервые представила планы работы на российском рынке
- 1 **Finnopolis 2015: что** оказалось в центре

внимания первого Форума инновационных финансовых технологий **RECS'2015: стоящие** перед государственными организациями задачи в области ЭДО и управления контентом в условиях кризиса стали еще более актуальными

УПОМИНАНИЕ ФИРМ В НОМЕРЕ

ВымпелКом. 6	Касперского . . . 12	Технопром. 6	Huawei. 1	R-Style. 1,8,12
Инфосистемы Джет12	Логика бизнеса. . . 1	T-Платформы. . . . 6	IBM 1,6,8	SAP 2
Код Безопасности12	ННК 6	ЭОС 1	Inspur. 1,6	Tripp Lite 10
Компьюлинк. 12	Рикор 6	ASUS 6	Microsoft. 8,12	Yadro 6
Лаборатория	Смарт Лайн Инк . 12	HP 8	Oracle 8	ZTE 6

- 2 **SAP объявила** о развертывании двух своих флагманских облачных решений, Arriba и SuccessFactors, на мощностях собственного московского ЦОДа
- 6 **Об инфраструктуре** для цифрового бизнеса, импортозамещении и новых возможностях, предоставляемых консорциумом Open-POWER
- 6 **ASUS представила** в России серию новых планшетов премиального класса ZenPad

ЭКСПЕРТИЗА

- 8 **Григорий Сизоненко** об отечественном рынке информационных техноло-

гий в исторической перспективе и с точки зрения вызовов сегодняшнего дня

- 10 **Главные аргументы** в пользу моновендорного подхода при построении дата-центра

ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ

- 11 **Дмитрий Назипов:** “В современной парадигме банк фактически становится для клиентов внешним казначеем и провайдером многочисленных дополнительных сервисов”
- 12 **Внешние и внутренние** угрозы информационной безопасности — где сегодня проходит граница раздела и есть ли она

БЛОГОСФЕРА PCWEEK.RU

Некрообзор аналогов Google ChromeOS Сергей Бессонов, pcweek.ru/foss/blog

Определив тренд в мировой ИТ-индустрии на использование хромбуков, мы решили попробовать применить такие веб-ноутбуки и рабочие места на практике — в реальных компаниях. И уткнулись в неожиданную проблему.

Проблема эта заключается в том, что и ChromeOS, и даже ChromiumOS намертво привязаны к аккаунту Google. Желание Google зарабатывать на своей ОС понятно и логично, но иметь рабочие учётные записи пользователей где-то за океаном и вообще-то неправильно, а для государственных компаний с недавних пор просто недопустимо. Поэтому была предпринята попытка найти альтернативное решение.

Казалось бы, взять любой Linux и обрезать его до состояния ChromeOS — элементарная задача. Но реальность оказалась намного сложнее. В общем, нам не удалось найти современную ОС, созданную по принципу ChromeOS. Отсутствие необходимости администрирования клиентских устройств, простота освоения ОС, безопасность данных и прочие преимущества такого решения, по-видимому, никому не нужны.

Первой попыткой сделать альтернативу ChromeOS, по всей вероятности, стоит считать gOS, которая так и заявлялась: “An alternative OS with Google Apps and other Web 2.0 apps for the masses”. Существовала версия с использованием приложений MySpaces вместо Google. Кто помнит MySpaces? Вот. ОС перестала существовать в 2009-м.

Другая ОС, попавшая в обзор, — JoliOS, развиваемая в проекте JoliCloud. Основанная на кусках компонентов Ubuntu 10.04, эта ОС последний раз выходила в 2011 г. В наличии, естественно, браузер и часть программ, DE сформировано из настроенного Gnome 2. Самый красивый дистрибутив из обзора, исходный код лежит на Github, его хотя бы можно посмотреть и даже, может быть, использовать.

Ещё один дистрибутив — BrowserLinux. Последняя версия — 5.0.1, причём версия дистрибутива совпадает с версией Firefox, используемого как основа. Firefox завёрнут в DE на основе Openbox, что позволяет существенно сэкономить ресурсы и реализовать, наверное, самый нетребовательный дистрибутив из обзора. В качестве основы взят PuppyLinux. Последняя версия также от 2011 г.

И, наконец, самый эзотерический дистрибутив — Asgard. Несмотря на то что это современный дистрибутив, релиз которого состоялся буквально “на днях”, всего лишь год назад, использовать его в корпоративной среде мы тоже не можем, поскольку он построен не просто на базе Firefox, но на базе Vimperator.

И управление музыкой в стиле :playmedia и :stopmedia вряд ли придётся по вкусу скучающему офисному планктону.

Может быть, мы что-то пропустили. Но если нет, то получается, что несмотря на успех Google в корпоративном секторе и кажущуюся простоту создания веб-дистрибутива, последователей у Google не нашлось. А жаль...

Импортозамещение: о чём мы предпочитаем не говорить Сергей Голубев, pcweek.ru/foss/blog

Все разговоры об импортозамещении как-то крутятся вокруг одного и того же, что никогда не называется явно. Вот и в заметке “Бесплатный сыр в мышеловке, или Ещё раз про СПО” говорится о некоей препятствующей импортозамещению причине, которая в действительности вовсе и не причина, а только следствие.

“Народ, который не хочет кормить свою армию, будет кормить чужую” — эта фраза написана на первых страницах любого дембельского альбома. Разумеется, вместо армии можно подставить что угодно — машиностроение, авиацию, фундаментальную науку... В том числе и ИТ-отрасль. В этом, собственно, и заключается главный смысл импортозамещения — “кормить своих”. Всё остальное — второстепенные детали.

Понимание этого автоматически расставляет все точки над “i”. Почему мы кормим чужую ИТ-отрасль? Потому что в течение 25 лет (а может, и дольше) не хотели кормить свою.

А если кормить свою, то никакого выбора между свободным и проприетарным попросту нет. Есть выбор между свободным отечественным (даже если это очень и очень условно отечественное) и проприетарным отечественным. Иными словами, при внятном курсе на импортозамещение у пользователя десктопа есть выбор между “Альт Линукс”, РОСА, Calculate и... И получается, что всё.

На практике это означает, что бизнесу следует либо использовать СПО и “платить (как минимум за развёртывание, доработку и поддержку) специализирующимся на этом направлении сторонним компаниям”, либо использовать ППО и платить за его создание с нуля. Либо отказать от импортозамещения, но о последствиях данного шага уже написано в дембельских альбомах.

При этом важно понимать, что никаких дополнительных расходов на отечественное ПО нет. Чудес не бывает, и то, что было сэкономлено вчера, придётся заплатить завтра.

Разумеется, ИТ — никакое не исключение. Если город экономил на ремонте дорог десять лет, то на одиннадцатый ему придётся выложить сумму не меньше той, что была сэкономлена. А наверняка даже и больше.

Но уместно ли в данном случае говорить о каких-то дополнительных расходах? Разумеется, нет — речь может идти скорее о возврате долгов.

А долгов, увы, накопилось много. Не только перед ИТ. И отдавать их всё равно придётся — не так, так эдак...

Деревянное российское делопроизводство. Что нам нужно от государства?

Вадим Малых,
pcweek.ru/ecm/blog

Действительно — что на самом деле нам нужно от государства? Что мы не можем сделать сами и чем оно нам так мешает?

Тут, на мой взгляд, три основных аспекта. Первый и главный — конечно же электронные архивы. Об этом уже и, правда, смешно говорить, но проблема до сих пор остается основной, как три, и пять, и более лет назад. Итак, государство просто обязано принять волевое решение по поводу электронных архивов. А именно — адаптировать американский стандарт OAIS (признанный во всем мире) и дать разработчикам возможность начать реализовывать конкретные решения на его основе. За то время, что мы топчемся вокруг да около, это можно было бы сделать уже несколько десятков раз! Вместо того чтобы тратить деньги на какие-то непонятные национальные СЭД-платформы (где она, кстати?), мы могли бы вложить их в перевод и адаптацию стандарта. Это было бы реальное и всем нужное дело!

Зарубежные коллеги активно исследуют вопросы, связанные с сохранностью, юридической значимостью и другими аспектами электронных документов. В Интернете тонны информации, существуют целые проекты, финансируемые различными госструктурами. Мы же пока ограничиваемся охами и вздохами на тему “да, проблема сложная и требует решения”. Что это? Официальная позиция государства! Итак, второе, что государство просто обязано сделать, — изменить эту позицию.

Третий аспект очень четко сформулировал Владимир Баласанян: “В середине 1990-х была изобретена метафора СЭД как некоего клона ЕСМ-системы, адаптированного под реалии советского/российского бумажного делопроизводства, сложившегося окончательно во второй половине прошлого века. Похоже, сегодня эта метафора себя исчерпала. Ведущие разработчики, по сути, уже давно реализовали сформулированный в прошлом веке функционал и сейчас преимущественно заняты технической модернизацией своих систем с учетом современных ИТ. А вот сам предмет автоматизации никакой модернизации не претерпел. Речь идет даже не о возможности совершенствования традиционных принципов делопроизводства, а о хотя бы пересмотре технологических стереотипов работы

в условиях использования электронных документов и сетевых технологий коллективной работы”...

Как Microsoft будет монетизировать Windows 10?

Андрей Колесов,
pcweek.ru/pc/blog

Этот вопрос обсуждается на ИТ-рынке уже почти год — с тех пор, как стало известно о масштабном бесплатном распространении новой ОС для текущих пользователей Windows.

Эксперты сходятся во мнении, что основная часть денег от настольной Windows 10 по-прежнему будет поступать в виде лицензионных отчислений за продажу продукта, но доля продажи “коробок” будет сокращаться до нуля: останутся только OEM-продажи и корпоративные подписки. А доход от этих продаж в абсолютном выражении будет сокращаться.

Зато будут увеличиваться объемы поступлений от рекламы, которая предлагается пользователям через Windows. И еще Microsoft будет пытаться разными способами монетизировать большие данные о сотнях миллионов своих пользователей, причем здесь имеются в виду не просто регистрационные данные, а огромные потоки информации об их повседневной жизни. Как все это будет происходить в реальности, сказать пока сложно, многое тут представляется чуть ли не научной фантастикой, но мы видим, как на наших глазах многие фантазии о далеком будущем становятся явью.

И третье важное направление — это Магазин приложений, распространение через этот канал продуктов независимых разработчиков. Идея эта, конечно, не нова, тут компания идет следом за Apple и Google. Но если эти две компании никогда особенно не работали через партнерскую сеть (модель их бизнеса изначально была ориентирована на прямые продажи пользователям), то для Microsoft это как раз серьезная корректировка ее партнерской экосистемы, каналов продаж. И дело тут даже не в том, что компания будет напрямую продавать своих продукты, — она становится каналом продаж (глобальным дилером) продуктов независимых поставщиков, т. е. будет получать долю прибыли, которая раньше доставалась дистрибуторам-дилерам.

По этому поводу надо сказать, что совсем недавно на корпоративном блоге Microsoft появилась информация о том, что “средний” пользователь Windows 10 загружает из Windows Store в шесть раз больше приложений, чем это делал “средний” пользователь Windows 8.

Наверное, главная фишка Windows 10 в этом и заключается: чтобы пользователь чаще ходил в магазин. Чем чаще ходит, тем больше покупает...

FROM AGILITY
TO IMAGINATION



HUAWEI NETWORK CONFERENCE 2015

13 октября 2015 года | Лотте отель, Москва



Зарегистрируйтесь сегодня
hnc.huawei.com/ru/





Учредитель и издатель
ЗАО «СК ПРЕСС»

Издательский директор

Е. АДЛЕРОВ

Издатель группы ИТ

Н. ФЕДУЛОВ

Издатель

С. ДОЛЬНИКОВ

Директор по продажам

М. СИНИЛЬЩИКОВА

Генеральный директор

Л. ТЕПЛИЦКИЙ

Шеф-редактор группы ИТ

Р. ГЕРР

Ведущий эксперт группы ИТ

С. КОСТЯКОВ

Редакция

Главный редактор

А. МАКСИМОВ

1-й заместитель главного редактора

И. ЛАПИНСКИЙ

Научные редакторы

В. ВАСИЛЬЕВ,

Е. ГОРЕТКИНА,

О. ПАВЛОВА, С. СВИНАРЕВ,

П. ЧАЧИН

Обозреватели

С. ГОЛУБЕВ, С. БОБРОВСКИЙ,

А. КОЛЕСОВ

Специальный корреспондент

В. МИТИН

Корреспонденты

О. ЗВОНАРЕВА,

М. РАЗУМОВА, М. ФАТЕЕВА

Тестовая лаборатория

А. БАТЫРЬ

Ответственный секретарь

Е. КАЧАЛОВА

Литературные редакторы

Н. БОГОЯВЛЕНСКАЯ,

Т. НИКИТИНА, Т. ТОДЕР

Фотограф

О. ЛЫСЕНКО

Художественный редактор

Л. НИКОЛАЕВА

Группа компьютерной верстки

С. АМОСОВ, А. МАНУЙЛОВ

Техническая поддержка

К. ГУЩИН, С. РОГОНОВ

Корректор

И. МОРГУНОВСКАЯ

Тел./факс: (495) 974-2260

E-mail: editorial@pcweek.ru

Отдел рекламы

Руководитель отдела рекламы

С. ВАЙСЕРМАН

Тел./факс:

(495) 974-2260, 974-2263

E-mail: adv@pcweek.ru

Распространение

ЗАО «СК Пресс»

Отдел распространения, подписка

Тел.: +7(495) 974-2260

Факс: +7(495) 974-2263

E-mail: distribution@skpress.ru

Адрес: 109147, Москва,

ул. Марксистская, д. 34, к. 10,

3-й этаж, оф. 328

© СК Пресс, 2015

109147, Россия, Москва,

ул. Марксистская, д. 34, корп. 10,

PC WEEK/Russian Edition.

Перепечатка материалов допускается

только с разрешения редакции.

За содержание рекламных объявлений

и материалов под грифом "PC Week

promotion", "Специальный проект"

и "По материалам компании" редакция

ответственности не несет.

Газета зарегистрирована Комитетом РФ

по печати 29 марта 1995 г.

Свидетельство о регистрации № 013458.

Отпечатано в ООО "Доминико",

тел.: (495) 380-3451.

Тираж 35 000.

Цена свободная.

Использованы гарнитуры шрифтов

"Темза", "Телиос" фирмы TypeMarket.

Инфраструктура для цифрового бизнеса и импортозамещения

СЕРГЕЙ СВИНАРЕВ

В фокусе внимания конференции IBM System Forum, прошедшей в Москве в середине сентября, была инфраструктура для цифрового бизнеса. Термин "цифровой бизнес" используется довольно широко, но поскольку каждый понимает его немножко по-своему, далеко не лишними оказались пояснения, данные разными экспертами. Так, генеральный директор IBM в России и СНГ Андрей Филатов привел в пример такие новые, принципиально изменившие привычные модели ведения бизнеса компании, как Uber, Alibaba и Airbnb, которые не обладают большими собственными производственными активами, но чрезвычайно эффективно и инновационно используют активы информационные. Несмотря на столь впечатляющие примеры, лишь 10% опрошенных IBM компаний считают, что они готовы к цифровому бизнесу.

По мнению ИТ-директора "Банк ХоумКредит" Алексея Евтушенко, банковский сектор понимает важность перехода к цифровому бизнесу, но испытывает сложности как в постановке задач, так и в их реализации, при этом что все технологии для этого практически готовы. А директор по развитию ИКТ-партнерства "ВымпелКома" Татьяна Фомина сообщила, что в оргструктуре ее компании даже появился блок Digital под руководством CDO (Chief Digital Officer), цель которого превратить телеком-

оператора из условно говоря "транспортной трубы" в поставщика сложных цифровых сервисов. Технический директор "Электронной Москвы" Дмитрий Чернов обратил внимание на то, что элементы цифрового

на этой платформе, не опасаясь потерять контроль над своими изделиями или подвергнуться тем или иным санкционным ограничениям. В России импортозамещение в ИТ-отрасли, как правило, связывают с разработкой ПО, и именно

на этом направлении сосредоточены усилия государственных органов, в частности Минкомсвязи.

Заместитель директора департамента инфраструктурных проектов этого министерства Варган Хачатуров начал свое выступление с заявления о том, что импортозамещение — это совсем не то, что понимают под ним журналисты. По его словам, последние трактуют его как запрет импорта западных технологий, а на самом деле импортозамещение призвано "развить отечественные компетенции в разных сферах ИТ". Как вскоре выяснилось, некоторые инициативы Минкомсвязи непонятны не только журналистам. В частности, Варган Хачатуров заявил, что финансовую поддержку со стороны государства получают не собственно опенсорсные компании, занимающиеся созданием приоритетных отечественных продуктов с открытым кодом (ОС, СУБД), а отдельные разработчики, участвующие в подобных проектах. Сразу же возник вопрос: как это сделать, если государство не имеет права оплачивать работу физических лиц? Докладчик разъяснил, что с этой целью

планируется создать некую некоммерческую организацию, которая и станет выплачивать деньги. Тут же кто-то вспомнил, что подобная некоммерческая организация (Национальная программная платформа, НПП) уже создавалась, и поинтересовался ее судьбой. Как оказалось, НПП по-прежнему существует, и при желании ее тоже можно подключить к этой деятельности. Были вопросы и относительно преференций, отдаваемых в госзакупках отечественным продуктам, попавшим в специальный реестр российского ПО. По словам Варгана Хачатурова, одним из важных критериев для включения продукта в реестр, если в нем наряду с отечественными используются и зарубежные технологии, будет содержащаяся в нем доля российской интеллектуальной собственности. В каких единицах собираются измерять интеллектуальную собственность, понять довольно трудно. Участники дискуссии выразили также опасение, что благодаря преференциям отечественные продукты подтянутся по цене к западным, что негативно скажется на ИТ-бюджетах заказчиков.

Говоря о возможностях, предоставляемых консорциумом OpenPOWER, генеральный директор компании "Т-Платформы" Всеволод Опанасенко отметил, что раньше существовали три модели взаимодействия производителя чипов с разработчиками: традиционная для IBM (и процессоры, и системы имели

ПРОДОЛЖЕНИЕ НА С. 10 ▶



Андрей Филатов

Новые планшеты ASUS ZenPad премиального класса

ВЛАДИМИР РОМАНЧЕНКО

А ASUS официально представила в России серию новых планшетов премиального класса ZenPad под управлением Android 5.0 Lollipop. Впервые планшеты ASUS

обзавелись поддержкой сменных панелей корпусов различных расцветок и с дополнительной функциональностью. Кроме того, они первыми в мире получили поддержку технологии DTS-HD Premium Sound, преобразующей стереосигнал в многоканальный виртуальный звук. Ряд новых моделей также получил поддержку стилуса. Некоторые новинки получили универсальный разъем нового поколения USB 3.0 Type C.

Планшеты ZenPad представлены моделями с экранами трех размеров, каждый из которых выполнен по IPS-технологии и поддерживает набор функций для повышения качества изображения при работе с мультимедийными приложениями ASUS VisualMaster, включая ASUS Tru2Life и ASUS TruVivid. Аппараты доступны в версиях как с поддержкой только Wi-Fi, так и в вариантах с LTE/3G с поддержкой мобильной телефонии.

7-дюймовые ZenPad C 7.0 (Z170C/CG/MG) имеют ориги-

нальную отделку задней панели под тисненую кожу. Планшеты доступны в черном, белом, красном и серебристом корпусах, в варианте с поддержкой



8-дюймовый планшет ASUS ZenPad 8.0 на процессоре Intel Atom x3

Wi-Fi (Z170C) или 3G и функций мобильной телефонии (Z170CG, Z170MG). Модели Z170C и Z170CG оснащаются процессором Intel Atom x3, модель Z170MG выполнена на 64-разрядном 4-ядерном процессоре MTK. Планшеты оснащены 2-Мп основной и 0,3-Мп фронтальной камерами с технологией ASUS PixelMaster для съемки фото и видео даже в условиях низкой освещенности.

8-дюймовые ZenPad 8.0 будут доступны в версии Z380C на процессоре Intel Atom x3 и Z380KL на базе чипа Qualcomm Snapdragon 410 MSM8916. Планшеты оснащены 5-Мп основной и 2-Мп фронтальной камерами

с технологией PixelMaster. Задняя панель планшетов имеет отделку под тисненую кожу, а корпус имеет скругленные углы металлической рамки корпуса для удобного захвата рукой. Модели ZenPad 8.0 предлагаются в модификациях с поддержкой Wi-Fi и 4G/LTE, в трёх вариантах цветового исполнения корпуса: черном, белом и серебристом.

Премиальная модель ZenPad S 8.0 (Z580CA) оснащена 8-дюймовым экраном с разрешением 1536×2048, рекордным в своем сегменте объемом системной памяти 4 Гб и производительным 2,3-ГГц 4-ядерным 64-разрядным процессором Atom Z3580. Планшет очень компактный, толщина корпуса всего 6,6 мм, масса 299 г. Модель оснащена 8-Мп основной и 2-Мп фронтальной камерами с технологией PixelMaster. Задняя панель планшета доступна в двух цветовых исполнениях, белом и черном, с отделкой под тисненую кожу. Для ZenPad S 8.0 опционально доступен стилус Z stylus с высокой чувствительностью, распознаванием до 1024 уровней нажатия и тонким, 1,2-мм, наконечником.

Старшая модель ZenPad 10 премиального класса с 10,1-дюймовым IPS-экраном (1280×800) представлена тремя версиями: с поддержкой LTE/Wi-Fi (Z300CL),

3G/Wi-Fi (Z300CG) и Wi-Fi (Z300C), в трёх цветовых вариантах оформления корпуса: черном, белом и серебристом, с отделкой задней панели под тисненую кожу. Модель выполнена на процессоре Intel Atom Z3560. На передней панели ZenPad 10 размещены стереодинамики, а дополнительная док-станция ASUS Audio Dock расширяет функциональность планшета клавиатурой и стереосистемой ASUS SonicMaster. Док-станция можно подключить к планшету на расстоянии до 10 м по Bluetooth. ZenPad 10 также можно использовать вместе с опциональным стилусом Z Stylus.

Для новых планшетов будет доступен широкий ассортимент дополнительных аксессуаров, таких как чехлы TriCover для защиты и использования в качестве подставки с тремя углами наклона, аккумулятор Power Case, заменяющий заднюю крышку планшетов Z380C/KL и увеличивающий время автономной работы до 14 часов, чехлы Audio Cover с шестью встроенными динамиками для воспроизведения звука в формате 5.1. Для моделей Z380C/KL, Z580CA и Z300C/CG/CL будут доступны фирменные чехлы Zen Clutch в виде модной сумки-клатча. □

ПРОВЕРЕННЫЕ ВРЕМЕНЕМ ИНФРАСТРУКТУРНЫЕ РЕШЕНИЯ LENOVO



БОЛЬШИЕ ДАННЫЕ
И АНАЛИТИКА



ВИРТУАЛИЗАЦИЯ



ОБЛАЧНЫЕ
ВЫЧИСЛЕНИЯ



ВЫСОКОПРОИЗВОДИТЕЛЬНЫЕ
ВЫЧИСЛЕНИЯ



БИЗНЕС
ПРИЛОЖЕНИЯ



БАЗЫ
ДАННЫХ



КОНВЕРГЕНТНЫЕ
СИСТЕМЫ

**ЭТАЛОННЫЕ АРХИТЕКТУРЫ
ДЛЯ ДОСТИЖЕНИЯ БИЗНЕС-ЦЕЛЕЙ
ПРИ РАЗУМНЫХ ЗАТРАТАХ НА ИТ – ДАЖЕ С УЧЕТОМ
МЕНЯЮЩЕЙСЯ РЫНОЧНОЙ СИТУАЦИИ**

www.lenovo.com

Григорий Сизоненко: “Мы раньше IBM сообразили, что делать бизнес на ПК малоцелесообразно”

СТАНИСЛАВ МАКАРОВ

Говоря о становлении в России индустрии информационных технологий, мы неизбежно возвращаемся к тому уникальному периоду, продолжавшемуся около десяти лет, когда перестройка в 1985 г. чуть приоткрыла железный занавес и в страну стали попадать первые персональные компьютеры. Сначала небольшим ручейком по линии Академии наук, а чуть позже — мощным потоком через разные СП и коммерческие фирмы. То была “эпоха первоначального накопления капитала” — почти все наши известные ИТ-компании выросли на торговле ПК, что в некотором роде даже странно, потому что эта модель бизнеса не предполагала какой-то заметной интеллектуальной составляющей. Вы же не видели, чтобы успешный торговец зерном вдруг стал фермером! Наверное, сама природа этого “умного товара” сподвигла продавцов компьютеров остаться в технологическом бизнесе — стать системными интеграторами и разработчиками.

ИВК — “Информационная Внедренческая Компания” — была организована выпускниками МВТУ имени Баумана в 1988 г. Григорий Сизоненко пришел в ИВК годом позже с должности заместителя секретаря парткома МВТУ. “Ушел в коммерцию”, — как говорили тогда. С 1996-го он возглавляет ИВК в должности генерального директора.

Мы встретились, чтобы поговорить об отечественном рынке информационных технологий — в исторической перспективе и с точки зрения вызовов сегодняшнего дня.

Бизнес на ПК — как это делалось в России

Из-за того, что в СССР компьютеров делали мало и еще меньше закупали, а технический прогресс все-таки шел своим чередом, возник огромный отложенный спрос, который блокировался искусственным ограничением импорта. Валюта в СССР была уникальным ресурсом, доступным далеко не каждому, и поэтому вполне логично, что импортеры — кому было разрешено таковыми быть, старались извлечь максимальную для себя выгоду, а на “персоналках” это получалось лучше всего. Официально в 1989 г. доллар стоил 63 копейки, но цена персонального компьютера для отечественного заказчика могла доходить и до 20 тыс. долл. Бизнес был очень высокомаржинальный, однако это быстро закончилось...

Если посмотреть на нынешних олигархов, то многие “поднялись” именно на продаже компьютеров. Какова точно была прибыльность в процентах, сейчас не скажу, знаю только, что с продажи одного компьютера я купил автомобиль. А со ста можно было купить целый автопарк! Но вскоре сам рынок убил маржу, потому что появилось очень много поставщиков, которые начали сбивать цену. Одно дело, когда у тебя рентабельность тысяча процентов, а потом раз — и пятьсот, потом триста, сто, пятьдесят, двадцать... десять... Сейчас у дистрибьютора маржа в районе 5%, да еще побегать нужно, чтобы продать. Прошло три-четыре года, и стало грустно. Длинный бизнес на таком рынке не построишь, и тогда мы решили заняться сборкой компьютеров.

Помните, у нас в МВТУ был ректор Алексей Елисеев? Космонавт, дважды Герой Советского Союза. В 1991 г. он перешел на работу в ИВК, и как человек государственный, он продвигал идею, что надо организовывать производство компьютеров в России. А в ИВК ему говорили: “Мы готовы, но только в партнер-



Григорий Сизоненко

стве с какой-то российской компанией”. Елисеев сделал нам предложение — сказал, ребята, посмотрите завод в Зеленограде, может быть, удастся совместно с IBM организовать производство. Мы поехали в Зеленоград, увидели “Квант” — ничего себе! Совсем новый завод, только построили! Стоят японские линии, с них даже пленку еще не сняли, роботы-тележки, автоматические склады! Завод — сказка! (В период с 1987 по 1992 гг. завод прошёл техническое перевооружение стоимостью около 100 млн. долл., установлена сборочная линия японской компании Daifuki. — [Википедия](#).)

В Советском Союзе собирались построить три таких завода. Один из них, “Квант”, оснащён был полностью, в Воронеже построили здание и завезли оборудование, но не смонтировали, а в Кичинево вообще только стены возвели. Эти три завода и должны были обеспечить Советский Союз персональными компьютерами. Каждый из них имел проектную мощность в миллион компьютеров в год.

Мы увидели: есть заказчик — IBM, который готов собирать свои компьютеры и мониторы. Есть завод — исключительный! И приняли решение участвовать в приватизации “Кванта”. Схемы там были не простые, это да... Однако нам удалось получить контрольный пакет акций этого завода. На переговорах с IBM я лично принимал участие в согласовании вопроса, что мы будем выпускать свои компьютеры под маркой ИВК и оказывать услуги по производству техники IBM. И мы на самом деле, как собственники этого завода, собирали мониторы и компьютеры для IBM. Выделили для них, куда они завезли свое оборудование для сборки и тестирования мониторов. В цеху, оснащённом роботами-тележками, развернули сборку компьютеров IBM. А в большом цехе, оснащённом конвейерными линиями, организовали собственное производство.

В то время администрацией Ельцина руководил Сергей Филатов, а при нем была комиссия по информатизации. И ваш почтенный слуга на этой комиссии выступал с большим докладом о развитии компьютерного производства в Российской Федерации. Были приняты решения, что государственные структуры должны закупать российскую технику... (Всё удивительным образом повторяется... — С. М.)

Тогда многие поняли, что нужно начинать свою сборку. Причем не все компании собирали компьютеры в России: кто-то собирал их на Тайване и потом импортировал. Но вскоре изменилась таможенная политика и стало выгоднее завозить комплектующие и здесь соби-

рать. В отличие от других сборщиков у нас были просто огромные производственные мощности. Сейчас уже не секрет, мы собирали компьютеры не только для IBM, но и для “Виста”, R&K и еще для ряда небольших компаний, которые нам приносили заказы.

Где-то до 1996—1997 гг. мы занимались производством офисной вычислительной техники. В целом мы пытались строить свой бизнес, оглядываясь на IBM, — у нас была своя программа, маркетинг, техническая политика... Как раз в 1996-м открыли большой офис, создали дилерскую сеть по всей стране, заключили договор с Intel и OEM-договор с Microsoft. В какой-то момент это были реально большие объемы, огромный поток денег — такое счастливое состояние, когда всё получается! Но мы же бауманцы, нас учили мыслить системно — хоть экономике и финансам нас и не учили, но организацию, подготовку и планирование производства — это мы проходили. Я решил сесть и посчитать деньги: сервис, скидки, ремонт, гарантии, зарплата, аренда и т. д. И вдруг оказалось, что денег в обороте много, а прибыли нет!

Мы раньше IBM сообразили, что делать бизнес на персональных компьютерах в какой-то момент становится экономически малоцелесообразно. Это же очевидно — при массовом производстве возросла конкуренция, и компьютеры фактически стали обычной техникой для дома. Когда у тебя на глазах прибыль с тысячи процентов падает до тридцати (тогда, в 1997 г., так и было), ты понимаешь, что здесь только вопрос времени, что она упадет до критической величины и ты не сможешь развиваться. И мы решили перестроить и диверсифицировать бизнес.

Во-первых, мы закрыли всю дилерскую сеть. Это было мое личное решение. Зафиксировали убытки и закрыли проект. Перешли на прямые продажи. Объемы продаж сильно упали. Но я до сих пор считаю, что это был абсолютно правильный для компании ход, несмотря на то, что на этом фоне набрали силу наши конкуренты — R&K, “Вист” и другие. Но где они все сегодня? Они остались там, в прошлом. Низкомаржинальный бизнес с неизбежностью приводит к таким результатам. А вот R-Style тогда тоже ушел в высокомаржинальный бизнес, они молодцы.

К слову сказать, европейские и американские компании также не выдержали конкуренции с “желтой сборкой” — где сейчас Olivetti, Bull, Siemens, Gateway и другие ПК так называемой “белой сборки”? Их тоже нет. У нас же большинство “красных сборщиков” окончательно смёл кризис 1998 г. — на этом фоне решение ИВК выглядит особенно пророческим.

Монетизировать инженерные знания

Когда бурят первые скважины на новом месторождении, сначала нефть бьет фонтаном, только подставляй трубу. Потом напор ослабевает, “черное золото” приходится выкачивать насосами, нагнетать воду в пласт и применять более сложные и дорогие технологии добычи. Не всякая добывающая компания способна быть рентабельной в таких условиях. Аналогичная картина сложилась и на рынке компьютеров: добывать маржу простыми средствами стало очень сложно, поэтому пришлось подумать о менее массовых, но более прибыльных сегментах рынка, где децезивизация товара не является конечным аргументом. Логичным путем развития событий выглядит разработка рыночных ниш, не затронутых повальной конъюнктурой.

Мы до сих пор делаем персональные компьютеры. Немного. Значительно

больше делаем “компьютеров со специальными свойствами”, устанавливаемых, например, на колесных или гусеничных машинах, которые проектируют выпускники факультета “К” нашего МВТУ. Они работают в жестких условиях, с вибрацией, с перепадами температур, что важно для военных, МЧС и других подобных заказчиков. Мы приняли решение уйти в этот намного более маржинальный рынок, где работа идет совсем по другим сценариям. Допустим, открываются ОКР на создание системы, которая решает какие-то задачи в интересах заказчика. И в рамках этих ОКР заказчику нужен “вычислитель” с определенными характеристиками. Он должен работать с такой-то производительностью, выдерживать высокие вибрационные нагрузки, иметь заданные габариты и т. д. Под эти требования проектируется реальный компьютер. Именно проектируется! Здесь традиционное “купил-продал” не работает.

Поскольку из комплектующих в России мало что есть, приходится смотреть весь мировой рынок. У немцев ты покупаешь одно, у американцев другое, у японцев третье, у китайцев четвертое, собираешь этот “вычислитель” и поставляешь заказчику. Заказчик проводит комплексные испытания и ставит систему на снабжение — и дальше ты находишься в системе со своими десятичными номерами. Можешь делать свои “вычислители” десятилетиями. И никаких тебе конкурсов каждый год! Только ждать этого счастливого мгновения можно долго, и хуже того — изделие вообще может не пойти в серию. Вот таким образом мы являемся поставщиками специальных вычислителей к широкому ряду различных изделий для различных структур, которые работают в интересах государства. Зачастую мы даже не знаем, чем занимаются те комплексы, куда мы поставляем нашу продукцию.

Другая ниша — это компьютеры, предназначенные для обработки конфиденциальной информации. Как только речь заходит об этом, а еще и о грифе как-нибудь, то тут без вариантов — надо делать только свое. Причем опять-таки не обязательно все делать из одних лишь своих комплектующих. Важнее разрабатывать собственные архитектурные решения, чем мы и занимаемся сейчас. Такую защищенную технику мы уже представили ряду заказчиков, которые работают с конфиденциальной информацией высокого уровня. Это реально другая техника, она отличается от обычных серийных компьютеров, которые всего лишь прошли спецпроверки и специсследования, то есть проверки на отсутствие недекларируемых возможностей (попросту говоря, закладок) и на уровень ПЭМИ (побочные электромагнитные излучения). Каждый инженер понимает, что если есть какое-то электромагнитное поле, то его можно преобразовать и таким образом считать информацию. Специальными средствами уровень излучения обычного компьютера можно снизить, но совсем незначительно. Чтобы компьютер совершенно не “светил”, применяются другие архитектурные и инженерные решения, другие материалы, кабели и пр.

Наши инженеры спроектировали компьютер, у которого практически нет побочного электромагнитного излучения, и мы начали их производство. Я полагаю, что через один-два года государство начнет массово закупать эту технику — у нас уже формируется на них очередь. Говорю об этой разработке впервые, специально для PC Week/RE.

Нельзя запрыгнуть на небоскреб

Есть сферы, где попытки “догнать и перегнать” будут бесполезны. К их числу отнести и потребительскую микроэлектронику, поскольку Россия здесь будет явно неконкурентоспособна. Нет смысла возрождать свое производство, потому что китайцы все равно сделают дешевле. ▶

► И никакие разговоры об импортозамещении не изменят этого факта. Но существует другой рынок, где без отечественных разработок просто не обойтись. И надо туда лезть, там осваиваться.

Мне как-то на глаза попала простая и очевидная фраза: нельзя запрыгнуть на небоскреб, на него можно только забраться. С падениями, страховкой, но всё равно нужно ползти вверх. Поднять микроэлектронику — это для нас небоскреб, мы это понимаем. Наши зарубежные партнеры очень грамотно завели нас в эту ситуацию и сказали: “У нас же мировое разделение труда, международное! У вас классная, ответственная задача — обеспечивать весь мир энергоресурсами. А за это берите спокойно чипы, процессоры — зачем вам самим их делать?”

Но когда ты этим не занимаешься, ты вообще теряешь связь с технологией. И наступит момент, когда ты даже не будешь понимать, как это работает, устроено и как такое вообще возможно. Поэтому нужно развивать собственное производство микроэлектроники хотя бы для того, чтобы поддерживать свой интеллектуальный уровень. Государство наконец начало это понимать. Пусть ему сейчас тяжело, пусть оно пожинает горькие плоды, так сказать, либеральной экономики, но это нужно делать.

От сборки компьютеров к разработке ПО

Очевидно, что строя бизнес на далекую перспективу, нужно заниматься проектами с большой добавленной стоимостью. В 1998 г. я собрал наш научно-технический совет и сказал: “Друзья, нужны идеи! Идеи, которые потрясут мир. Или по крайней мере Россию. Давайте фантазируйте! Нам нужно найти свою нишу, чем мы будем заниматься в ближайшие десять лет”.

Одна из идей, появившихся после этого мозгового штурма, относилась к интеграционным платформам. Дело в том, что у наших крупных заказчиков из Министерства обороны и МВД уже тогда были очень сложные и крупные автоматизированные системы. Я думаю, на гражданке до сих пор еще не вышли на тот уровень, который тогда был у силовиков. То были мощнейшие системы, функционировавшие в огромной гетерогенной среде! Однако в конце 1990-х настала пора менять все эти ЕС, “Наири”, “Электроник”, ДВК и другие устаревшие машины на что-то более современное. А представляете, сколько там прикладного софта?

Энтузиасты выбрали вроде бы очевидный путь решения, который заключался в том, чтобы написать свою операционную систему и под нее переписать все прикладное ПО. И частично это было реализовано — появилась ОС МСВС, и на ней стали разрабатывать прикладной софт.

Но были и другие заказчики, которые не могли позволить себе нарушить функционирование уже действующих систем. Они искали пути безболезненного перехода, чтобы можно было выбросить старые машины, но сохранить прикладные задачи. Нашлись умные люди, подсказавшие: посмотрите на идеологию IBM, на трехуровневую архитектуру, когда приложения как бы отрывают от операционки и размещают в некий промежуточный слой. Сейчас мы называем это middleware, а тогда и слова такого не было — говорили “мониторы транзакций”. И мы решили: вот этим и займемся.

В высоких кабинетах нас сначала не поняли. И не понимали много лет: “Какие технологии? Какая архитектура?” Пришлось открыть внутренние ОКР. Начали разрабатывать свой middleware — технологию интеграции разнородных ресурсов.

Разница состоит в том, что middleware — это не прикладной софт, а именно инфраструктурная технология, которая позволяет создавать и органично поддерживать развитие информационных систем с учетом практически любых революционных изменений в сфере информационных технологий.

Мы пришли в очень серьезное управление Министерства обороны. Там оказались грамотные товарищи, которые понимали, что им нужно быстро решить свои задачи, а не переписывать весь прикладной софт и что наша технология позволяет это сделать. Они сказали: “Мы готовы купить у вас это ПО, давайте”.

Через некоторое время заказчик пригласил меня на объект информатизации: “Пойдем, покажу, что вы натворили со своим софтом”. Представляете, огромный зал, вычислительный центр. И совершенно пустой! Посередине зала стоит стол, на нем — компактные серверы IBM, а внутри — наш софт и все унаследованное ПО заказчика. Именно тогда мы заработали первые деньги на собственном инфраструктурном софте!

Продавать технологию всегда сложнее, чем готовый прикладной продукт. Нам приходилось много доказывать, рассказывать, убеждать. Найти понимающего заказчика и заинтересовать его технологией — это тяжелый труд. Но такие заказчики были. Один из них — я снимаю перед ними шляпу — это НИИ “Восход”. В 2004 г. они выиграли конкурс на создание ГАС “Правосудие” — огромную систему, объединяющую 3,5 тыс. объектов на 100 тыс. пользователей. Когда они выбирали платформу для создания этой системы, была конкуренция между IBM и нашим “ИВК Юпитером”. Надо отдать должное IBM — это действительно хорошая платформа. Но оценив финансовые возможности, “Восход” решил строить ГАС “Правосудие” на российской технологии. Вот тогда мы впервые вошли в крупнейший государственный проект.

“Продвинутые” решения — только для грамотных заказчиков

Ситуация, с которой столкнулась ИВК, выводя на рынок новую технологию, прекрасно иллюстрирует общее положение дел в отрасли ИТ. Уровень системной сложности возрос настолько, что даже высококвалифицированные ИТ-специалисты не всегда до конца понимают, как работает та или иная технология. Заказчики, в силу объективных причин, разбираются в ИТ еще меньше. Тем не менее сторонам надо стремиться к взаимопониманию.

Это очень большая тема. Компетенция заказчиков вообще очень разная, но она сильно упала по сравнению с девяностыми годами. Если тогда к нам приходили специалисты и жестко формулировали свои требования, то сейчас не всегда найдешь заказчика, который может технически грамотно поставить задачу. Двадцать лет интеграции в мировое разделение труда сделали из нас потребителей среднего уровня, которые умеют написать в общем-то среднее техзадание под зарубежные технологии. Сейчас я выйду на рынок, крикну: “Смотрите, отечественная инфраструктурная технология!” Вышел, крикнул — дурак, да? А в ответ — тишина. Или ещё того хуже: “Какие еще отечественные ИТ? Такие технологии делают только на Западе, откуда они в России?! В нашей стране не умеют писать серьезный программный код!”

Вопрос задан очень точно: “А как продать технологию?” Когда ты говоришь о технологии, заказчики зачастую просто впадают в ступор. В особенности если говорить о том, что делаем мы, — об инфраструктуре, которую не пощупать и не увидеть на пользовательском уровне.

Низкий поклон нашему первому заказчику, который в 1999-м понял нашу технологию. Тогда мы поверили в собственные силы.

Документооборот на middleware

Мощь инфраструктурных технологий проявляется, в частности, в том, что с их помощью можно гораздо быстрее реализовывать прикладные задачи.

Расскажу об одном проекте. Просто технологию, как я говорил, продать очень сложно. Только очень вездливому, умному и не ангажированному заказчику можно убедить покупать отечественную технологию. Потому что все зашорены технологиями IBM, HP, Oracle, Microsoft... И когда приходит ИВК, российская компания, — какие технологии, о чем ты говоришь?! И мы, чтобы показать конкретное применение нашей технологии, сделали одну прикладную разработку — документооборот “ИВК-БюрократЪ”. У нас в стране существует много систем электронного документооборота, может быть, я заблуждаюсь относительно того, насколько передовой выглядит наша система, но, на мой взгляд, она имеет весомые преимущества.

Например, наша СЭД сегодня устойчиво работает на сотнях территориально-распределенных объектов от Камчатки до Калининграда, от Новосибирских островов до Казахстана.

По всей территории России, по народным каналам связи, и спутниковым, и наземным. На операционных системах Windows, MSVC, Linux. С электронной подписью, сквозным контролем исполнения поручений, с гарантированностью всех сервисов. В системе можно одновременно обрабатывать информацию с четырьмя грифами конфиденциальности. И это на 100% наша, российская разработка.

Мы выиграли открытый конкурс и сейчас являемся головными исполнителями по системе электронного документооборота Министерства обороны РФ. Разумеется, есть контроль исполнения, там целое контрольное управление. Входящий участок мы интегрировали со СМЭВ и МЭДО — это Правительство, Администрация Президента; без задержки идет поток документов, сразу преобразуется в нужные форматы, грифы расставляются, регистрация, номер, поручение — и полетел по стране, получи, исполнитель. А контролер видит конечного исполнителя хоть на Камчатке. Многие ругают Анатолия Сердюкова, но этот проект в Министерстве обороны инициировал именно он. Не захотел жить в девятнадцатом веке с посылными, с пачками бумаг. Вот и вынудил всех переходить на электронный документооборот. Такая вот история.

Мы решили эту задачу и показали действенность нашей технологической платформы, нашего middleware. Написали прикладной функционал, причем буквально за два-три месяца сделали весь этот документооборот. Поскольку системная часть была уже готова, писать пришлось только саму логику обработки документов. В этом очевидное преимущество платформы, когда ты можешь разработку вести не три года, а квартал, ну полгода и через полгода выдавать готовые системы.

Импортозамещение: не надо ждать десять лет

Минкомсвязи утвердило план импортозамещения программного обеспечения 1 апреля 2015 г. На момент разработки плана доля импортных клиентских и мобильных операционных систем на российском рынке составляла 95%. Но к 2020 г. министерство планировало понизить ее до 75%, а к 2025-му довести до 50%. Всего на развитие отечественного софта ведомство просит 18 млрд. руб. По словам представителя Минэкономразвития, финансироваться проекты будут через вновь созданную автономную некоммерческую организацию (АНО) коллективной разработки программного обеспечения.

Если министр Николай Никифоров внимательно прочтет мои предложения, которые я ему отправил, он увидит, что не нужно ждать десять лет, чтобы выйти на уровень импортозамещения в 50%. Надо создавать рынок потребления уже имеющихся в стране разработок. Именно в этом должна сейчас проявиться роль государства. Возьмите наши технологии, технологии наших российских партнеров, и уже завтра по некоторым направлениям мы закроем 90%.

Сейчас создаются структуры, которые занимаются импортозамещением, им выделяются деньги из бюджета — на создание чего-то! Нам, разработчикам, говорят: “Давайте, вы тоже объединитесь в некие консорциумы, и государство даст вам денег”. Но, как мне кажется, это свидетельствует о некоем непонимании принципов разработки софта. Как можно каким-то консорциумом за бюджетные деньги разрабатывать ПО? А права собственности? А как в дальнейшем работать с рынком? Я глубоко убежден, что ПО может и должен разрабатывать только частный капитал, разве что кто-то с кем-то договорится о кооперации.

Нам надо не десять лет догонять Запад, чтобы достичь уровня 50% отечественного ПО. Нет, у нас всего два-три года — и мы уже должны гнать на экспорт нашим партнерам свои технологии. Если мы еще чуть-чуть посидим, то и эта территория будет занята. Но инфраструктурные технологии — это не антивирус, который сам себя продает. Здесь должна быть поддержка государства — вот российская компания привезла вам российские технологии. Сам я никогда не продам технологию в крупный проект типа нашей ГАС “Правосудие” в какой-нибудь другой стране, потому что люди везде понимают, что технологии — это крючок, на который если ты сел, то много десятилетий потом будешь на нем сидеть. Тут без государственных гарантий не обойтись.

PC Week/RE — площадка для разговора о технологиях

Насколько сейчас нужны или не нужны компьютерные журналы? Мы живем в новых информационных реалиях, поэтому роль СМИ приходится переосмысливать. Привычные формы материала все еще востребованы читателями, но вместе с тем появляется запрос на что-то новое. В 2015 г. PC Week/RE отмечает двадцатилетний юбилей, но все так же остается источником актуальной информации об информационных технологиях.

Двадцать лет — это история! Не все пережили, а вы удержались! Я понимаю, что все переживают сложные времена. И вы переживали. И мы переживали. И каждый по-своему защищал свой бизнес, развивал, двигал. Вы молодцы! Я сейчас читаю прессу преимущественно в электронном виде, но, если честно, больше люблю бумажные журналы. Это дело привычки, я понимаю. Хочется полистать, вернуться, взглянуть еще раз. Что-то понравится — отчекнул, показал кому-то. Мне многое интересно в вашем издании, я знакомлюсь с мнениями людей. А как без этого? ИВК — не очень публичная компания, мы мало участвуем в каких-то внешних мероприятиях. Так получилось исторически. Недавно встретился с Василием Васиним (R-Style), он говорит: “Слушай, я думал, тебя уже нет!” Так что журналы и PC Week/RE в том числе — это моя связь с миром. Поэтому вы развивайтесь, пишите.

И пусть импортозамещение — неудачное слово, но текущая ситуация всё-таки поворачивает нас к тому, чтобы разрабатывать собственные технологии. А для обсуждения этой темы нужны какие-то площадки, где профессионалы смогут обмениваться мнениями, экспериментальными подходами, просто общаться. Где можно говорить именно об ИТ, а не только о бизнесе — кто кому что продал и сколько на этом заработал. ▣

Построение ЦОДа: моновендорный подход против мультивендорного

С ростом бизнеса любому предприятию и организации требуется и увеличение вычислительных возможностей. Это касается как крупных компаний и холдингов, так и представителей среднего и малого бизнеса. Построение новых комплексов и масштабирование уже имеющихся ресурсов — задачи непростые, требующие грамотного подхода и оптимальных решений, которые, с одной стороны, позволят предприятию сэкономить свой бюджет, не переплатив лишнего, а с другой стороны — позволят получить надежную и сбалансированную инфраструктуру, максимально удобную для модернизации и дальнейшего масштабирования. Это справедливо как для крупных центров обработки данных, так и для небольших серверных комнат, ведь, по сути, и те и другие выполняют одну и ту же задачу — обеспечивают компании возможность хранить, получать, отправлять и обрабатывать информацию, которая в современном мире, как известно, является одним из основных бизнес-активов.

Очередной кризис, бушующий сегодня в России, заставляет компании экономить и более внимательно относиться к затратам. В этой связи перед заказчиками часто возникает вопрос, какой подход лучше избрать при построении центра обработки данных или обычной серверной комнаты — моновендорный или мультивендорный. В пользу второго подхода часто выдвигаются такие аргументы, как возможность выбора самых доступных на рынке решений от различных поставщиков и производителей. С одной стороны, это удобно, так как позволяет воспользоваться различными скидками и прочими привлекательными предложениями со стороны вендоров, но с другой стороны — интеграция различных компонентов в единую и бесперебойно работающую ИТ-инфраструктуру превращается, по сути, в головную боль для сотрудников ИТ-подразделений. Да и с технической поддержкой возникают определенные сложности, поскольку у каждого производителя она своя, к каждому нужно обращаться отдельно, при этом каждый, естественно, несет ответственность только за свои продукты.

Моновендорный подход при построении ЦОДа тоже имеет как плюсы, так и минусы. Из минусов следует отметить зависимость от единого поставщика, который может уйти с рынка, прекратить работать с тем или иным заказчиком по политическим мотивам (что особенно актуально сегодня в России), изменить ценовую политику, прекратить поддержку тех или иных продуктов и решений и т. д. Все это создает дополнительные риски и сложности для заказчиков, которые могут быть уменьшены при наличии у данного вендора широкой партнерской сети в России, при этом партнеры должны обладать всеми необходимыми компетенциями по поддержке и обслуживанию. Что же касается плюсов, то здесь они несомненны. Прежде всего это удобство, легкость и простота интеграции различных компонентов, в том

числе и выпущенных в разные годы. Ведь чаще всего производители уделяют пристальное внимание совместимости новых продуктов с legacy-решениями собственного производства, чтобы дать возможность своим заказчикам “мягко” и постепенно модернизировать свою ИТ-инфраструктуру. Наконец, серьезным преимуществом в пользу моновендорного подхода можно назвать гибкую ценовую политику. Согласитесь, получить хорошую скидку от вендора намного легче, если вы приобретаете целый стек решений, а не какое-то одно.



Сегодня нередко возникают ситуации, когда ведущие американские или европейские производители ИТ-решений из-за сложной политической ситуации сокращают свое присутствие на российском рынке, перестают работать с российскими заказчиками. Но им на смену приходят как азиатские вендоры, так и компании “второго эшелона” из тех же США и Европы, которые, конечно, не пойдут на прямое нарушение законодательства своих стран, но при этом приложат максимум усилий для того, чтобы удержать существующих и приобрести новых заказчиков в России, от которых “отказались” их конкуренты.

Компанию Tripp Lite сложно назвать игроком “второго эшелона”. В США она достаточно известна, однако на российском рынке ее присутствие не столь широко. В наибольшей степени она известна специалистам в области инфраструктурных решений для сетей электропитания, однако продуктовый портфель Tripp Lite намного шире. Он включает в себя достаточно

обширный набор продуктов для построения ЦОДов, вычислительных узлов, распределенных мультисервисных сетей, серверных помещений и т. д.

В качестве примера расскажем, как можно собрать комплексное решение для обслуживания одного или нескольких серверов на примере типовых продуктов компании Tripp Lite.

Очевидно, что сначала надо серверный комплекс где-то разместить — значит, для размещения серверов необходим специальный шкаф, например модель SR42UB. Она представляет собой конструктив в наиболее часто используемой конфигурации: стандартная глубина — чуть более 1 м, ширина — 600 мм, монтажное пространство для размещения оборудования — 42U. Шкаф поставляется уже в собранном виде, что позволяет сэкономить время на сборку и установку и сразу же после распаковки приступить к размещению оборудования. При этом высота около 2 м и наличие роликов позволяют провезти его в стандартный дверной проем в собранном виде. Важным элементом любого серверного шкафа является вентиляция. В данной модели площадь perforации составляет более 65% от общей площади дверей. Наконец, решены и задачи по безопасности — установлены запираемые на ключ съемные боковые двери и боковые панели, что исключает несанкционированный доступ к оборудованию, размещенному внутри шкафа. Кстати, внутри шкафа имеются специальные монтажные направляющие, которые обеспечивают установку вертикальных аксессуаров, таких как кабельные организаторы и ПДУ, без инструментов!

После того как конструктив выбран и оборудование размещено, стоит задуматься о том, что серверное оборудование нуждается в надежном резервном электропитании, поскольку любые сбои и простои инфраструктуры чреваты финансовыми потерями для бизнеса. Одним из решений данной проблемы для узлов небольшой мощности может стать онлайнный источник бесперебойного питания Tripp Lite SU20KRTG. Эта модель ИБП с двойным преобразованием, мощностью 20 кВА/18кВт занимает всего 12U стоечного пространства. При необходимости время работы ИБП может быть продлено благодаря дополнительным внешним аккумуляторным батареям. Замену внешних батарей можно осуществлять в режиме эксплуатации, без необходимости отключения оборудования. Главной отличительной особенностью решений Tripp Lite класса online в сегменте мощностей 6—20 кВА является наличие интегрированного сервисного байпаса в съемную вводно-распределительную панель, что обеспечивает практически нулевое время простоя оборудования в год.

Помимо однофазных решений линейка ИБП Tripp Lite включает мощные 3-фазные модульные ИБП мощностью от 20 до 120 кВА. Учитывая возможность параллельного подключения до 4-х таких

систем, на их основе можно строить комплексы с потреблением до 480 кВА. Работа в параллельном режиме и модульность позволяют также строить комплексы с разными уровнями резервирования — от самых простых до сложных.

Не всегда одной точки — ИБП — хватает для снабжения питанием потребителей даже в пределах одного шкафа, поэтому в этом случае для распределения питания от ИБП в ЦОДе или серверном помещении применяются распределители питания (PDU, Power Distribution Unit). Модели PDU на текущий момент имеют множество модификаций и функциональных особенностей — компания Tripp Lite предлагает потребителям базовые, с измерителем, контролируемые и управляемые PDU мощностью от 3,6 до 27,7 кВт. На текущий момент флагманами линейки PDU являются управляемые блоки, рассчитанные на 27,7кВт потребляемой мощности, с функцией удаленного контроля и управления, при этом обеспечивается удаленный контроль потребления тока для каждой розетки индивидуально! Но не всем требуются такие мощности, поэтому можно выбрать нужный именно вам PDU с необходимым функционалом.

Оборудование в серверных помещениях нуждается также и в охлаждении. Для этой цели могут быть использованы энергосберегающие кондиционеры. Одна из моделей компании Tripp Lite, SRXC00L33K, обеспечивает мощность охлаждения 33 000 BTU (9,7 кВт) при снижении потребляемой электрической мощности на одну треть. За счет адаптивной технологии управления скоростью вращения вентиляторов устройство поддерживает охлаждение на таком уровне, какой необходим. А отсутствие бросков пусковых токов при старте системы возможно благодаря инверторному компрессору постоянного тока с регулируемой частотой вращения и электронному расширительному вентилю с микропроцессорным управлением. Функция плавного пуска ограничивает бросок пускового тока, предотвращая возникновение шумов в линии и перегрузок цепи, а повторное увлажнение конденсата и его вывод с потоком выпускаемого воздуха исключает необходимость в наличии сливного отверстия в полу и резервуара для сбора воды.

Мы рассказали лишь о некоторых продуктах компании Tripp Lite, которые могут обеспечить надежную, бесперебойную и комфортную работу серверного парка.

Для управления ИБП, PDU и кондиционерами Tripp Lite предлагает бесплатное ПО локального и сетевого управления PowerAlert. PowerAlert состоит из трех компонентов — PowerAlert Local для локального управления ИБП через USB- или Com-порт, PowerAlert Shutdown Agent для корректного отключения группы серверов и PowerAlert NMS для централизованного удаленного контроля и мониторинга более 250 устройств из единого административного интерфейса.

Инфраструктура...

◀ ПРОДОЛЖЕНИЕ СО С. 6

закрытую архитектуру) модель x86 (архитектура процессора закрыта, но доступны референсные дизайны аппаратных платформ) и подход ARM (архитектура процессора открыта, но не поддерживается разработка платформ). Модель, предлагаемая OpenPOWER, объединяет лучшие качества указанных трех подходов и является сегодня единственной архитектурой, способной конкурировать с x86 на рынке тяжелых корпоративных систем. С другой стороны, если планируется проектирование собственных кристаллов, то следует помнить о достаточно высокой стоимости лицензирования ядра процессора (деньги получает не IBM, а консорциум). Если же компания будет заниматься только ди-

зайном систем (но не процессоров), то, по мнению Всеволода Опанасенко, у архитектуры OpenPOWER нет особых преимуществ перед x86.

Со своей стороны менеджер московского офиса IBM по продуктам и решениям Power Systems Алексей Перевозчиков отметил, что аналогичные по числу процессоров серверы на Power пусть и вдвое дороже, но зато втрое производительнее машин на x86. Кроме того, возможность разрабатывать собственный микрокод открывает перспективы для создания отечественных доверенных систем, сертифицированных местными регулирующими органами. Российские участники консорциума OpenPOWER — компании “Технопром” и Yadro уже приступили к проектированию собственных систем. Как сообщил президент Национальной компьютерной корпорации (ННК) Алек-

сандр Калинин, Yadro (входит в ННК) заключила уже около десятка контрактов с российскими заказчиками и через несколько месяцев планирует выйти на рынок с собственными продуктами. Пока речь идет в основном о сборке из импортных комплектующих, но у компании есть планы по постепенной локализации производства в нашей стране.

В апреле консорциум OpenPOWER присоединила еще одна российская компания — “Рикор”, обладающая собственной производственной базой в Арзамасе и центром разработки в Москве. Как рассказал ее вице-президент Борис Иванов, у “Рикор” весьма амбициозные планы: наряду с разработкой системной платы и адаптации решений на базе Linux компания к 2019 г. собирается разработать и передать в производство собственную версию процессора Power, которую

можно будет сертифицировать в российских государственных органах.

Насколько реальны такие планы?

Опыт китайской компании Suzhou PowerCore, о котором рассказывал Алексей Перевозчиков, свидетельствует о том, что подобную задачу вполне можно решить. Вступив в консорциум OpenPOWER в начале 2014 г., она уже в марте 2015-го представила собственный Power-процессор CP1, на основе которого к концу нынешнего года начнется выпуск линейки двухпроцессорных серверов RedPower. Следует, правда, учесть, что в течение этого года при поддержке министерства промышленности и информационных технологий Китая был учрежден альянс China Power Technology Alliance, а в консорциум OpenPOWER вступили еще 12 местных компаний, включая такие крупные, как Inspur и ZTE. □

“ИТ-руководитель должен рассматривать каждую проблему и глазами бизнес-заказчика”

СЕРГЕЙ КОСТЯКОВ

У людей, которые сегодня занимают ключевые позиции в руководстве ИТ-подразделений крупнейших структур отечественного бизнеса, карьера почти всегда связана с развитием самого ИТ-рынка в России. Об этом, а также о перспективах развития и автоматизации банковского сектора экономики рассказывает старший вице-президент, руководитель департамента информационных технологий банка ВТБ Дмитрий Назипов.

Ваша карьера в ИТ фактически охватывает все характерные для отечественного ИТ-рынка периоды. Поэтому вначале расскажите о том, как она развивалась.

В моей карьере условно можно выделить три этапа. Первый, в начале 1990-х, по сути, совпал с эпохой становления информационных технологий как самостоятельной отрасли в экономике современной России. Думаю, и сейчас многие помнят характерные приметы того времени. Экзотические схемы поставки только появившихся персональных компьютеров, иногда за бартер, иногда за разные квази-деньги, например векселя, первые локальные сети на коаксиальном кабеле, первые модемы и предтеча Интернета сеть Релком. Как правило, капитанами бизнеса смутно формулировалась лишь общая цель использования компьютеров для того, чтобы бухгалтеры или, скажем, кладовщики решали на них свои учетные задачи.

В любом случае необходимо было создавать программное обеспечение соответствующей функциональности для бизнес-приложений, чем я и начал заниматься в начале 1990-х, руководя подразделением разработки достаточно крупной региональной ИТ-компании. Помимо профессионального опыта программирования это дало мне возможность уже тогда понять ключевую проблематику корпоративного рынка, почувствовать, какие тенденции проявятся в перспективе. Сейчас многие выводы того времени могут, наверное, показаться очевидными, но, повторю, это были “лохматые” девяностые...

Очень важно, что уже в то время у меня была возможность плотно общаться с людьми, которых сегодня принято называть ключевыми бизнес-пользователями. И соответственно вплоть до нюансов понять их отношение к информационным технологиям, мотивацию применения ИТ-продуктов, степень подготовки к работе с ними и т. д.

Мой профессиональный круг общения в то время в основном состоял из руководителей предприятий, главных бухгалтеров и экономистов, а это люди весьма консервативных взглядов, часто с опаской подходящие к компьютеру и ИТ в целом. Тем не менее со временем некоторые из них настолько увлеклись информационными технологиями, что нам приходилось встраивать в классический функционал производственных ИТ-систем весьма экзотические функции.

Второй этап моей карьеры был связан с государственным сектором. Десять лет я руководил ИТ-департаментом Правительства Чувашской Республики и про-



Дмитрий Назипов

граммой развития ИТ данного региона. Свою карьеру там я завершил на посту министра по информатизации и связи.

В известной мере это тоже был старт практически с нуля. К моменту моего прихода на все правительство Чувашии было пять компьютеров, с помощью которых печатали документы для первых лиц республики.

Когда я уходил, компьютеры были уже в каждом кабинете, развивался безбумажный документооборот. Сервис электронной почты и правительственный сегмент Интернета охватывал сотни организаций на всей территории республики. Но самое главное, наверное, в том, что тогда я, что называется, оказался в самой гуще событий. Я застал начало реализации известной программы “Электронная Россия”, которая позднее трансформировалась в “Электронное правительство” и “Электронное общество”, и в то время наш регион был выбран на федеральном уровне в качестве пилотного.

А в 2004 г. я пришел на работу в банк ВТБ. Здесь ситуация была уже несколько иная, я начал работать в сфере бизнеса с уже сложившимися на тот момент подходами к автоматизации и достаточно зрелыми бизнес-процессами. Впрочем, в отношении развития этих подходов банковская отрасль уже тогда была и по сей день остается весьма динамичной.

Как выделенные вами этапы карьеры связаны между собой? Что оставалось неизменным и что менялось?

Неизменным оставалась основная специальность — ИТ, но радикально отличались запросы заказчиков и сами подходы к автоматизации ИТ-систем. Это было и остается весьма увлекательным — участие в становлении и развитии отрасли ИТ! Как я уже упоминал, сначала у меня был опыт коммерческой разработки программного обеспечения по заказу предприятий самых разных отраслей — от оборонного сектора до сельского хозяйства. Затем, на государственной службе я осознал, каким образом формируется общественный интерес к тому или иному направлению развития ИТ и сервисов. То время в целом характеризуется становлением фундаментального подхода к автоматизации государствен-

ПРОДОЛЖЕНИЕ НА С. 14 ►



ЭКСПЕРТИЗА. ИННОВАЦИИ. ФОКУС НА КЛИЕНТА. КОМПЛЕКСНЫЕ РЕШЕНИЯ В СФЕРЕ ИТ-БЕЗОПАСНОСТИ.

ЭТО – ПРАВИЛЬНЫЙ ПОДХОД!

«Мы установили решение Kaspersky Small Office Security, и теперь я спокойно думаю о том, как помочь бизнесу в нашей области, а не о том, как бы не поймать вирус на ноутбук»

Наталья Нестерова,
директор журнала «Бизнес и Власть»,
Вологда



www.kaspersky.ru/podhod

+7 800 755 88 08

© АО «Лаборатория Касперского», 2015



KASPERSKY Lab

Внутренние и внешние ИБ-угрозы: есть ли смысл в их разделении?

ВАЛЕРИЙ ВАСИЛЬЕВ

Усложнение корпоративных ИКТ-инфраструктур и ландшафта киберугроз требует комплексного подхода к организации корпоративной информационной безопасности. Тем не менее по-прежнему принято различать внутренние и внешние ИБ-угрозы и связанные с ними риски. В данном обзоре мы постарались выяснить актуальность разделения ИБ-угроз на внешние и внутренние, определить, где проходит граница между этими видами ИБ-угроз, какие специальные технологии и инструменты используются для противодействия им, в каких структурных компонентах корпоративной ИБ-системы организуется комплексное противодействие обоим видам угроз.

ОБЗОР

Актуальность разделения ИБ-угроз на внешние и внутренние

Еще сравнительно недавно вопрос о целесообразности разделения угроз на внешние и внутренние можно было отнести к разряду надуманных. Так, по мнению директора по развитию бизнеса Центра информационной безопасности компании «Инфосистемы Джет» Евгения Акимова, такое разделение имеет вполне практический смысл, позволяя четко определиться с адекватными механизмами защиты. Более того, как полагает менеджер продукта компании «Код Безопасности» Иван Бойцов, разделение ИБ-угроз по типам и источникам актуально всегда — это общепринятая практика, поскольку универсальной защиты сразу от всех типов угроз не существует. Некоторые меры защиты могут быть общими как для внешних, так и для внутренних угроз, но большая часть из них все же направлена только на один тип нарушителя. В качестве примера г-н Бойцов приводит «Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России, где тоже разделяются угрозы, связанные с внешним или внутренним нарушителем, и дополнительно выделяются угрозы, возникающие в результате внедрения аппаратных закладок и вредоносных программ. «Такое разделение угроз, — подчеркивает Иван Бойцов, — помогает определить характерные для данной компании уязвимости, оценить возможные риски и эффективнее применять соответствующие меры защиты».

Вместе с тем эксперты отмечают важные перемены в области ИБ. Ранее считалось, отмечает руководитель программ безопасности Microsoft в России Андрей Бешков, что внутренние сотрудники, которые могут представлять угрозу для предприятия своими намеренными действиями или халатностью, несмотря на то, что имеют больше возможностей, чем атакующие извне, все-таки надежно контролируются, поскольку находятся внутри периметра. Однако в последние годы в связи с коньюмеризацией ИТ и распространением практики BYOD корпоративный периметр стал размываться, а то и полностью исчезать.

Подтверждая этот тезис, директор по решениям DeviceLock компании «Смарт Лайн Инк» Сергей Вахонин обращает внимание на то, что большинство сервисов социальных сетей, приложения облачных хранилищ, мессенджеры, используемые персоналом, попросту игнорируют корпоративные средства защиты и границы инфраструктуры: «Практически все сетевые приложения, созданные для удобства пользователей, для удовлетворения их социальных потребностей, функционируют абсолютно без какой-либо обратной связи с инструментарием корпоративной безопасности и контроля.

Модель информационной безопасности потребительских приложений основывается на том, что все решения о способах и уровне авторизации, аутентификации и уровне доступа к данным принимает конечный пользователь, который далеко не всегда является владельцем данных, будучи также сотрудником какой-либо организации». Все упомянутое выше позволяет Сергею Вахонину сделать вывод о том, что современная корпоративная модель ИБ, чтобы стать реально эффективной, должна быть информационно-центричной, опираться на совокупность контроля непосредственно данных и различных потоков их передачи и распространения.

По некоторым оценкам, внутренний сотрудник сегодня оказывается замешан в 80% ИБ-инцидентов. Довольно часто, по словам Андрея Бешкова, злоумышленники сначала захватывают идентификационные данные внутреннего сотрудника и уже затем действуют от его имени. Поэтому осталось мало смысла в разделении ИБ-угроз на внешние и внутренние. «В современных условиях, — считает он, — нужно вести проактивную ИБ-работу и разделять предприятие периметрами не только снаружи, но и внутри».

Схожей точки зрения придерживается и начальник отдела информационной безопасности ГК «Компьюлинк» Игорь Гавриш, который предлагает разделять внешние и внутренние угрозы лишь для обозначения класса применяемых для противодействия им технических решений, но не в рамках построения и модернизации системы информационной безопасности. Это, по его мнению, стало неактуально.

С тем, что наиболее опасные угрозы для корпоративной ИБ сегодня все чаще имеют гибридный характер, а потому стратегия обеспечения ИБ должна развиваться с учетом этой тенденции, согласен и Олег Глебов, менеджер по сопровождению корпоративных продаж «Лаборатории Касперского». В то же время, считает он, риски, связанные со злонамеренной инсайдерской активностью, резонно остаются исключительно внутренней проблемой и должны рассматриваться отдельно.

Внешние и внутренние угрозы — что опаснее?

Неоднозначность в подходах к разделению ИБ-угроз отражают и результаты недавнего исследования института SANS, показавшие, что 74% опрошенных ИБ-специалистов озабочены внутренними угрозами; 32% признают, что у них нет возможностей противостоять инсайдерам; 28% отметили, что в их организациях защита от инсайдеров вообще не считается приоритетной; 62% считают, что в планах реагирования на инциденты нет различия между внешними атакующими и внутренними.

В то же время в недавно опубликованных компанией Solar Security результатах исследований примерно 64% изученных ее специалистами ИБ-инцидентов, случившихся в I квартале 2015 г., были классифицированы как имеющие именно внутренние причины.

«Нехорошие» сотрудники своими нелегитимными действиями внутри предприятия могут причинять ему ущерб не только в виде утечек данных, но и в виде прямого воровства денежных и материальных ресурсов с использованием ИТ-систем. Бывают случаи, когда персонал организует реальные хакерские атаки внутри компании. Например, очень сложно противостоять угрозам, при реализации которых сотрудники компании вступают вговор с третьими лицами. Так, если злоумышленнику крайне непросто внедрить вредо-

носный код в продакшн-систему (для этого требуется обойти массу барьеров и только после этого провести внедрение кода, который будет, к примеру, перенаправлять злоумышленнику информацию о заказе в интернет-магазине), то при возможности «договориться» с разработчиком приложения задача существенно упрощается. Обнаружение таких угроз требует выстроенных процессов безопасной разработки софта, о которых сейчас, увы, больше говорят, чем что-то реально делают.

По мнению Андрея Бешкова, внутренние угрозы находятся сейчас как бы ниже уровня чувствительности радара обнаружения атак: «Мало кто с ними реально разбирается и мало кто занимается защитой от них». Вместе с тем, учитывая то, что инсайдеры изначально имеют немалые полномочия доступа к ресурсам, они, по мнению Андрея Бешкова, опаснее внешних атакующих, поскольку с внешними угрозами индустрия ИБ, как он считает, уже более или менее научилась бороться.

Сергей Вахонин обращает внимание на разницу в подходах служб ИБ к противодействию внутренним и внешним угрозам. «Почему-то считается нормальным и правильным, — отмечает он, — внешним угрозам именно противодействовать, отражать внешние атаки, не допускать компрометации учетных записей и т. д. При этом в плане противодействия наиболее актуальной угрозе внутреннего характера — утечкам данных — зачастую подход обратный. Многие службы ИБ допускают утечки, преследуя только одну цель — зафиксировать утечку, а затем уже провести расследование инцидента».

Традиционно, считает Андрей Бешков, предприятия чрезмерно доверяют своим сотрудникам: «Их защита напоминает яйцо: снаружи более или менее твердая скорлупа, а внутри мягкая среда, и как только злоумышленник попадает в нее, он может делать все, что хочет».

Внутренние атаки, отмечает Иван Бойцов, остаются самыми опасными из-за размеров причиняемых ими прямых убытков. Это подтверждают ежегодные отчеты, публикуемые ISACA, PwC, Verizon и другими аналитическими компаниями. Происходит это потому, что потенциальный внутренний нарушитель знает, как устроены информационные системы, и зачастую располагает прямым доступом к конфиденциальной информации. Кроме того, внутреннему нарушителю заранее известно, какую информацию можно использовать для извлечения собственной прибыли.

Внешний же нарушитель должен потратить гораздо больше сил для атаки. Ему необходимо не только провести разведку и найти уязвимые места в системе защиты, но и определить ценность и локализацию полезных для него данных. С другой стороны, внешние атаки, по мнению Ивана Бойцова, опасны из-за косвенных убытков, так как часто они направлены на отказ в обслуживании публичной инфраструктуры организации. Такие атаки ведут к простоям в обслуживании клиентов, упущенной прибыли и репутационным потерям.

С этими выводами согласен ведущий консультант по ИБ компании R-Style Антон Зыков, который тоже считает, что угрозы, которые могут быть реализованы внутренним нарушителем, опаснее, так как он уже находится в офисе, в сети компании и обладает рядом экстра-возможностей: делегированным доступом, информацией, знаниями и способами их получения; по этой же причине внутренний пользователь часто становится первичной мишенью для внешних нарушителей.

Впрочем, есть и другое мнение. В отличие от процитированных выше экспер-

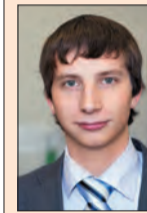
Наши эксперты



ЕВГЕНИЙ АКИМОВ, директор по развитию бизнеса Центра информационной безопасности компании «Инфосистемы Джет»



АНДРЕЙ БЕШКОВ, руководитель программ безопасности Microsoft в России



ИВАН БОЙЦОВ, менеджер продукта компании «Код Безопасности»



СЕРГЕЙ ВАХОНИН, директор по решениям DeviceLock компании «Смарт Лайн Инк»



ИГОРЬ ГАВРИШ, начальник отдела информационной безопасности ГК «Компьюлинк»



ОЛЕГ ГЛЕБОВ, менеджер по сопровождению корпоративных продаж «Лаборатории Касперского»



АНТОН ЗЫКОВ, ведущий консультант по ИБ компании R-Style

тов Евгений Акимов полагает, что самые опасные ИБ-угрозы сегодня связаны с деятельностью внешних злоумышленников, чья активность в первую очередь направлена на кражу денег (например, через списание средств с банковских счетов с помощью вредоносной программы, подсаженной на компьютер главного бухгалтера). Жертвой такой атаки может оказаться любое предприятие — не обязательно банк.

Следует также помнить, что возможности внутренних и внешних нарушителей со временем эволюционируют. Сергей Вахонин и Игорь Гавриш обращают внимание на то, что внешняя атака, если преодолевает средства защиты корпоративного периметра, переходит в категорию внутренних угроз.

Современные кибератаки, добавляет Антон Зыков, проводятся сразу по нескольким векторам — как по внешним, так и по внутренним. Все чаще применяются сложные комплексные атаки типа таргетированных (APT-атаки). Поэтому наряду с традиционными инструмен-

► тами необходимо применять подходы, позволяющие адекватно противостоять новым вызовам. Такие подходы строятся на принципе “знай своего врага и знай себя”. Смысл его заключается в способности компании прогнозировать поведение нарушителя и выявлять отклонения от нормальных среднестатистических признаков поведения своих пользователей. Для реализации этого принципа компания должна обладать информацией о том, что происходит во внешней среде и у себя внутри.

Слияние защиты от атак по внутренним и внешним векторам в защиту от единой, комплексной атаки произошло благодаря серьезным инвестициям компаний в средства защиты периметра сети, которые стали представлять собой эффективный заслон от внешних угроз, полагает Олег Глебов. С экономической стороны затраты на атаку “в лоб” могут оказаться для злоумышленников выше, чем возможная выгода в случае ее успеха. В результате злоумышленникам гораздо дешевле и проще использовать методы социальной инженерии, атаковать поставщиков и партнеров, использовать иные методы для того, чтобы попасть внутрь сети в обход средств защиты. В этом случае в помощь периметровой защите подключаются технологии не превентивного характера, а детектирующие, которые нацелены на максимально быстрое обнаружение любой подозрительной активности внутри инфраструктуры.

Защита от внешних и внутренних ИБ-угроз

Традиционно меры и средства защиты разделяются на организационные и технические. В обзоре мы тоже следуем такому разделению.

Организационные меры. Как отмечает Игорь Гавриш, организационные меры включают в себя, как минимум, назначение ответственного за ИБ в компании, контроль исполнения пользователем положений нормативно-правовых актов в области ИБ (НПА) по работе с информационными системами, регламентов и инструкций работы с подсистемами ИБ. Комплект НПА объединяют в рамках единой политики ИБ. Для выполнения требований законодательства по защите персональных данных в структуре НПА предусматривают дополнительные документы, запрашиваемые регуляторами в ходе проведения проверок.

Для обеспечения защиты от внутренних нарушителей в трудовых соглашениях с работниками компании прописывают пункты об ответственности за разглашение конфиденциальной информации, а также вводят режим коммерческой тайны, позволяющий, согласно законодательству, защитить интересы работодателя.

Говоря об организационных мерах, способствующих защите конфиденциальной информации от разглашения лицами, не являющимися сотрудниками компании, Игорь Гавриш предлагает в первую очередь заключать соглашения с контрагентами о неразглашении конфиденциальной информации, ставшей известной представителям контрагента в ходе договорных отношений. Для обеспечения доказуемости такого рода разглашений необходимо опять же ввести в компании режим коммерческой тайны, потому что в противном случае невозможно будет доказать, что являлось информацией, составляющей коммерческую тайну, а что — нет.

“Организационными мерами, — отмечает Антон Зыков, — невозможно воздействовать на поведение внешних нарушителей — субъектов, с которыми компания никак не связана формально. Зато их можно и нужно применять к внутренним пользователям, с тем чтобы они и сами не совершали нарушений, и не стали жертвами внешних нарушите-

лей, попадаясь на всевозможные уловки. В первую очередь к таким мерам относятся повышение ИБ-осведомленности и четкая регламентация выполняемых бизнес-операций”.

В организационных мерах обнаружить новые веяния, по мнению Ивана Бойцова, сложно, так как состав таких мер практически не меняется — разработка моделей угроз, нарушителей, защиты, составление политики безопасности, инструкций для сотрудников и регламентов работы, ввод режима коммерческой тайны и т. д. Все эти меры обязательны и необходимы для любой инфраструктуры и позволяют формализовать и упорядочить подход к защите информации.

Большую роль в защите от внутренних и внешних угроз играет обучение персонала вопросам защиты информации. Так как множество атак производится с помощью социальной инженерии, т. е. нетехническими методами, защиту от таких угроз можно выстроить только с помощью информирования сотрудников и обучения их работе по регламентам.

Если атака все же случилась, то первым лицом в реагировании, как отмечает Олег Глебов, в большинстве случаев становится вовсе не офицер ИБ, а сотрудник технической поддержки. Упущенное время оставляет злоумышленникам возможности для успешного завершения атаки и сокрытия следов. Поэтому правильная подготовка сотрудников технической поддержки в части ИТ-ориентированного обучения аспектам ИБ — важнейший элемент первичного детектирования и фильтрации ИБ-инцидентов от ИТ-событий.

Андрей Бешков рекомендует начинать строить ИБ-защиту вовсе не с внедрения технологических средств и инструментов. В первую очередь, полагает он, следует провести классификацию данных и процессов, чтобы понять, что именно предстоит защищать и каковы приоритетные направления защиты, поскольку без установкой приоритетов все будет защищено одинаково плохо. При этом приоритеты должен определять не ИБ-специалист, а представители бизнеса компании. Следует выяснить, какие системы необходимо защищать в первую очередь, т. е. такие, без которых бизнес просто остановится, определить системы, на защите которых можно сэкономить или вообще не защищать.

В этом могут помочь инструменты, позволяющие понять, где и что хранится в корпоративной среде. Поможет также инвентаризация систем ИКТ-инфраструктуры на предмет выяснения того, где и что установлено, и в налаживании правильного управления обновлениями систем и изменениями конфигураций (с помощью соответствующих продуктов).

Затем предстоит решить, как сегментировать внутренние и внешние сети. Это нужно сделать обязательно, потому что компрометация инфраструктуры в длительной перспективе неизбежна, следовательно, нужно строить изолированные отсеки, как на кораблях или подводных лодках, дабы повысить живучесть инфраструктуры и сервисов в целом.

В особо защищаемые сегменты нужно вынести жизненно важные для бизнеса системы и решить, из каких сегментов сети к ним будет доступ — будут ли, например, эти системы доступны сотрудникам с мобильными устройствами или только тем, которые пользуются стационарными ПК из внутренней сети.

После этого надо постараться минимизировать число привилегированных пользователей и внедрить ролевой доступ к системам. Затем можно начинать внедрять системы протоколирования действий привилегированных пользователей и ограничить количество действий, доступных для выполнения ими.

Практически все упомянутые меры защиты актуальны и для внешних, и для

внутренних атак. “В условиях, когда атаки стали выполняться сразу по нескольким векторам, стоит избавиться от веры в единый периметр и создавать несколько периметров и сегментов сети для минимизации ущерба, — считает Андрей Бешков. — Вера в неуязвимость инфраструктуры губительна. Это значит, что особое внимание стоит уделить тестированию инфраструктуры на проникновение”.

Нужно также спланировать регулярный поиск, возможно, уже происходящих компрометаций систем, учитывая, что с момента компрометации до момента ее обнаружения проходит в среднем более 200 дней. За это время атакующие надежно и удобно обустраиваются в захваченных инфраструктурах. В результате изгонять их оттуда очень сложно, поэтому чем раньше обнаруживается компрометация, тем легче бороться с атакующими. В этом может помочь внедрение систем класса SIEM и систем анализа поведения инфраструктуры и пользователей. На вершине всей архитектуры защиты должны располагаться меры и средства по обеспечению непрерывности бизнеса, включающие в себя тренинги по реагированию на инциденты и восстановлению бизнеса после инцидента.

Технические средства. До тех пор, полагает Евгений Акимов, пока внешние и внутренние злоумышленники не начинают работать в связке, механизмы защиты от них, как правило, выстраиваются разные.

Для противодействия внешним и внутренним угрозам применяют специализированные средства защиты, начиная с систем предотвращения вторжений и межсетевых экранов и завершая комплексами решений, направленными на противодействие таргетированным атакам: песочницы, системы управления ИБ и событиями ИБ, веб-шлюзы, шлюзы электронной почты, средства мониторинга действий администраторов и других привилегированных пользователей, контроль выполняемых транзакций и поведенческих моделей, контроль уязвимостей инфраструктурных компонентов и бизнес-приложений и др.

В связи с постоянными изменениями (прежде всего во внешней среде) данные для таких средств нужно поддерживать в актуальном состоянии, для чего должен быть выстроен четкий процесс постоянного мониторинга на базе служб реагирования на инциденты (SOC) с применением аналитических данных из внешних и внутренних источников (Threat Intelligence).

Против внутренних угроз упомянутые выше решения применяются редко — для этого прежде всего используются хорошо известные системы управления доступом, системы предотвращения утечек данных, а теперь и фрод-машины, выявляющие мошеннические схемы в различных бизнес-операциях, начиная от воровства на кассовых аппаратах и завершая нарушениями в логистике.

Подход к защите от внешних угроз, отмечает Иван Бойцов, постепенно смещается в сторону усиления контроля защищенности. На рынке появляются новые инструменты для проверки политики безопасности, правильности настройки оборудования и проведения анализа защищенности.

На фоне растущего числа и качества угроз и, как следствие, количества и усложнения применяемых средств защиты на первый план выходят задачи управления всей корпоративной ИБ-системой. Вести мониторинг и управлять всеми защитными механизмами, внедренными в компании, становится затруднительно и дорого. В то же время несовместимость и разрозненность средств защиты информации (СЗИ) сами по себе создают дополнительные угрозы ИБ. Поэтому сейчас вендоры стремятся совмещать защитные механизмы в одном продукте

и предоставлять заказчику возможность работать с ними через единый интерфейс управления.

Комплексный подход к защите, считает Иван Бойцов, в первую очередь выражается в корреляции событий безопасности и интеграции различных механизмов защиты между собой. Современная система защиты должна строиться не на разрозненных средствах защиты, способных работать только в своей узкой области, а на комплексных продуктах, умеющих сопоставлять между собой различные события и позволяющих вырабатывать комплексную реакцию в зависимости от общей ситуации.

Олег Глебов обращает внимание на рост востребованности систем автоматизации процессов расследования инцидентов (форензика). Эти системы не являются превентивными, но, относясь к средствам апостериорной защиты, предлагают мощный инструментарий для постоянного сбора данных и проведения глубоких расследований на постоянной основе или в случае уже произошедших инцидентов (неважно, внутренних или внешних).

К сожалению, сегодня, отмечает Игорь Гавриш, только небольшое число компаний имеют проработанную стратегию, используют такие комплексные решения, как сбор и корреляция событий ИБ (из источников внешних и внутренних угроз), комбинированные решения сетевой безопасности (защиты от внешних и внутренних угроз). По его мнению, комплексный подход к организации корпоративной ИБ — сущность достаточно сложная, система менеджмента ИБ для обеспечения комплексности должна быть частью общей системы управления компанией и должна основываться на управлении бизнес-рисками для создания, внедрения, эксплуатации, мониторинга, анализа, поддержания и улучшения ИБ.

Нельзя также забывать, что обеспечение ИБ — непрерывный процесс. Пока существует сама информация, требующая защиты, система менеджмента ИБ (СМИБ) должна основываться на известной модели PDCA (Plan-Do-Act-Control, планирование — осуществление — проверка — действие).

Роль государственного регулирования при построении защиты от внешних и внутренних угроз

Государственное регулирование в области ИБ, независимо от происходящих в экономике и политике процессов, по мнению Ивана Бойцова, играет важную роль в любое время, так как защищает интересы государства и его граждан. Конечно же, органы регулирования ориентируются на общую политику государства в области кибербезопасности и в других смежных областях (например, импортозамещении). В то же время он считает, что основное влияние на регуляторов и формирование нормативно-правовой базы оказывает развитие ИТ, появление новых векторов атак и другие технические изменения.

Обращаясь к конкретным направлениям регулирования, Олег Глебов отмечает, что жесткие требования сертификации ПО, как минимум, показали свою пользу в борьбе с незадекларированным функционалом (бэкдорами, закладками и т. п.). Резонно, на его взгляд, рассмотреть возможность для промышленных предприятий и энергетики иметь средства сбора данных о состоянии критичных процессов в технологических сетях, которые могли бы передавать эту информацию, например, в государственные центры мониторинга критичной инфраструктуры. Это, по его мнению, позволило бы не только снизить время обнаружения готовящихся внешних атак на промышленные инфраструктуры, но и проводить расследования по фактам о причинах возникновения инцидентов. □

Finnopolis 2015...

◀ ПРОДОЛЖЕНИЕ СО С. 1

было бы отнести перевод денег, предоставляемый некоторыми социальными сетями для своих участников, а также использование денежных средств, хранящихся на счетах пользователей мобильных устройств, в качестве универсальных средств платежа.

И наконец, еще одну тему, обозначенную г-ном Грефом и прошедшую красной нитью через все последующие дискуссии мероприятия, можно определить как использование виртуальных денег и криптовалют в широкой практике финансовых расчетов.

На данные вызовы, связанные в основном с развитием ИКТ, самого банковского бизнеса, а также с трансформацией привычек клиентов, обязательно должен складываться ответ со стороны:

— государства как регулятора взаимоотношений участников рынка и инициатора формирования базовой ИКТ-инфраструктуры для функционирования электронного бизнеса в целом;

— отдельных финансовых компаний в отношении трансформации стратегии и операционных процессов, которые бы отвечали вновь складывающейся ситуации;

— банковского сообщества, создающего предпосылки

для создания и развития новой инфраструктуры финансовых услуг в стране;

— участников ИТ-рынка в отношении конкретных предложений по автоматизации финансовых институтов в современных условиях.

И эти вопросы также обсуждались на Finnopolis 2015.

Еще один ключевой участник панельной дискуссии Форума, председатель Банка России Эльвира Набиуллина сделала явный акцент на том, что роль ЦБ в регулировании новой инфраструктуры финансовых сервисов должна быть не ведущей, а скорее ведомой. В ее трактовке это означает, что возглавляемой ей организации целесообразно постоянно мониторить развитие рынка финансовых услуг и ждать появления любых устойчивых и значимых для него изменений. И только после этого следует готовить регулирующие акты и лоббировать законодательные инициативы, полностью адекватные складывающейся ситуации.

Что касается формирования базовой ИКТ-инфраструктуры для функционирования электронного бизнеса, Николай Никифоров отметил, что сегодня в России в Интернет ежедневно выходят около 60 млн. человек и каждый день к широкополосному доступу подключается порядка 12 тыс. новых пользователей. Цель же в

настоящее время состоит в том, чтобы охватить данным форматом доступа в Сеть не только крупные города (что, как известно, уже сделано), но и все населенные пункты страны с численностью населения от 250 человек.

По поводу вопроса о том, как может меняться сама финансовая индустрия, весьма показательно мнение одного из официальных партнеров конференции — китайской компании Huawei. Дело в том, что в последнее время компания перестает позиционировать себя как поставщик (хотя и очень крупный) преимущественно телекоммуникационных решений и переходит к продвижению широкого спектра инфраструктурных решений корпоративного уровня, выходя соответственно на отраслевые рынки. Финансовая же индустрия для Huawei является одной из ключевых, и свои предложения компания должна определять с учетом самых последних отраслевых тенденций и никак иначе.

По мнению выступившего на конференции президента Huawei в России Вань Бяо, банки сегодня отходят от роли финансовых посредников и двигаются к оказанию полного набора комплексных финансовых услуг, в том числе интегрируя в них элементы сервисов, предоставляемых небанковскими структурами. Другой отмеченной им заметной тенденцией является смещение акцента большинства современных индустрий от производства продуктов к их продвижению на рынок, что для банков означает переход к необходимости плотного взаимодействия со всей клиентской аудиторией, а не только с наиболее активной ее частью.

Подобная ситуация, по мнению главы Huawei в России, требует адекватных отраслевых решений в сфере ИТ-инфраструктуры, на развитие которой во многом и направлена деятельность компании.

Сегодня компания, в частности, предлагает финансовой отрасли:

- создание открытой распределенной ИТ-инфраструктуры, способной поддерживать наиболее популярные в корпоративном мире открытые платформы (OpenStack, Hadoop, OpenFlow) и содержащей все их основные компоненты;

- формирование полноценной платформы категории Big Data (Huawei FusionInsight), имеющей богатый спектр инструментов работы с неструктурированной информацией.

Конкретные аппаратные и программные элементы данной инфраструктуры были продемонстрированы на форуме. Что касается готовых прикладных решений в сфере автоматизации предоставления финансовых сервисов, Huawei активно сотрудничает с ISV-компаниями, создавая, по словам руководителей самой компании, отраслевые (и в том числе финансовую) экосистемы. Такая политика уже начала реализовываться и в России. □

ИТ-руководитель...

◀ ПРОДОЛЖЕНИЕ СО С. 11

Лично мне приходится заниматься целым спектром ИТ-направлений: строить центры обработки данных, внедрять информационные системы, думать о концепции информационной безопасности, а еще и самому популяризировать информационные технологии.

С приходом в ВТБ мне пришлось осваивать профессиональные тонкости функционирования финансовой отрасли, в которой ИТ играет ключевую роль.

Дала ли мне что-либо синергия, полученная от этого опыта? Конечно! Важно панорамное видение ИТ-проблематики (360-view — С.К.). Суть его примерно в следующем: ИТ-руководитель должен рассматривать каждую сколько-нибудь значимую проблему не только как глава ИТ-департамента, но и глазами бизнес-заказчика и с позиции одного из топ-менеджеров компании, и только осознав все эти аспекты, принимать решение. Иногда бывает важно понять, какова значимость технологии для общества в целом (пусть и в некоторой перспективе), какой социальный эффект она может дать. Думаю, что это разнообразие практического опыта, который не почерпнешь ни в одном учебнике, дорогого стоит.

Давайте перейдем к вашей нынешней деятельности...

Очевидно, что сегодня в банковской отрасли информационные технологии являются одним из основных драйверов развития и непременным условием для ведения бизнеса. Но они же порождают самые серьезные вызовы для будущего банковского сектора.

Например, если посмотреть на туристическую отрасль, то мы увидим, что за последние несколько лет в этой сфере произошли радикальные изменения, которые ударили по бизнесу туристических агентств. Для туризма ИТ всегда являлись мощным инструментом (системы бронирования, промо-сай-

ты и пр.), но в данном случае тенденции, работающие против традиционной модели бизнеса, оказались явно сильнее. Привычный механизм профессионального посредничества, реализуемого турагентством между путешественником, перевозчиком и отелем, был нарушен именно информационными технологиями. Сейчас мы можем наблюдать также и за болезненной, но неизбежной трансформацией отрасли городских такси.

И банковскую отрасль может ждать что-то подобное?

У нас ситуация несколько иная и не столь драматичная. Сегодня банкинг фактически представляет собой совокупность сервисов, многие из которых могут быть легко обособлены. Многим из них (не в последнюю очередь благодаря развитию все тех же ИТ) могут заниматься отдельные компании, а не банки. Буквально на днях у меня была беседа с руководителями компании Huawei, которые рассказывали мне о взрывном росте популярности в Китае одной из локальных социальных сетей. К ней привязаны сервисы электронного кошелька и процессинга, что позволяет участникам этой сети переводить друг другу деньги без комиссии. Социальная сеть зарабатывает не на переводах и может позволить себе обнулить комиссии, попутно убивая бизнес WesternUnion, MoneyGram и других платежных сетей.

Еще один весьма интересный пример также связан с развивающимися рынками. Тот факт, что качественными банковскими услугами не были охвачены большинство регионов Кении, позволил ведущему мобильному оператору страны запустить сервис денежных переводов и микрофинансирования M-Pesa. Деньги в данном случае хранятся на счете мобильного оператора и напрямую привязаны к номеру мобильного телефона, что для большинства населения страны оказалось очень удобно. Но самое примечательное здесь в другом. Когда коммерческие банки Кении, осознав угрозу, пожаловались в Центральный банк

этой страны, он их не поддержал и не запретил деятельность сотового оператора, по факту ослабляющего розничный бизнес традиционных банков.

Резюме из всего сказанного следующее. Информационные технологии, проникая повсюду, могут эффективно работать не только на благо развития различных индустрий, но и иногда фактически против них, радикально трансформируя, а иногда и разрушая их. В конечном итоге все определяет здоровая конкуренция.

В таком случае, какие идеи наиболее вероятно станут основой для развития банковского сервиса будущего?

Я думаю, в современной парадигме банк фактически становится для клиентов внешним казначеем и провайдером многочисленных дополнительных сервисов. Типичным сценарием становится формирование на базе банковских сервисов канала для доступа к электронным торговым площадкам, электронным магазинам. Также банк может выступать агрегатором финансовых услуг внешних провайдеров сервисов. Если же смотреть более широко, то разнообразие небанковских финансовых сервисов, с одной стороны, создает на рынке конкуренцию, с другой — предоставляет кредитным организациям более широкие возможности на рынке собственно финансовых сервисов.

С точки зрения внутренних банковских процессов все большее число операций осуществляется в полностью автоматическом режиме, что является результатом расширения функциональности ИТ-систем. Это позволяет существенно снижать затраты при одновременном повышении надежности и оперативности проведения транзакций.

Разумеется, это в полной мере относится и к Группе ВТБ. Учитывая все вышеназванные тенденции как на розничном, так и на корпоративном рынке, мы сейчас очень много работаем над развитием портфеля ИТ-проектов и успешно продвигаемся в этом направлении. □

ООО "Урал-Пресс"
г. Екатеринбург — осуществляет подписку крупнейших российских предприятий в более чем 60 своих филиалах и представительствах.
Тел./факс (343) 26-26-543 (многоканальный);
(343) 26-26-135;
e-mail: info@ural-press.ru;
www.ural-press.ru

Представительство в Москве:
Тел. (495) 789-86-36;
факс (495) 789-86-37;
e-mail: moskva@ural-press.ru

ВНИМАНИЕ!
Для оформления бесплатной корпоративной подписки на PC Week/RE можно обращаться в отдел распространения по тел. (495) 974-2260 или E-mail: podpiska@skpress.ru, pretenzii@skpress.ru
Если у Вас возникли проблемы с получением номеров PC Week/RE по корпоративной подписке, пожалуйста, сообщите об этом в редакцию PC Week/RE по адресу: editorial@pcweek.ru или по телефону: (495) 974-2260.
Редакция

PCWEEK RUSSIAN EDITION № 16 (893) **БЕСПЛАТНАЯ ИНФОРМАЦИЯ ОТ ФИРМ!**

ПОЖАЛУЙСТА, ЗАПОЛНИТЕ ПЕЧАТНЫМИ БУКВАМИ:

Ф.И.О. _____

ФИРМА _____

ДОЛЖНОСТЬ _____

АДРЕС _____

ТЕЛЕФОН _____

ФАКС _____

E-MAIL _____

<input type="checkbox"/> 1С	1
<input type="checkbox"/> АКВАРИУС	16
<input type="checkbox"/> ЛАБОРАТОРИЯ КАСПЕРСКОГО	11
<input type="checkbox"/> ASUS	3
<input type="checkbox"/> HUAWEI	5
<input type="checkbox"/> LENOVO	7

ОТМЕТЬТЕ ФИРМЫ, ПО КОТОРЫМ ВЫ ХОТИТЕ ПОЛУЧИТЬ ДОПОЛНИТЕЛЬНУЮ ИНФОРМАЦИЮ, И ВЫШЛИТЕ ЗАПОЛНЕННУЮ КАРТОЧКУ В АДРЕС РЕДАКЦИИ: 109147, РОССИЯ, МОСКВА, УЛ. МАРКСИСТСКАЯ, Д. 34, КОРП. 10, PC WEEK/RUSSIAN EDITION; или по факсу: +7 (495) 974-2260, 974-2263.

PC WEEK RUSSIAN EDITION

КОРПОРАТИВНАЯ ПОДПИСКА

Уважаемые читатели!

Только полностью заполненная анкета, рассчитанная на руководителей, отвечающих за автоматизацию предприятий; специалистов по аппаратному и программному обеспечению, телекоммуникациям, сетевым и информационным технологиям из организаций, имеющих более 10 компьютеров, дает право на бесплатную подписку на газету PC Week/RE в течение года с момента получения анкеты. Вы также можете заполнить анкету на сайте: www.pcweek.ru/subscribe_print/.

Примечание. На домашний адрес еженедельник по бесплатной корпоративной подписке не высылается. Данная форма подписки распространяется только на территорию РФ.

Я хочу, чтобы моя организация получала PC Week/RE !

Название организации: _____

Почтовый адрес организации:

Индекс: _____ Область: _____

Город: _____

Улица: _____ Дом: _____

Фамилия, имя, отчество: _____

Подразделение / отдел: _____

Должность: _____

Телефон: _____ Факс: _____

E-mail: _____ WWW: _____

(Заполните анкету печатными буквами!)

1. К какой отрасли относится Ваше предприятие?

1. Энергетика
2. Связь и телекоммуникации
3. Производство, не связанное с вычислительной техникой (добывающие и перерабатывающие отрасли, машиностроение и т. п.)
4. Финансовый сектор (кроме банков)
5. Банковский сектор
6. Архитектура и строительство
7. Торговля товарами, не связанными с информационными технологиями
8. Транспорт
9. Информационные технологии (см. также вопрос 2)
10. Реклама и маркетинг
11. Научно-исследовательская деятельность (НИИ и вузы)
12. Государственно-административные структуры
13. Военные организации
14. Образование
15. Медицина
16. Издательская деятельность и полиграфия
17. Иное (что именно) _____

2. Если основной профиль Вашего предприятия – информационные технологии, то уточните, пожалуйста, сегмент, в котором предприятие работает:

1. Системная интеграция
2. Дистрибуция
3. Телекоммуникации
4. Производство средств ВТ
5. Продажа компьютеров
6. Ремонт компьютерного оборудования
7. Разработка и продажа ПО
8. Консалтинг
9. Иное (что именно) _____

3. Форма собственности Вашей организации (отметьте только один пункт)

1. Госпредприятие
2. ОАО (открытое акционерное общество)
3. ЗАО (закрытое акционерное общество)
4. Зарубежная фирма
5. СП (совместное предприятие)
6. ТОО (товарищество с ограниченной ответственностью) или ООО (Общество с ограниченной ответственностью)

4. К какой категории относится подразделение, в котором Вы работаете? (отметьте только один пункт)

1. Дирекция
2. Информационно-аналитический отдел
3. Техническая поддержка
4. Служба АСУ/ИТ
5. ВЦ
6. Инженерно-конструкторский отдел (САПР)
7. Отдел рекламы и маркетинга
8. Бухгалтерия/Финансы
9. Производственное подразделение
10. Научно-исследовательское подразделение
11. Учебное подразделение
12. Отдел продаж
13. Отдел закупок/логистики
14. Иное (что именно) _____

5. Ваш должностной статус (отметьте только один пункт)

1. Директор / президент / владелец
2. Зам. директора / вице-президент
3. Руководитель подразделения
4. Сотрудник / менеджер
5. Консультант
6. Иное (что именно) _____

6. Ваш возраст

1. До 20 лет
2. 21–25 лет
3. 26–30 лет
4. 31–35 лет
5. 36–40 лет
6. 41–50 лет
7. 51–60 лет
8. Более 60 лет

7. Численность сотрудников в Вашей организации

1. Меньше 10 человек
2. 10–100 человек
3. 101–500 человек
4. 501–1000 человек
5. 1001–5000 человек
6. Более 5000 человек

8. Численность компьютерного парка Вашей организации

1. 10–20 компьютеров
2. 21–50 компьютеров

3. 51–100 компьютеров
4. 101–500 компьютеров
5. 501–1000 компьютеров
6. 1001–3000 компьютеров
7. 3001–5000 компьютеров
8. Более 5000 компьютеров

9. Какие ОС используются в Вашей организации ?

1. DOS
2. Windows 3.xx
3. Windows 9x/ME
4. Windows NT/2K/XP/2003
5. OS/2
6. Mac OS
7. Linux
8. AIX
9. Solaris/SunOS
10. Free BSD
11. HP/UX
12. Novell NetWare
13. OS/400
14. Другие варианты UNIX
15. Иное (что именно) _____

10. Коммуникационные возможности компьютеров Вашей организации

1. Имеют выход в Интернет по выделенной линии
2. Объединены в intranet
3. Объединены в extranet
4. Подключены к ЛВС
5. Не объединены в сеть
6. Dial Up доступ в Интернет

11. Имеет ли сеть Вашей организации территориально распределенную структуру (охватывает более одного здания)?

Да Нет

12. Собирается ли Ваше предприятие устанавливать интрасети (intranet) в ближайший год ?

Да Нет

13. Сколько серверов в сети Вашей организации ?

14. Если в Вашей организации используются мэйнфреймы, то какие именно?

1. ЕС ЭВМ
2. IBM
3. Unisys
4. VAX
5. Иное (что именно) _____
6. Не используются

15. Компьютеры каких фирм-изготовителей используются на Вашем предприятии?

- | | | | |
|-------------------|--------------------------|--------------------------|--------------------------|
| “Аквариус” | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| ВИСТ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| “Формоза” | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Acer | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Apple | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| CLR | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Compaq | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Dell | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Fujitsu Siemens | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Gateway | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Hewlett-Packard | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| IBM | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Kraftway | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| R.&K. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| R-Style | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Rover Computers | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Sun | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Siemens Nixdorf | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Toshiba | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Иное (что именно) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

16. Какое прикладное ПО используется в Вашей организации?

1. Средства разработки ПО
2. Офисные приложения
3. СУБД
4. Бухгалтерские и складские программы
5. Издательские системы
6. Графические системы
7. Статистические пакеты
8. ПО для управления производственными процессами
9. Программы электронной почты
10. САПР
11. Браузеры Internet
12. Web-серверы
13. Иное (что именно) _____

17. Если в Вашей организации установлено ПО масштаба предприятия, то каких фирм-разработчиков?

1. “1С”
2. “АйТи”
3. “Галактика”
4. “Парус”
5. BAAN
6. Navision
7. Oracle
8. SAP
9. Epicor Scala
10. ПО собственной разработки
11. Иное (что именно) _____

18. Существует ли на Вашем предприятии единая корпоративная информационная система?

Да Нет

19. Если Ваша организация не имеет своего Web-узла, то собирается ли она в ближайший год завести его?

Да Нет

20. Если Вы используете СУБД в своей деятельности, то какие именно?

1. Adabas
2. Cache
3. DB2
4. dBase
5. FoxPro
6. Informix
7. Ingress
8. MS Access
9. MS SQL Server
10. Oracle
11. Progress
12. Sybase
13. Иное (что именно) _____

21. Как Вы оцениваете свое влияние на решение о покупке средств информационных технологий для своей организации? (отметьте только один пункт)

1. Принимаю решение о покупке (подписываю документ)
2. Составляю спецификацию (выбираю средства) и рекомендую приобрести
3. Не участвую в этом процессе
4. Иное (что именно) _____

22. На приобретение каких из перечисленных групп продуктов или услуг Вы оказываете влияние (покупаете, рекомендуете, составляете спецификацию)?

- Системы**
1. Мэйнфреймы
 2. Миникомпьютеры
 3. Серверы
 4. Рабочие станции
 5. ПК
 6. Тонкие клиенты
 7. Ноутбуки
 8. Карманные ПК
 9. Концентраторы
 10. Коммутаторы
 11. Мосты
 12. Шлюзы
 13. Маршрутизаторы
 14. Сетевые адаптеры
 15. Беспроводные сети
 16. Глобальные сети
 17. Локальные сети
 18. Телекоммуникации
- Периферийное оборудование**
19. Лазерные принтеры
 20. Струйные принтеры
 21. Мониторы

22. Сканеры
23. Модемы
24. ИБП (UPS)

- Память**
25. Жесткие диски
 26. CD-ROM
 27. Системы архивирования
 28. RAID
 29. Системы хранения данных

- Программное обеспечение**
30. Электронная почта
 31. Групповое ПО
 32. СУБД
 33. Сетевое ПО
 34. Хранилища данных
 35. Электронная коммерция
 36. ПО для Web-дизайна
 37. ПО для Интернета
 38. Java
 39. Операционные системы
 40. Мультимедийные приложения

41. Средства разработки программ
42. CASE-системы
43. САПР (CAD/CAM)
44. Системы управления проектами
45. ПО для архивирования
46. Внешние сервисы
47. Ничего из вышеперечисленного

23. Каков наивысший уровень, для которого Вы оказываете влияние на покупку компьютерных изделий или услуг (служб)?

1. Более чем для одной компании
2. Для всего предприятия
3. Для подразделения, расположенного в нескольких местах
4. Для нескольких подразделений в одном здании
5. Для одного подразделения
6. Для рабочей группы
7. Только для себя
8. Не влияю
9. Иное (что именно) _____

24. Через каких провайдеров в настоящее время Ваша фирма получает доступ в интернет и другие интернет-услуги?

1. “Демос”
2. МТУ-Интел
3. “Релком”
4. Combellga
5. Comstar
6. Golden Telecom
7. Equant
8. ORC
9. Telmos
10. Zebra Telecom
11. Через других (каких именно) _____

Дата заполнения _____

Отдайте заполненную анкету представителям PC Week/RE либо пришлите ее по адресу: 109147, Москва, ул. Марксистская, д. 34, корп. 10, PC Week/RE.

Анкету можно отправить на e-mail: info@pcweek.ru



Aquarius Server E30 S11

сверхкомпактный сервер
на базе процессоров Intel®

- один процессор серии Intel® Xeon®
- до 16GB оперативной памяти
- до 4 дисков с горячей заменой
- блокировка передней панели
- размеры 230 x 210 x 275 мм, низкий уровень шума
- возможна установка в обычном помещении
- повышенная безопасность с технологиями Intel



ИДЕАЛЕН ДЛЯ:

- ГОСУСЛУГ
- МЕДИЦИНЫ
- КОММЕРЦИИ
- ОБРАЗОВАНИЯ
- БЕЗОПАСНОСТИ

Компания «Аквариус»:

142784, Россия, г. Москва, Румянцево,
Киевское ш. 6, стр.1, БЦ «Комсити», тел.: (495) 729-5150
question@aq.ru | www.aq.ru

Наши дистрибьюторы:

OCS: www.ocs.ru | Landata: www.landata.ru
Широкая сеть авторизованных бизнес-партнеров.

