

PC WEEK



18+

№ 8-9 (907-908) • 31 МАЯ • 2016 • МОСКВА

<http://www.pcweek.ru>

1C **ERP**

УАЗ оптимизировал управление производством с помощью «1C:ERP»

- сократил межоперационные запасы материалов на 40,5%
- высвободил 32% оборотных средств из запасов ТМЦ
- оптимизировал использование ресурсов на 20%

Open Source и цифровой суверенитет России

НИКОЛАЙ НОСОВ

Что такое “цифровой суверенитет”? Можно ли его добиться в современном мире? Как он связан с импортозамещением? Поможет ли в этом Open Source? Каковы плюсы и минусы использования этой модели для обеспечения цифрового суверенитета? Эти и многие другие вопросы обсуждались на прошедшем 23 мая форуме “ИТ+Суверенитет”, организованном Институтом развития Интернета (ИРИ).

Что такое цифровой суверенитет

В последнее время уделяется повышенное внимание вопросам обеспечения ИТ-суверенитета России.

“Современная ситуация такова, что цифровой суверенитет внезапно стал таким же важным, как традиционный, “офлайнный” суверенитет, предполагающий государственные границы, деньги, власть”, — отметил советник президента РФ, председатель совета ИРИ Герман Клименко. Он сказал, что появились достаточно серьезные проблемы, например трансграничная интернет-торговля, торговля программным обеспечением, торговля без регистрации юридического лица, которые не так легко



Герман Клименко

решить в рамках классического римского права. “Тема цифрового суверенитета становится крайне важной, от него зависит процветание нашей экономики. Здесь много вопросов и больших вызовов, которые одни и те же и у нас, и у наших зарубежных коллег, с которыми мы конкурируем и которые активно нас прессингуют”, — добавил г-н Клименко.

Председатель комитета Госдумы по информполитике, информтехнологиям и связи, член совета ИРИ Леонид Левин объяснил, что “ИТ-суверенитет — это в первую очередь независимость наших сервисов и нашей ИТ-инфраструктуры от внешних влияний и воздействий. И мы должны работать не только в направлении развития отечественных сервисов и программного обеспечения, но и думать о защите наших интернет-границ и их суверенности при сохранении основного принципа трансграничности Интернета”.

Суверенитет и импортозамещение

ИТ-суверенитет более широкое понятие, чем импортозамещение. Оно включает в себя обеспечение кибербезопасности страны, возможность защиты своих критически

ПРОДОЛЖЕНИЕ НА С. 6 ►

Чипмейкеры намерены объединить процессоры и ускорители

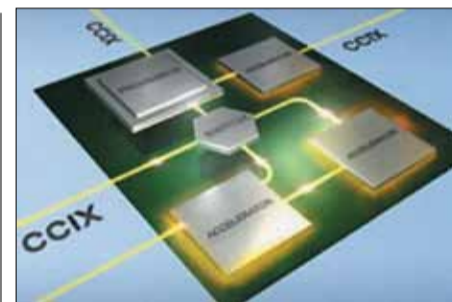
ДЖЕФФРИ БЕРТ

Компании IBM, ARM и AMD в числе прочих ИТ-вендоров собираются создать единую взаимосвязанную матрицу для дата-центров, которая позволит микропроцессорам и графическим ускорителям различных производителей обмениваться данными, не требуя для этого сложного программирования.

Если верить официальным представителям компаний — участниц проекта, новая шина с когерентным кэшем для ускорителей (Cache Coherent Interconnect for Accelerators, CCIX) повысит эффективность работы серверов и сделает их более пригодными к выполнению таких перспективных для дата-центров рабочих заданий, как аналитика больших данных, машинное обучение, беспроводные сети 4G и 5G, аналитика видеоданных и виртуализация сетевых функций (NFV).

В проекте также участвуют такие вендоры, как Huawei Technologies, Mellanox Technologies, Qualcomm и производители программируемых вентильных матриц (FPGA) компания Xilinx, заявившая, что в новый план развития ее 16-нанометровых FPGA-чипов UltraScale+ будут входить модели с интегрированной высокоскоростной памятью (High-Bandwidth Memory, HBM) и поддержкой CCIX.

Матрица CCIX позволит различным микросхемам, графическим ускорителям и сетевым микрочипам — от про-



цессоров и графических микросхем до FPGA-матриц — обеспечить беспрепятственный обмен данными между системами, построенными на базе этих компонентов. Новые виды рабочих нагрузок требуют все более быстрой и эффективной обработки данных, поэтому производители систем подключают к ЦПУ (как к чипам x86 производства Intel и AMD, так и к микропроцессорам POWER от IBM и однокристальным системам на базе архитектуры ARM) дополнительные вычислительные мощности в виде FPGA-матриц, графических процессоров (GPU) и цифровых сигнальных процессоров (DSP), чтобы быстрее, эффективнее и дешевле решать различные задачи.

Спецификация на единую взаимосвязанную сеть, позволяющую обмениваться данными процессорам с несовместимой функциональной архитектурой, должна ускорить реализацию этих возможностей.

ПРОДОЛЖЕНИЕ НА С. 6 ►

В НОМЕРЕ:

Зачем переходить на ЭДО 10

Кибербезопасность железных дорог 8

ИТ в финансовом секторе 14



О перспективах ИИТ в энергетике 16

Интернет вещей — уже мейнстрим? 17

Schneider Electric: будущее за гибридной облачной средой с граничными серверами

ИГОРЬ НОВИКОВ

Компания Schneider Electric провела в Париже встречу руководителей промышленных компаний Innovation Summit 2016. Главными темами для обсуждений стали тренды в развитии технологий в области энергопотребления, автоматизации и ИТ.

Председатель правления Schneider Electric Жан-Паскаль Трикуар отметил, что компания видит свою главную цель в развитии технологий, предоставляя каждому клиенту возможность добиваться наилучших результатов в своем бизнесе. По его мнению, важность применения новых технологий будет нарастать, а ценность от внедрения инноваций, в частности в электрообеспечении, будет становиться еще более существенной.

По оценкам аналитиков Международного энергетического агентства (IEA), объем потребления электричества в промышленности будет расти как минимум до 2040 г. Темпы этого роста будут вдвое превышать темпы роста потребления других видов энергии. Главным двигателем для роста потребления электроэнергии он видит стремительное наращивание количества применяемых цифровых устройств, кото-



Жан-Паскаль Трикуар

рое значительно увеличится с приходом Интернета вещей.

По данным Cisco, к 2020 г. на каждого сотрудника будет приходиться более 20 подключаемых устройств, при этом, по данным Bloomberg, к 2040 г. до 70% вводимых в эксплуатацию электрических мощностей будет приходиться на возобновляемые источники энергии.

Главными причинами будущего роста потребностей в энергообеспечении г-н Трикуар называет:

- рост численности населения (к 2050 г. число городских жителей в мире увеличится на 2,5 млрд. человек);

- рост числа сетевых устройств и устройств Интернета вещей (в течение ближайших пяти лет их количество увеличится на 50 млрд. шт.);
- рост энергопотребления в промышленности в целом (по прогнозам, оно вырастет в ближайшие 35 лет как минимум на 50%).

Вопросы использования электроэнергии в промышленности рассматривались на саммите под разным углом зрения: на глобальном уровне, в промышленности, жилищном строительстве и т. д. Большой интерес вызвала тема развития электрообеспечения в корпоративных и облачных ЦОДах. Этой теме был посвящен специальный круглый стол “Data Center: In the Cloud and at the Edge”.

ЦОДы будущего: в облаке и на сетевой периферии

Ведущий круглого стола Кевин Браун, вице-президент Schneider Electric по технологиям и ЦОДам, предложил обсудить основные тренды развития ИТ-инфраструктур, коснувшись таких направлений, как Интернет вещей, конвергенция технологий и возрастающее внимание со стороны государственных регуляторов к применению

ПРОДОЛЖЕНИЕ НА С. 3 ►



от 79 990 руб.

ASUS ZenBook™ UX305CA Мощный. Легкий. Стильный.

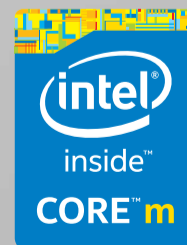


- Новейший процессор Intel® Core™ m7-6Y75
- Операционная система Windows 10 Домашняя
- Ошеломляющий 13,3" IPS-дисплей с разрешением QHD+ (3200x1800)* или Full HD (1920x1080) и матовым покрытием
- Абсолютно бесшумный благодаря пассивной системе охлаждения

Улучшить классический дизайн ультрабуков Zenbook было непросто, однако мы смогли это сделать. Новая модель Zenbook UX305 выполнена в изумительном по красоте корпусе толщиной 12,3 мм и весом всего 1,2 кг. В ее аппаратную конфигурацию входит невероятно четкий 13,3-дюймовый дисплей формата QHD+, мощный процессор Intel® Core™ M шестого поколения и высокоскоростной твердотельный накопитель емкостью до 512 Гб. Это тот же Zenbook, что и раньше, только лучше!

Intel Inside[®], значит потрясающие возможности.

* 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:

V [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)

Новая жизнь ИТ-инфраструктуры

ЕЛЕНА ГОРЕТКИНА

Сейчас рынок инфраструктуры переживает период эволюционных изменений, считает Мартин Касасо — один из авторов научной статьи, положившей в 2005-м начало эре программно-определяемых сетей (Software Defined Networks, SDN).

“В области традиционной инфраструктуры происходят сдвиги, и мы находимся на пороге нового этапа — золотого века инфраструктуры, — заявил он на конференции Interop, проходившей недавно в Лас-Вегасе. — Сейчас многие говорят, что инфраструктура умирает, но я уверен, что, напротив, она просто возрождается в новом виде”.

По его мнению, благодаря SDN молодым компаниям сейчас легче выйти на рынок с новыми идеями и продуктами, чем когда-либо в истории ИТ. Причина заключается в совпадении трех ключевых факторов: переход от “железа” к софту, появление сервиса “ПО как услуга” и рост влияния разработчиков.

SDN-стартап может построить новаторские продукты и наладить их выпуск быстрее и с меньшими затратами, чем поставщик оборудования. В перспективе такой стартап может превратиться

в серьезного игрока на рынке. Этот тезис подтверждает собственный опыт Касасо. В 2007-м он стал сооснователем компании Nicira, которую в 2012-м купила VMware за более чем миллиард долларов. Сейчас Касасо является генеральным партнером венчурного фонда Andreessen Horowitz.

Для него термин SDN относится к функционалу, который реализован чисто программными средствами без какого-либо специализированного “железа”. Он уверен, что благодаря распространению единой аппаратной платформы, такой как x86, а также мобильных ОС iOS и Android, появляется стандартный интерфейс для реализации программно-определяемой инфраструктуры.

Заглядывая дальше в будущее, Касасо отметил важную роль перехода от ПО к сервисам, который подстегивает развитие публичных облаков и сервисов “ПО как услуга”. За счет такого сервисного подхода компании могут обойти проблемы, связанные с развертыванием инфраструктуры и управлением ею.



Мартин Касасо

Он уверен, что использование сервисов становится трендом и в области инфраструктуры: “Заказчики все активнее покупают продукты в виде услуг”. В качестве примера он привел компанию Andreessen Horowitz, которая продвигает ИТ-продукты как в виде услуг, так и в традиционном виде для установки у заказчика, получая от них примерно одинаковый доход.

Что касается влияния разработчиков, то благодаря программно-определяемым технологиям у них появляется больше возможностей влиять на процесс приобретения ИТ в своих компаниях даже несмотря на то, что они не распоряжаются финансами. “Этот сдвиг оказывает влияние на традиционные каналы продвижения продуктов, так как разработчиков больше интересуют не отчеты аналитиков и коммерческие связи между поставщиками, а чисто технические вопросы”, — сказал Касасо.

По его мнению, разработчики ищут поддержки у других разработчиков, стараясь организовать активные сообщества, и считают, что наилучшая модель — это Open Source, которая избавляет от многих

проблем при адаптации ПО. “Я уверен, что хороший Open Source-проект обеспечит больше успеха на рынке, чем любой маркетинговый бюджет”, — считает Касасо.

Его оптимизм в отношении программно-определяемых сетей разделяет IDC, по прогнозу которой рынок SDN будет ежегодно расти в среднем на 53,9% и к 2020-му достигнет 12,5 млрд. долл. Правда, IDC включает в понятие SDN не только ПО и сервисы, но и физическую сетевую инфраструктуру, на которую приходится и будет приходится основная часть рынка SDN.

Однако быстрее растет программный сегмент, включающий средства виртуализации и управления, а также SDN-приложения (для обеспечения безопасности и реализации сетевого функционала). По прогнозу, он будет ежегодно расти на 64—66% и к 2020-му достигнет 5,9 млрд. долл.

Как отмечают аналитики, благодаря SDN в области сетевой инфраструктуры происходит постепенный переход от “железа” к софту. Для вендоров это подразумевает сдвиг в сторону бизнес-модели, основанной на ПО и услугах. Для предприятий это подразумевает усиление внимания к сотрудничеству в области ИТ и понимания того, как сети обеспечивают доставку приложений и тем самым влияют на бизнес.

Schneider Electric...

▶ ПРОДОЛЖЕНИЕ СО С. 1

и хранению в ЦОДах данных и их безопасности.

Понимание этих трендов, по мнению г-на Брауна, может быть полезно разработчикам для эволюции их подходов при строительстве ЦОДов и выборе новых продуктов в проектах по выстраиванию гибридных облачных конфигураций.

Как отметили участники дискуссии, в условиях нарастающего проникновения в промышленность цифровых технологий наблюдается миграция корпоративных приложений из корпоративных ЦОДов в публичные и частные облака. Рост объема передаваемого контента ведет к повышению объема трафика. В результате многие участники рынка начинают сталкиваться с проблемами при доставке контента по сетям.

Чтобы возможности возводимых сетей соответствовали предъявляемым требованиям, необходимо обеспечить централизацию вычислительных мощностей в основном облаке, размещаемом в крупном ЦОДе, и параллельно осуществлять децентрализацию систем хранения и потребительских служб, размещая их на периферийных сетевых облачных узлах как можно ближе к потребителям. Именно такую облачную модель с граничными облачными серверами (Edge Computing) компания Schneider Electric назвала как наиболее оптимальную с точки зрения решаемых пользовательских задач и предъявляемых требований по обеспечению эффективной эксплуатации.

В этих условиях стратегия развития Schneider Electric, как отметил Кевин Браун, направлена на повышение эффективности энергопотребления на предприятиях путем конвергенции применяемых технологических операций и ИТ, а также модернизации электрических сетей по концепции Smart Grid.

По мнению Энди Лоуренса, вице-президента аналитической компании 451 Group, ускоренное развитие облачных технологий и развитие Интернета вещей окажут существенное влияние на развитие кор-

поративных систем энергопотребления. “Речь не идет о каком-то маркетинговом мифе, — подчеркнул он. — За этим стоит реальный набор технологий, которые будут стремительно развиваться в ближайшие 5—10 лет”.

С ним согласен другой участник круглого стола Прит Банержи, руководитель технологического подразделения Schneider Electric. “В течение прошедших 20 лет влияние ИТ было более заметно прежде

100 мс считалась типовой, хотя при строительстве ЦОДов разработчики стремились обеспечить более высокий уровень, когда задержки не превышают 25 мс.

Как отметил Кевин Браун, сегодня многое меняется. Приобретая оборудование для ЦОДов, компании ориентируются на топовые характеристики, указываемые вендором в спецификации. Однако реальные скорости, получаемые после строительства сети, оказываются заметно ниже заявленных.

С появлением слишком больших задержек возникают заторы трафика, что не позволяет использовать на полную мощность доступную производительность сетевых устройств. В условиях, когда объемы передаваемого контента нарастают, а также меняется соотношение между типами передаваемых данных, важность величины задержек становится критической.

Для улучшения характеристик сетей при передаче контента, особенно потоковых данных, сервис-провайдеры внедряют системы кэширования, размещая данные на промежуточных серверах и стараясь максимально приблизить их к получателю. Предлагаемая Schneider Electric оптимизация таких сетей — вышеупомянутая гибридная облачная модель с граничными серверами Edge Computing.

“При строительстве ЦОДов мы внимательно наблюдаем за запросами потребителей, — рассказал Бернанд Оурганьян, руководитель департамента технологий и безопасности Microsoft France. — Мы видим стремление наших пользователей работать в высокопроизводительной ИТ-среде с задержками не более 1 мс. Именно такие условия мы считаем идеальными сегодня для заказчиков”.

Говоря о будущем ЦОДов, он подчеркнул, что крупные заказчики не останавливаются на использовании только публичных облаков: “Они будут строить собственные облачные ЦОДы, объединяя их с другими и обеспечивая тем самым гибкие условия для потребителей”.

Пример практической реализации такой модели показал Кнут Молауг, руководитель компании Green Mountain: “У нас сей-

час работает два облачных ЦОДа. Мы измеряем в них все, что только возможно. У нас есть около 2000 точек контроля. Это позволяет эффективно управлять трафиком, энергопотреблением и другими параметрами работы ЦОДа”.

“При строительстве ЦОДов, — дополнил Даниэль Доймо, вице-президент Schneider Electric, руководитель подразделения Global Solution Business, — во главу угла мы ставим требования согласованности, защищенности и гибкости при использовании оборудования. Это позволяет обеспечить заданные требования по задержкам. Schneider Electric постоянно совершенствует свою методику проектирования ЦОДов, активно используя модульный принцип и гибкость при выборе компонентов”.

Конвергенция ИТ и технологических процессов

Участники круглого стола затронули также тему конвергенции ИТ и технологических процессов при строительстве ЦОДов. Для этих задач Schneider Electric применяет собственный подход, направленный на создание интеллектуальных систем управления энергией. Предложенная компанией “умная” системная архитектура EcoStruxure позволяет автоматически измерять, отслеживать и управлять расходом энергии в ЦОДе, обеспечивать требования, предъявляемые к расходу энергии.

Как было отмечено, EcoStruxure позволяет визуализировать движение энергии в ЦОДах, вести учет и управление ею. Благодаря высокой масштабируемости EcoStruxure можно применять при строительстве не только новых ЦОДов, но также и при модернизации существующих.

Отвечая на вопрос, какое будущее ожидает ЦОДы, Хал Грант, вице-президент Schneider Electric, руководитель департамента IT Business, заявил: “Это будут многочисленные центры обработки небольшого размера, где будут активно использоваться Edge- и IoT-приложения, collocation. В них будут размещаться приложения и сервисы, работающие с другими облаками и корпоративными ЦОДами. Придерживаясь такой модели будущего, Schneider Electric внимательно изучает потребности заказчиков, опираясь на принципы Agile-разработки. Цель компании — предложить решения, наиболее подходящие нашим заказчикам”.



Участники круглого стола

всего на потребительском рынке, — заявил он. — Многие стали пользоваться смартфонами, планшетами. Сейчас около 2 млрд. человек общаются между собой с помощью этих устройств. Однако активное проникновение Интернета вещей приведет к тому, что ИТ начнут смещаться сильнее в сторону корпоративного сегмента. Распространение облачных вычислений и развитие экосистемы ЦОДов будет положительно сказываться на развитии этого тренда. Для проникновения IoT потребуются создать множество новых программ, которые будут предоставлять данные для различных информационных систем. Развитие IoT будет способствовать дальнейшему росту эффективности использования облаков и ЦОДов”, — считает Прит Банержи.

Высокопроизводительная передача трафика стала насущной необходимостью

Важным показателем качества работы современных ЦОДов являются задержки, возникающие при передаче данных. Этот параметр отражает время, затрачиваемое на передачу пакетов в направлении получателя и на обратный путь. До недавнего времени задержка на уровне менее

СОДЕРЖАНИЕ

№ 8-9 (907-908) • 31 МАЯ, 2016 • Страница 4

НОВОСТИ

- 1 **Что такое “цифровой суверенитет”** и можно ли его добиться
- 1 **ИТ-вендоры намерены** сообща создать единую матрицу, которая обеспечит обмен данными между разнородными CPU, GPU, FPGA
- 1 **Schneider Electric: ЦОДы будущего** — в облаке и на сетевой периферии

- 3 **Использование сервисов** становится трендом в области инфраструктуры.
- 19 **Блокчейн-стартапы** получают в России поддержку

ЭКСПЕРТИЗА

- 7 **Эффективный ЦОД** для СМБ: от “локутного” строительства к комплексному подходу

УПОМИНАНИЕ ФИРМ В НОМЕРЕ

ГК ХОСТ	AMD	IBM	Qualcomm
Инфосистемы Джет	ARM	IBS	SAP
Компьюлинк	Asus	Intel	Schneider Electric
Терн	Axoft	Mellanox Technologies	Tibco Software
Техносерв Консалтинг	Huawei	Nvidia	Xilinx

- 8 **Борис Макаров:** “Оказалось, что во многих случаях использование импортного оборудования ничем не оправдано”
- 10 **Сергей Тарасов:** “Главные эффекты от внедрения ЭДО заключаются в ускорении бизнес-процессов и повышении их надежности”
- 11 **Алексей Катрич:** “Классическая роль банка по созданию и предоставлению клиентам финансовых продуктов меняется”
- 12 **ИБП APC Back-UPS BX650LI-GR** обеспечит надежное питание нескольких устройств и обойдется недорого
- 12 **ASUS Zenfone MAX** — смартфон для тех, кто увеличению производительности предпочитает продление времени автономной работы

- 13 **Екатерина Лозовая:** “Предприятиям оказались нужны не только средства генерации отчетов, но также возможности выявления скрытых закономерностей и построения прогнозов”
- 14 **Каковы приоритеты** банков в области информатизации и что может предложить им ИТ-индустрия

ТРЕНДЫ И ПЕРСПЕКТИВЫ

- 16 **Евгений Грабчак:** “Концепции Индустриального Интернета у нас пока нет, и в этом заключается основная проблема”
- 18 **Андрей Биветски:** “Мы считаем, что Интернет вещей — это самое перспективное направление в горизонте следующих трех-пяти лет”

БЛОГОСФЕРА PCWEEK.RU

Права граждан vs обязанности государства: приключения WhatsApp в Бразилии

Андрей Колесов,

pcweek.ru/security/blog

Как разрешить противоречие между правом граждан на тайну переписки и обязанностями государства по обеспечению безопасности и правопорядка, для чего соответствующим его органам нужно иметь доступ к частной корреспонденции людей, подозреваемых в преступлениях (разумеется, с соблюдением действующего законодательства). В старые времена все было просто: почтовая служба была в руках государства, а люди переписывались, как правило, без использования секретных шифров.

Сегодня ситуация совсем иная: массовые коммуникационные функции ушли из рук государства, а операторы связи стали все шире использовать шифрование. Причем такое (шифрование end-to-end), что даже сами не знают, о чем переписываются их клиенты. Как же “те, кому надо” смогут прочитать письма “тех, кому надо”?

Общепринятого на мировом уровне ответа на этот вопрос пока нет, но похоже, что всеобщее право на тайну переписки оценивается обществом все же выше, чем борьба с отдельными преступниками. В феврале — марте мы наблюдали за конфликтом “Apple против ФБР” (возможно, история на юридическом уровне еще не закончилась, но пока видно, что победила точка зрения Apple — тайна переписки важнее), а недавно аналогичная история случилась в Бразилии.

Утром 2 мая СМИ сообщили, что по решению окружного суда из бразильского штата Сержипи операторы сотовой связи должны заблокировать на 72 ч мессенджер WhatsApp за то, что компания-владелец (Facebook) в очередной раз отказалась раскрыть личные данные пользователей, которых подозревают в преступлениях, в том числе связанных с оборотом наркотиков.

Но уже через несколько часов более высокая судебная инстанция Бразилии отменила данное распоряжение, объяснив это тем, что права десятков миллионов людей на свободу обмена информацией (число пользователей WhatsApp в Бразилии — 100 млн., это 90% населения страны) важнее борьбы с десятком подозреваемых в преступлениях.

В этой истории самое интересное — точное повторение ситуации декабря прошлого года. Тогда по аналогичной причине суд заблокировал мессенджер на 48 ч, но уже через 12 ч отменил свое решение. Еще один любопытный момент в этой истории: в обоих случаях речь шла не о запрете WhatsApp, а в нанесении финансового ущерба: сервис отключался на некоторое время. В результате наблюдался массовый приток новых пользователей у сервисов-конкурентов. Так, сообщалось, что 17 декабря 2015 г.

число пользователей Telegram увеличилось сразу на 4 млн. человек.

Есть и еще один вопрос: почему подобные конфликты возникают именно у “больших сервисов” типа WhatsApp? Потому, что преступники пользуются ими, или потому, что другие сервисы легче идут на сотрудничество с “теми, кому нужно”?

СПО для бизнеса или бизнес для СПО

Сергей Голубев,

pcweek.ru/foss/blog

К статье “Свободное ПО открывает новые горизонты для бизнеса”, опубликованной ещё в начале месяца, оставлен лишь один содержательный комментарий, но материал заслуживает более широкого обсуждения.

Во-первых, непонятна роль государства, о чём справедливо замечает Валерий Белошапкин (автор того самого единственного комментария). Ведь “генеральная линия” была в принципе правильной. Сначала — внедрение СПО в школы, а уже потом — НацОС, НПП, 2299-р и пр. План вполне разумный и реалистичный, а вот его реализация — не очень.

На мой взгляд, главная проблема заключалась в том, что фактически сорванный школьный проект в дальнейшем почему-то стали считать успешным. И начали строить здание на фундаменте, существующем только в отчетах и прочих бумагах.

Ведь совершенно очевидно, что “новый подход”, согласно которому центр передатчика региона инициативу по переходу на СПО, будет работать только в одном случае — при наличии в регионах крупных центров компетентности. А эти центры, в свою очередь, должны были быть созданы в ходе реализации школьного проекта.

Нестыковка налицо, но разобраться почему-то никто не хочет. Знаменитое русское “проехали” и тут сыграло свою роль.

Во-вторых, роль бизнеса непонятна ещё больше. Я понимаю, что не стоит судить о положении дел в отрасли исключительно по публикациям в СМИ. Тем не менее если сравнить “их” прессу с “нашей”, то в глаза бросается одно различие.

“Там” значительная часть материалов информирует читателей о том, что бизнес делает для СПО. У нас — что СПО может сделать для бизнеса. Разница в подходах очевидна и показательна.

В статье приводятся слова Дмитрия Варёнова: “В России уже выросло не одно поколение, не видевшее ничего, кроме проприетарных продуктов. Во многом виной тому отсутствовавшая долгие годы эффективная борьба с пиратством: люди просто привыкли брать всё даром. В результате мы получили пользователей, знакомых лишь с определёнными продуктами, а всё новое у них сразу приобретает статус неудобного, неправильного, слишком сложного”.

По-моему, дальше должен следовать

рассказ о создании силами бизнеса образовательного проекта типа Picademy. Ничего подобного — проблема названа, а её решением пусть занимается кто-то другой. А вот кто этот самый “кто-то другой”, совершенно непонятно.

Может быть, пора уже бизнесу сменить концепцию “что СПО может сделать для меня” на “что я могу сделать для СПО”?

“За Linux пока никто не платит...”

Сергей Голубев,

pcweek.ru/foss/blog

Года четыре назад я начал эксперимент, который завершился буквально за несколько дней до майских праздников. Эксперимент заключался в том, что на одном небольшом предприятии я установил Ubuntu на компьютер одного сотрудника, которому был не нужен “1С”. Он использовал только браузер, поэтому никаких проблем не ожидалось.

Несколько лет Ubuntu работала без каких-либо нареканий. По крайней мере, мне тот сотрудник не жаловался. Однако в начале апреля его компания заключила договор с какой-то небольшой компьютерной фирмой, которая взялась обслуживать их машинный парк. И моментально одним даже таким условным корпоративным пользователем Ubuntu стало меньше.

Городок у нас относительно небольшой и найти того самого специалиста никакого труда не составило. И вот что я узнал.

Оказывается, специалист прекрасно знает Linux. По крайней мере, на его личном ноутбуке стоит не абы что, а Gentoo. Поддерживать Ubuntu он мог бы запросто. Но не захотел. О причинах этого он рассказал следующее: “Ты как Ubuntu устанавливал? Наверняка, час уваривал и денег не взял. Только поэтому они и согласились. Теперь ты хочешь, чтобы я предложил им то же самое, но не даром? Нереально это. Стараниями сообщества у мелкого заказчика уже сложилось твёрдое убеждение, что если кто-то установит ему Linux, то ему платить не нужно. Более того, он ещё сам тебе должен будет. Мы при всём уважении к Open Source не популяризацией занимаемся, а деньги зарабатываем. А за Linux пока никто не платит”.

И хочется возразить, да нечего. Хотя налицо явно парадоксальная ситуация — системный интегратор местечкового уровня сам использует одно, а своим клиентам предлагает другое. По-моему, в этом есть что-то глобально неправильное и противоречащее обычной житейской логике.

Windows Phone: неожиданное возвращение

Сергей Стельмах,

pcweek.ru/mobile/blog

Думаете, ещё месяц-другой и на мобильном рынке останутся только iOS и Android? Нет, Windows Phone, несмотря на то что Microsoft взяла паузу для переосмысления

своего мобильного бизнеса, продолжает оставаться на плаву и даже растёт!

Если верить статистике Net Applications, за минувший месяц доля Windows Phone выросла с 2,54 до 4,03%, что является для неё рекордным значением. Обычно она составляет около 3%, так что рост сразу на 1,5% — необычное явление для этой ОС. Чем такой рост обусловлен, непонятно, но определённо положительную роль сыграла информация о том, что Microsoft не уходит с рынка смартфонов. Это могло вызвать всплеск продаж, и возможно — не кратковременный.

Стоит также отметить, что в сегменте WP впервые сменился лидер. По данным AdDuplex, им стал смартфон Lumia 535, на который в глобальном масштабе приходится доля в 12,5%, тогда как прежний фаворит (Lumia 520) спустился на ступеньку ниже и занимает теперь второе место с долей 11,3%.

Что касается производителей WP-смартфонов, то здесь наблюдается абсолютное доминирование Microsoft.

Учитывая спад продаж iPhone, не вызывает удивления ослабление позиций iOS: за апрель ее рыночная доля сократилась с 31,76 до 28,42%. Android остаётся явным лидером, показав рост с 61,92 до 69,99%.

Остается добавить, что в этом году к основной тройке мобильных ОС должны добавиться такие конкуренты, как Ubuntu Touch и Tizen. Кажется, самое время их сторонникам проявить активность.

Открытые стандарты для беспроводных сетей помогут сократить расходы на Интернет вещей

Андрей Колесов,

pcweek.ru/iot/blog

Такой основной вывод сделали специалисты компании Machina Research по результатам выполненного ими исследования.

Они утверждают, что использование открытых стандартов для беспроводных сетей, таких как Bluetooth Low Energy и OneM2M, позволит сократить на 30% расходы на внедрение IoT-технологий и на 27% ускорить сам процесс их внедрения.

По оценкам экспертов, для автоматизации процесса управления своим коммунальным хозяйством (в том числе, например, для управления водоснабжением) города всего мира потратят до 2025 г. 1,12 трлн. долл. только на создание системы беспроводных коммуникаций. Но это в случае, если они будут ориентироваться на сегодняшние технологии, которые сейчас в основном являются проприетарными. Но если города будут применять открытые стандарты и технологии, то эта сумма может сократиться на 341 млрд. долл. — до 781 млрд. долл.

Интересно, как сама Machina Research оценит свои сегодняшние прогнозы через 10 лет...

Представляем новый сверхнадёжный 32-процессорный x86 сервер Huawei KunLun

Фундамент ИТ-системы для построения критически важных бизнес-приложений

Новый сервер Huawei KunLun – это основа для непрерывных бизнес-процессов. Инновационная межпроцессорная архитектура и технологии RAS 2.0 обеспечивают надёжность, необходимую для построения критически важных бизнес-приложений.

Leading New ICT

Building a Better Connected World*



Подробнее на
e.huawei.com/ru



* Создавая новые ИКТ, строя мир общения.

Реклама. 18+



Сервер Huawei KunLun на базе процессора Intel® Xeon®

Ultrabook, Celeron, Celeron Inside, Core Inside, логотип Intel, Intel Logo, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, логотип Intel Inside, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, vPro Inside, Xeon, Xeon Phi и Xeon Inside являются товарными знаками, права на которые принадлежат корпорации Intel на территории США и других стран.

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



Эффективный ЦОД для малых и средних предприятий

Важность ИТ как неотъемлемого инструмента ведения бизнеса и повышения его эффективности уже давно никто не оспаривает, и малые и средние предприятия не исключение. Не случайно во многих из них сегодня можно увидеть свой дата-центр — это могут быть всего несколько опутанных проводами стоек с компьютерным оборудованием, но без них нормальное функционирование предприятия уже невозможно. Более того, уже очевидно, что по крайней мере в обозримой перспективе многие предприятия, несмотря на все более широкое распространение облачных технологий и сервисов, предпочитают сохранить собственные ИТ-мощности. По разным причинам. Одни просто не захотят отдавать свои конфиденциальные данные во внешнее облако, другие заинтересованы в повышении своей капитализации (а собственный ЦОД этому способствует), третьим важно сохранить за собой свободу внесения изменений, четвертые делают ставку на гибридную ИТ-архитектуру...

Так или иначе, в связи с ростом потребностей в увеличении вычислительных ресурсов немало таких компаний уже сталкиваются или в ближайшее время могут столкнуться с необходимостью обновления (или создания нового) своего дата-центра, и не всегда прежний опыт в этом случае окажется полезным. Всего за несколько последних лет изменилось многое — обострилась конкуренция на рынке, нужно быстрее реагировать на запросы клиентов, в кратчайшие сроки формировать новые предложения. И, как следствие, выросли требования со стороны бизнеса к ИТ-инфраструктуре — ее надежности, возможности масштабирования, энергоэффективности. Вряд ли кого-либо сегодня устроит объяснения администратора, что ИТ-система временно недоступна из-за перегрева оборудования в стойке.

Изменились и средства для построения малых и средних центров обработки данных. Сегодня вендоры готовы предложить для них современные комплексные программные и аппаратные решения, которые обеспечат надежное электроснабжение и охлаждение компьютерного оборудования, а также возможность для его наращивания.

От "лоскутного"

строительства дата-центров к комплексному Типичная причина проблем небольших дата-центров — несогласованная работа отдельных компонентов, вызванная исторически сложившимся "лоскутным" подходом к проектированию, когда отдельные подсистемы от разных производителей пытаются скомпоновать в общее решение. При этом заказчик, исходя из своих индивидуальных требований и возможностей, выбирает то или иное оборудование по его характеристикам, которые могут быть вполне современными, но не учитывает особенности взаимодействия отдельных подсистем, что в итоге не позволяет в полной мере реализовать потенциал приобретенного оборудования.

Как упростить задачу и обеспечить оптимальный результат? Лучше всего воспользоваться передовым опытом тех, кто давно специализируется в данной сфере. Компания Schneider Electric, например, создала веб-портал проектирования инженерной инфраструктуры Design Portal. С его помощью можно достаточно просто разработать как большой ЦОД, так и инженерную инфраструктуру небольших и средних серверных помещений, получив спецификацию, гарантирующую, что все включенное в нее оборудование будет функционировать именно так, как заявляет производитель. Фактически

производитель берет на себя комплексное решение всей задачи, а заказчик получает единую точку ответственности за весь дата-центр. В результате у него не возникает "белых пятен" в инженерной инфраструктуре, за которые никто не отвечает.

Даже в том случае, когда заказчику необходимо действительно уникальное



Решение InfraStruxure for Small IT Spaces позволяет разворачивать критически важную ИТ-инфраструктуру в небольших помещениях

решение, вендор может кастомизировать оборудование, выбирая соответствующим образом компоненты из своего портфеля. Так устраняется риск создания любительских уникальных решений, которые в дальнейшем приведут к еще большим проблемам при модернизации дата-центра, делая ее слишком дорогой или физически невозможной.

Между тем модернизация дата-центра — это процесс, который идет постоянно, несмотря на то что средний срок службы оборудования в традиционном ЦОДе составляет около 10 лет. Как правило, главная ее цель — обеспечить рост вычислительной мощности в соответствии с ростом потребностей бизнеса.

Практика показывает, что первые изменения приходится вносить уже на этапе создания дата-центра. И если возможности изменений заложены в проект изначально, то все происходит относительно просто, с минимальными затратами и сохранением возможностей для эффективного обслуживания и гибкого наращивания инженерных систем в будущем.

Если же дата-центр создается без привлечения опытных специалистов, предусмотреть внесение изменений в будущем удастся не всегда. Вынужденная полная модернизация ЦОДа — это плата за игнорирование уже накопленной другими экспертами.

Энергоэффективность

Закладывая возможность будущего развития дата-центра, важно не забывать о резервах. Если подсчитать, что дает за год экономия всего 1 кВт потребляемой мощности, то получится вполне ощутимый результат. Средства, сэкономленные в результате снижения энергопотребления ЦОДа всего на несколько процентов, можно потратить, например, на установку дополнительного узла для повышения надежности дата-центра.

Чтобы правильно предусмотреть резервы, нужен соответствующий опыт, который есть у вендора. Он закладывает потенциал для роста энергоэффективности, например, при недозагруженности ИТ-мощностей.

Используя модульный принцип построения решений, он может предусмотреть режимы физического отключения части оборудования, когда в нем нет необходимости. Так удастся сохранить высокий уровень надежности работы ЦОДа и гибко управлять работой системы ИБП, охлаждения, других инженерных узлов.

Инженерная инфраструктура для малых помещений

Сегодня аббревиатура ЦОД знакома всем, чья работа так или иначе связана с использованием корпоративных ИТ-систем. Однако зачастую она ассоциируется с большими сооружениями и множеством стойко-мест, и именно для них, как полагают многие, создается современное инженерное оборудование, предлагаемое лидерами рынка. Между тем растущие ИТ-потребности предприятий малого и среднего бизнеса заставили ведущих производителей решений для ЦОДов обратить внимание и на тех, кому пока достаточно всего двух-трех стоек для обслуживания сотни пользователей.

Заказчики сегодня не говорят: "Нам нужно повысить эффективность ИБП" или "Нам нужно повысить надежность системы охлаждения дата-центра". Их запросы звучат иначе: "Нам нужно повысить надежность работы ЦОДа в целом" или "Мы хотим повысить эффективность его использования". Это новая ситуация на рынке, и сегодня на нем представлены готовые решения для ЦОДов любого размера.

Например, Schneider Electric имеет в своем арсенале решения даже на тот случай, когда заказчик может обойтись всего одной стойкой. И это не отдельные коробки с оборудованием, а комплексные решения.

Так, еще в 2012 г. компания вывела на рынок аппаратно-программное решение InfraStruxure for Small IT spaces, предназначенное для проектирования и построения ответственной инженерной инфраструктуры для небольших ИТ-помещений на малых и средних предприятиях. К достоинствам этого адаптивного решения относятся оперативность



Имея встроенные средства вентиляции и распределения электропитания, стойки NetShelter CX обеспечивают и высокую звукоизоляцию

монтажа, конфигурирования и инсталляции инфраструктуры в малых ИТ-помещениях, таких как серверная, коммутационный узел и даже неспециализированное пространство. В нем поддерживаются произвольные, но допустимые сочетания ИБП, стоек для серверов, средств организации кабелей, систем обеспечения физической безопасности, блоков распределения питания, оборудования охлаждения. Центральная

панель управления, объединяющая функции управления электропитанием на уровне отдельной розетки, учета энергопотребления и др., позволяет решать множество хронических проблем администрирования ИТ-систем посредством дистанционного мониторинга и управления системами электропитания, встроенных систем мониторинга, профилактического обслуживания и выдачи тревожных уведомлений.

Работу с этим масштабируемым решением дополнительно упрощают инструментарий проектирования и набор руководств по применению с конкретными рекомендациями по решению различных задач, а также описанием подходов к экономическому обоснованию внедрения.

В портфеле Schneider Electric сегодня есть решения даже под экзотические с точки зрения традиционного ЦОДа требования. Например, если у заказчика нет возможности выделить для установки стоек с оборудованием отдельную серверную комнату, их можно разместить прямо в офисном помещении. Обычная проблема в таком случае заключается в повышенном уровне шума, который мешает работе находящегося в том же помещении персонала. Разработанные инженерами Schneider Electric стойки NetShelter CX, внешне напоминающие обычные деревянные шкафы, решают эту проблему. Имея встроенные средства вентиляции и распределения электропитания, они обеспечивают и высокую звукоизоляцию. По сути, это маленькая серверная комната, где шум от установленного оборудования снижен до уровня, обычного для офиса в разгар рабочего дня.

Головоломка или готовое решение?

Надо признать, что создание (или модернизация) даже небольшого дата-центра или серверной комнаты с соблюдением современных запросов бизнеса — задача, требующая соответствующей квалификации, и решить ее своими силами компаниям малого и среднего бизнеса не просто. Их главные "болевы точки" — отсутствие подготовленных специалистов, ограниченные финансовые ресурсы. Проблема усугубляется разнообразием устройств, применяемых для доступа к сети, наличием жестких ограничений на выделение пространства под оборудование.

В такой ситуации задача становится настоящей головоломкой, а прежние подходы, выражавшиеся в комплектации дата-центра произвольными компонентами — набором ИБП, стойками для серверов, блоками распределения питания, оборудованием охлаждения, СКС — дают в итоге непредсказуемый результат.

Поэтому, в чем бы не заключалась задача, эффективнее решать ее, используя опыт, накопленный вендорами, чем изобретать собственный путь. В таком случае будущее развитие ЦОДа будет зависеть прежде всего от правильного выбора вендора. Если компания планирует развиваться, то лучший выбор — это вендор, предлагающий полный набор решений для построения ЦОДов любой мощности. У такого вендора есть и необходимый опыт, и возможности, чтобы обеспечить нужный результат, даже если потребуется значительно нарастить мощность дата-центра.

"За многие годы присутствия на рынке нами были реализованы самые разнообразные проекты: инженерные системы для суперкомпьютерных вычислений, классические машинные залы со стойками средней мощности на 4—5 кВт, стойки большой мощности, облачные решения, системы с блейд-серверами, — рассказывает Алексей Соловьев, системный архитектор компании Schneider Electric. — Комплексные решения обеспечили надежную инфраструктуру, и системы заказчиков работали эффективно. При этом мы создаем системы так, чтобы в дальнейшем их можно было эффективно обновлять и развивать".

Кибербезопасность российских железных дорог

НИКОЛАЙ НОСОВ

Безопасность транспорта — вопрос, касающийся каждого. Все мы бываем пассажирами. Как сейчас обстоит дело с обеспечением кибербезопасности железных

ИНТЕРВЬЮ дорог в России? Об этом нам рассказал **Борис Макаров**, руководитель Центра кибербезопасности ОАО НИИАС РЖД.

PC Week: Обеспечение безопасности физического объекта — комплексная задача. Как она решается на железной дороге? В чем специфика РЖД?

Б. М.: На железной дороге различают три вида безопасности:

- Функциональная безопасность, задачей которой является недопущение опасных состояний систем управления, приводящих к крушениям и столкновениям.

- Информационная, необходима для обеспечения целостности, доступности и конфиденциальности информации.

- Кибербезопасность, при этом определяется как функциональная безопасность при недостаточной апостериорной информации. То есть в условиях возникшей неопределенности при искусственном искажении информации должно быть обеспечено управление движением поездов.

Основная цель при решении проблем кибербезопасности в ОАО «РЖД» — сохранение способности различных программно-аппаратных систем автоматического управления обеспечивать безопасное и эффективное выполнение возложенных на них функциональных задач в условиях целенаправленных, умышленных, несанкционированно-деструктивных и, как правило, дистанционно-безуликовых воздействий различной физической природы. В первую очередь защищаются системы, при сбое функционирования которых есть угроза жизни и здоровью пассажиров, угроза утраты или порчи грузов.

Специфика РЖД — огромная инфраструктура. Железные дороги России занимают третье место в мире по протяженности после США — Канады, имеющих единую систему железных дорог, и Китая. Эксплуатационная протяженность Российских железных дорог — около 100 тыс. км, включающих около 5000 станций, 12 тыс. железнодорожных переездов, из которых 9000 — неохраняемые, соответственно доставляющие больше всего проблем.

Специфика заключается еще и в том, что одновременно используются оборудование и технологии, введенные в эксплуатацию еще в «царские» времена, и самые современные, внедренные буквально вчера.

Кроме того, существующая технологическая информационно-коммуникационная сеть РЖД содержит более 250 тыс. программно-аппаратных портов для подключения компьютеров и разного рода программно-управляемого оборудования. В производственной деятельнос-

**Борис Макаров**

ти используется более 233 тыс. цифровых и аналоговых радиостанций, 16 тыс. комплектов спутникового связного и навигационного оборудования, более 40 тыс. микропроцессорных систем управления (65 типов). Микропроцессоры начали использоваться с начала 1990-х, некоторым больше двадцати лет. Есть и «советские» (российские), и импортные.

PC Week: Трудно обеспечивать кибербезопасность такого большого разнообразия систем. Не планируется ли унификация автоматизированных систем управления РЖД?

Б. М.: В составе РЖД сейчас 16 железных дорог, которые строились в разное время. Используются на них системы имеют разные архитектуры, разные протоколы. Они друг с другом не стыкуются. Нет совместимости со старыми решениями. Поэтому пока делать унифицированные программно-аппаратные решения не получается. Но такая задача стоит и будет успешно решена.

PC Week: Легко ли провести кибератаку на РЖД?

Б. М.: Некоторые считают, что провести атаку на железную дорогу очень просто. Когда Президент РФ В. В. Путин приезжал в МИФИ, ему на факультете кибернетики показали модель успешной кибератаки на железную дорогу. Он поручил разобраться, и тогда выяснилось, что модель управления, взятая в МИФИ, была слишком далека от реально используемой.

Реальная система управления устроена так, что если даже хакер войдет в сеть верхнего уровня и даст команду, например, приводящую к столкновению поездов, то система нижнего уровня ее заблокирует. Но тем не менее проблемы есть.

PC Week: Какие?

Б. М.: В свое время, с целью снижения затрат, было принято непродуманное решение о сокращении обслуживающего аппарата, замене его АСУ и микропроцессорными системами управления (МПСУ). Аппарат сократили, однако появились возможности удаленного воздействия на автоматизированные системы.

Кроме того, в свое время наша радиоэлектронная промышленность умелыми руками реформаторов была угробрена,

что привело к повсеместному использованию импортных систем. Около 90% оборудования, поставившегося на железные дороги, было импортной комплектацией.

Сейчас в ОАО «РЖД» принята программа импортозамещения и сделаны первые шаги. Мы активно участвуем в этой программе. Оказалось, что во многих случаях использование импортного оборудования ничем не оправдано. Можно найти аналогичные системы внутри России, причем значительно дешевле и не хуже.

PC Week: Как вы относитесь к сообщениям об успешных атаках на АСУ ТП? Например, заражение вирусом Stuxnet центрифуг на заводе по обогащению урана в Иране или кибератака на компьютерные сети Прикарпатьеоблэнерго на Украине. Это хакеры или технологические ошибки?

Б. М.: Есть много инцидентов, которые внешне выглядят как кибератаки, а на самом деле являются следствием разгильдяйства и некомпетентности обслуживающего персонала. Такие инциденты составляют 30% от всех мировых кибератак. Их называют псевдокибератаками.

Однако в Иране кибератака была. В чем и призналась израильская разведка.

А вот на «Прикарпатьеоблэнерго» никаких кибератак не было — обычный бардак. Там более двадцати лет ничего не вкладывали в оборудование — все устарело и работает на живую нитку. Плюс, когда ушли Крым, Донбасс и Луганск, надо было все перекоммутировать, а ничего толком не сделали, так что чуть что не так — все валится.

PC Week: Что может являться целью кибератак на РЖД?

Б. М.: Объектами кибератак на железнодорожном транспорте могут являться системы диспетчерской и электрической централизации, формирующие безопасные маршруты движения поездов, системы обеспечения безопасного движения локомотивов и проезда железнодорожных переездов, системы защиты и регулирования электроснабжения, системы горочной автоматики, ответственные за сборку и расформирование поездов. Также с использованием летальных и нелетальных психофизических технологий могут проводиться атаки на операторов и обслуживающий персонал — диспетчеров, дежурных и машинистов.

Объектами, представляющими повышенную опасность, являются на верхнем уровне АСУ, а на нижнем уровне — АСУ ТП и МПСУ. На сегодняшний день в ОАО «РЖД» на верхнем уровне используется более 98 АСУ. Самая известная — АСУ продажи билетов «Экспресс-3». На нижнем локальном уровне управления используется примерно 40 тыс. МПСУ 65 типов.

Есть 10 видов МПСУ электрической централизации, отвечающих за безопасность движения, есть система маневровой

автоматической локомотивной сигнализации, работающая на станциях. Есть два вида локомотивных систем обеспечения безопасности движения поездов. Например, одна из них не допускает превышения определенного значения скорости на повороте.

Есть 31 тип микропроцессорных систем управления локомотивами, четыре вида МПСУ перегонных систем интервального регулирования движения поездов, поддерживающие необходимые интервалы движения между поездами. Ведь у поезда есть тормозной путь, и если вдруг что-то случится, поезд должен успеть затормозить. Тормозной путь у всех разный, он зависит от скорости движения и веса поезда. У «Сапсана» он может достигать 5 км.

На «Сапсане» система автоматического контроля технического состояния ревизует 76 параметров поезда. Автоматически сообщается, что впереди образовался затор, и локомотив автоматически начинает торможение. Более того, система контролирует и машиниста. Ему периодически подается сигнал бдительности, после чего машинист должен нажать на кнопку. Если он не нажал — включается сирена и идет голосовое предупреждение. Если машинист не отключил сирену, значит, с ним что-то произошло и поезд останавливается автоматически.

PC Week: А какие могут быть атаки?

Б. М.: Атаки могут быть прямые — инвазивные, непосредственно на программно-управляемые системы или комплексы (АСУ ТП, МПСУ). И косвенные — атаки на системы инженерного обеспечения (системы вентиляции — термостабилизации, системы автоматического пожаротушения, системы первичного и вторичного электропитания, шины заземления). Цель таких атак — нарушить работоспособность АСУ ТП или МПСУ.

PC Week: Существует ли какая-то устойчивая классификация кибератак на железную дорогу?

Б. М.: Да, вот перечень:

- кибершпионаж — несанкционированная передача данных, программ или географических координат (GPS или ГЛОНАСС) с помощью скрытых (незадекларированных) каналов связи;

- кибератака — разработка сценариев кибератак, хакерские и дружественные кибератаки, поиск киберуязвимостей;

- кибермошенничество — «продажа» фальшивых электронных билетов, взлом автоматов продажи билетов и квитанций оплаты багажа, взлом счетчиков учета энергоносителей и автоматических расходомеров и заправщиков;

- киберхалатность — кибератаки вследствие случайных ошибок или неквалифицированных действий персонала;

- киберсаботаж — снижение пропускной способности железной дороги вплоть до полной остановки движения;

- кибердиверсии — создание враждебных и опасных маршрутов следования (движения) поездов, особенно при перевозке особо опасных и социально значимых грузов, пассажирских и воинских перевозках.

PC Week: Можно подробнее рассказать о кибердиверсиях?

Б. М.: Примерами кибердиверсий могут служить крушение подвижного состава в кривых и на спуске из-за нарушения скоростного режима, перевод железнодорожных стрелок под составом, создание враждебных маршрутов следования, приводящих к столкновению со встречным, стоящим или впереди идущим поездом. Другие примеры — нарушение процесса сборки и расформирования составов (маневровые и горочные технологии), отказ автоматики железнодорожного переезда, неконтролируемая имитация ложной занятости или свободы железнодородных путей.

Кстати, атаки могут проводиться и на системы инженерного обеспечения: системы вторичного электропитания, которые, как правило, управляются дистанционно, шины заземления, системы пожаротушения, охраняемые системы. Мы их называем многофакторные атаки.

PC Week: Насколько соответствуют истине слухи, что хакеры перевели стрелки и столкнули два товарных поезда?

Б. М.: На самом деле этого не было. Однако в лабораторных условиях, исследуя оборудование, поставляемое в Россию одной очень известной иностранной фирмой, мы получили такие результаты. На стенде был осуществлен перевод стрелки под движущимся составом. Причем никаких следов наша кибератака не оставила. Было принято решение о запрете покупки данного оборудования.

PC Week: Как хакер может зайти в вашу сеть?

Б. М.: В системе есть сотни тысяч программно-аппаратных портов — точек входа в локальную сеть. Часть этой сети является полностью закрытой, а часть — комбинированной и из нее можно выходить в Интернет. Если известны архитектура, порт, протокол и схема управления портами, в принципе можно «зайти» в некоторое оборудование, зная место его дислокации. Конечно, мы проводим работы и блокируем уязвимости. Но вы же понимаете, что каждый день появляются новые эксплойты.

PC Week: Какова ваша политика в области лицензирования и сертификации?

Б. М.: В основном у нас используются версии Windows, имеющие сертификат безопасности ФСТЭК. Если же обнаруживается система без сертификата безопасности, то она, как правило, уничтожается.

Бывают проблемы, когда не хотят покупать новое ПО, а старые версии не получают поддержки производителя ▶

и новые уязвимости не закрываются. Например, кое-где еще используется Windows XP, уже не поддерживаемая Microsoft. Бывает, пользователи экономят и, чтобы не покупать новое, заимствуют никому не принадлежащее, брошенное ПО, в котором могут быть разные закладки. Бывают ситуации, когда сертификат безопасности ФСТЭК у программы есть, но он просрочен. Или система модифицирована, а пользователи не понимают, что после этого надо опять проходить сертификацию ФСТЭК, что является требованием государства.

PC Week: Когда даете свое заключение по кибербезопасности, вы проверяете исходный код на наличие закладок?

Б. М.: Есть свои сложности. Некоторые добросовестные поставщики дают исходный код и всячески содействуют, чтобы были выявлены разные недекларируемые возможности. Другие, наоборот, всячески препятствуют нашей работе. Они или не дают исходный код, или дают, но не полностью. Были случаи — нам дали исходный код, а он не собирается. Требуются еще файлы. И так по пять-шесть раз собираем, пока не получаем рабочую исполняемую версию ПО.

Общая беда для России — множество посредников при закупке. Кто-то из жадности или недомыслия не потребовал от поставщика ПО исходный код, а когда с посредников начинаешь спрашивать, выясняется, что закупили через фирму, которой уже нет. Так что получить исходные коды для исследования удается не всегда.

Сейчас разработано положение о порядке приобретения и хранения ПО, где четко прописано требование предоставления исходных кодов. Положение будет утверждено в ближайшее время. На Западе твердо требуют предоставления исходных кодов. Да, заключается соглашение о конфиденциальности, но тем не менее исходные коды должны быть. Ведь если их нет, то фирма-поставщик может использовать вас как “дойную корову”. Например, если что-то нужно изменить, даже незначительное, — придется обращаться к ним и не бесплатно. К сожалению, в РЖД такие ситуации встречаются достаточно часто.

PC Week: Закладки бывают только в продукции западных фирм?

Б. М.: В китайских системах мы такого не замечали. А в западных — были.

PC Week: Программы низкого уровня для контроллеров вы тоже тестируете?

Б. М.: Да, конечно. Причем в последнее время мы стали переходить на контроллеры и процессоры отечественного производства, такие как “Байкал” и “Эльбрус”. У нас есть несколько своих разработок. Кроме того, мы берем разработки других фирм и тоже проводим тестирование.

PC Week: Своему ПО доверия больше. Требуется ли вы от контроллеров возможности перепрошивки?

Б. М.: По-разному. В некоторых системах требуем, в некоторых нет. Было время, когда не было разнообразия поставщиков. Один, редко два. За последние пять лет положение изменилось. Появилась возможность выбора, можно ужесточать требования.

PC Week: Что еще можно сделать для борьбы с закладками?

Б. М.: В свое время был ГОСТ о порядке закупки для критически важных областей. Потом его отменили, мотивируя требованием прозрачности. Стало хуже в плане безопасности, потому что теперь всем понятно, куда и для чего закупается оборудование. А железнодорожный транспорт — критическая область. И туда могут засунуть закладки.

PC Week: Где вы проводите кибераудит? У себя в лаборатории?

Б. М.: С этим бывают проблемы. Иногда железнодорожные системы настолько громоздки, что к нам в лабораторию просто не помещаются. Приходится делать кибераудит на месте постоянной дислокации объекта. Особые сложности возникают, когда нужно делать кибераудит за пределами России.

Сейчас у нас идут переговоры с известной американской компанией. Представители этой фирмы предлагают проверить оборудование в их лаборатории. При этом просят предварительно передать им наше ПО, чтобы они могли его проверить на предмет закладок. Возможно, это делается для того, чтобы изучить наши методы исследования и так замаскировать свои уязвимости, чтобы мы ничего не нашли.

PC Week: Какие профилактические работы по кибербезопасности проводятся в РЖД?

Б. М.: Мы проводили и проводим тестирование систем МПСУ на кибербезопасность в соответствии с приказом ФСТЭК № 31 от 14 марта 2014 г. Нет ни одной системы, которая бы на 100% удовлетворяла требованиям. Разброс соответствия — в диапазоне от 16 до 75%. Многие поставщики, например Московский энергомеханический завод (МЭЗ), стали преобразовывать свои системы, устраняя выявленные недостатки. После выполнения этих работ мы будем проводить повторные исследования.

А иногда встречаем и непонимание. Говорят: “Да, вы нашли уязвимость, но она не в нашей зоне ответственности. Вы ее вскрыли через систему технологической связи, а за это связисты отвечают”. Не понимают, что сами должны были предусмотреть возможность входа через эту сеть и принять меры по обеспечению безопасности.

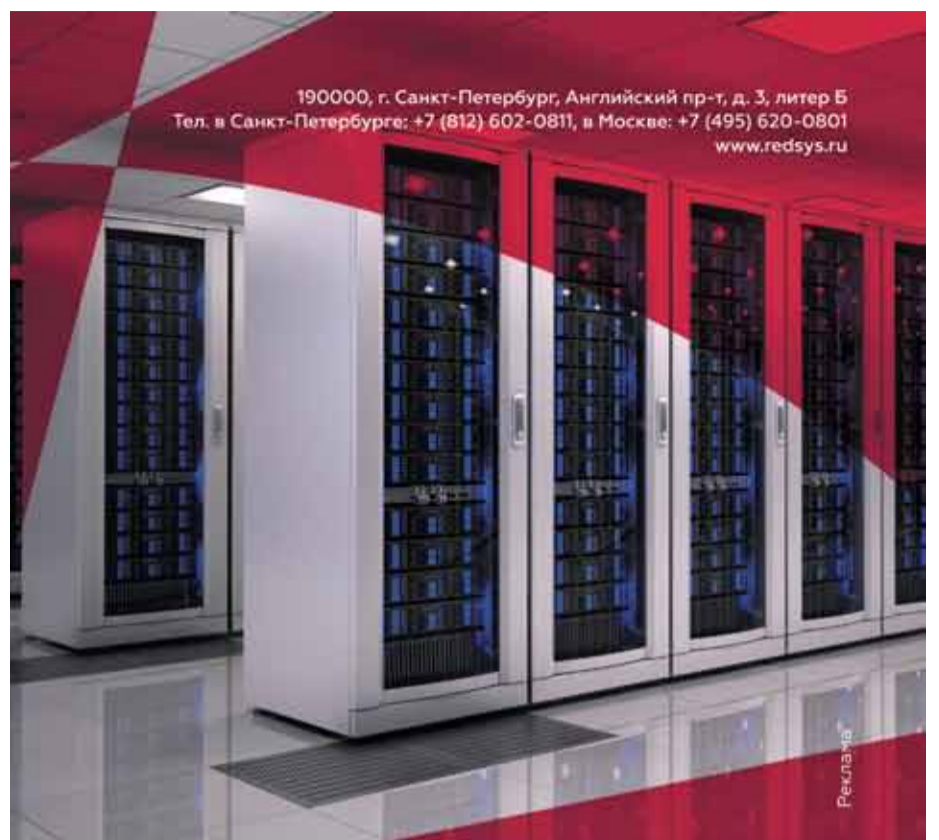
PC Week: Какие уязвимости удалось выявить в системах РЖД?

Б. М.: За последние два года мы исследовали более 30 систем. Мы выявили уязвимости в МПСУ и определили возможные кибератаки:

- блокирование работоспособности систем. Например, при загрузке системы считается контрольная сумма, она не совпадает, начинается перезагрузка и так еще и еще раз. Перезагрузка идет, а система продолжает оставаться неработоспособной;
- блокирование систем контроля каналов визуализации. Исполнительный механизм передает информацию о своем состоянии в диспетчерскую. И человек должен что-то включить или выключить. Если эта информация искажается, правильные решения человек не принимает;
- неконтролируемая имитация ложной занятости и свободы железнодорожных путей;
- возможность несанкционированного изменения исполняемого ПО и последующего перевода стрелок под движущимся составом (то, что мы выявили при тестировании системы одной западной фирмы);
- несанкционированная передача по радиоканалу информации о текущем состоянии технических систем локомотива и путевых машин (ПМ);
- возможность дистанционно и несанкционированно изменять параметры управления локомотивом и ПМ;
- несанкционированный контроль географических координат локомотива и ПМ;
- возможность перехвата управления.

Например, в контроллерах, закупленных у одной западной фирмы, была обнаружена система программно-управляемых ключей, которые, получив команду, делали короткое замыкание на шину, и платы выгорали. У спецслужб есть перечень фирм, замеченных в таких вещах.

ПРОДОЛЖЕНИЕ НА С. 15 ▶



Управление ресурсами ЦОД

IBM Systems Director — комплексный продукт для мониторинга и управления ИТ-инфраструктурой ЦОД

Цели и задачи внедрения IBM Systems Director

- Снижение стоимости владения ИТ-инфраструктурой
- Соответствие ИТ-инфраструктуры требованиям бизнеса

Автоматизация

- Централизованный мониторинг всей ИТ-инфраструктуры ЦОД
- Централизованное управление всей ИТ-инфраструктурой ЦОД
- Наглядное представление ИТ-инфраструктуры ЦОД
- Централизованная инвентаризация оборудования
- Автоматизация отчетности
- Анализ контрольных параметров с выдачей уведомлений
- Автоматизация рутинных операций

Стоимость владения ИТ-инфраструктурой

- Централизованное управление обновлениями и конфигурациями сокращает эксплуатационные затраты
- Сокращение расходов на персонал для поддержания ИТ-инфраструктуры в работоспособном состоянии за счет консолидации интерфейсов управления разных платформ в единой консоли управления и мониторинга
- Анализ загрузки и формирование рекомендаций для оптимизации ИТ-инфраструктуры
- Увеличение коэффициента доступности ИТ-инфраструктуры за счет своевременного отслеживания неисправностей и сбоев

Преимущества компании RedSys

- Наличие демо-центра с широким спектром оборудования
- Сильная команда профессионалов по направлению системы мониторинга и управления
- Уже реализованные проекты по направлению системы мониторинга и управления в крупных заказчиках
- Опыт сопровождения систем мониторинга и управления

г. Санкт-Петербург: +7 (812) 602-08-11, office.spb@redsys.ru
г. Москва: +7 (495) 620-08-01, project@redsys.ru
г. Новосибирск: +7 (383) 347-26-02, office.nsk@redsys.ru
г. Ростов-на-Дону: +7 (863) 308-96-27, office.don@redsys.ru
г. Нижний Новгород: +7 (831) 216-24-30, office.nn@redsys.ru
г. Хабаровск: +7 (4212) 31-45-30, office.dv@redsys.ru



RESPONSIBILITY
EFFICIENCY
DEVELOPMENT
REDSYS



Логотип IBM, логотип IBM Premier Business Partner, IBM Systems Director являются товарными знаками
Интеллектуальной собственности корпорации IBM, зарегистрированными во многих странах мира. Служба товарных знаков,
зарегистрированная IBM на настоящий момент, представлена по адресу: www.ibm.com/legal/copytrade.shtml

Переход дистрибьютора на ЭДО: опыт первопроходца

В последние годы темати-ка автоматизации доку-менториентированных бизнес-процессов неуклонно сме-щается от задач традиционного внутреннего организационно-распорядительного документооборота в сторону обеспечения электронного коммерческого взаимодействия предприятий. Начало этому процессу в существенной мере положило законодательное закрепление в 2012 г. возможности обмена электронными счетами-фактурами, которое, в свою очередь, послужило стимулом использования такого электронного способа и для передачи между организациями более широкого спектра деловых документов. При этом особенностью электронно-документационного взаимодействия контрагентов является законодательно закрепленная необходимость работы через сертифицированных операторов.

Как и в случае любых других инноваций, внедрение методов электронного взаимодействия организаций идет далеко не просто, на пути к повышению эффективности работы возникают трудности технического, организационного и нормативно-характера, отраслевой опыт вскрывает недостатки в законодательном регулировании. В то же время порой компании неожиданно открывают для себя новые, поначалу невидимые эффекты от внедренных технологий, новые возможности для улучшения своей деятельности. О том, как идет процесс перехода на электронный документооборот (ЭДО), что это дает компании, какие проблемы при этом возникают и как они решаются, обозревателю PC Week/RE Андрей Колесов беседовал с начальником отдела информационных технологий московского филиала компании “Катрен” Сергеем Тарасовым.

PC Week: Чем занимается ваша компания, какое место в ее деятельности занимают ИТ и что представляет собой ее документационное взаимодействие с контрагентами?

СЕРГЕЙ ТАРАСОВ: “Катрен” — это крупнейший в России дистрибьютор лекарственных средств, которому принадлежит около 17% данного рынка. Центральный офис находится в Новосибирске, компания работает во всех регионах страны через 28 филиалов. В нашем прайс-листе более 18 тыс. позиций, у нас свыше 700 поставщиков и более 43 тыс. пунктов доставки. Понятно, что бизнес “Катрена” базируется как раз на взаимодействии с внешними контрагентами, подавляющая их часть — это наши потребители, аптеки, которые получают от нас медикаменты и продают их частным лицам.

В качестве информационной системы управления компанией и всеми ее бизнес-процессами в “Катрене” используется собственная разработка, которая в интегрированном варианте решает задачи CRM, ERP, ECM и т. п. Ориентация на собственную ИТ-систему — изначально философия компании.

Понятно, что работа дистрибьютора сопровождается огром-



Сергей Тарасов

ным документопотоком. Сейчас мы только в московском филиале ежедневно создаем более семи тысяч пакетов, каждый из которых содержит не менее четырех документов. Эти пакеты отправляются нашим получателям, мы должны отслеживать их доставку, отвечать на возможные встречные запросы. Поток обмена документами растет, нужно снижать не только издержки на эту работу (печатать, ведение бумажного архива и пр.), но и повышать ее эффективность. Собственно, эти задачи были для нас главными при переходе на электронное взаимодействие с потребителями.

PC Week: А снижение издержек и повышение эффективности — это не одно и то же?

С. Т.: Это связанные понятия, но все же несколько различные. Например, наша компания не так давно запустила проект “Аптека.Ру” по прямой интернет-продаже лекарств частным лицам, используя партнеров в качестве доставочных пунктов. Понятно, что такая схема сопровождается резким увеличением объема документов, и ручными методами, даже если на них не жалеть денег, её реализовать практически невозможно. При этом, конечно, задача снижения издержек тоже является первостепенной: по мере роста бизнеса доля затрат на обеспечение документооборота растет (особенно с учетом роста курса валюты, поскольку стоимость ИТ привязана к ней), опережая, например, темпы роста складских и транспортных затрат.

PC Week: Вашему проекту перехода на внешний ЭДО уже более трех лет. Как вы охарактеризовали бы основные его этапы и эффекты, полученные от его реализации?

С. Т.: Да, решение о внедрении ЭДО было принято в октябре 2012 г., фактически сразу после принятия законов, разрешающих такое деловое общение, то есть “Катрен” стал одним из пионеров этого направления в России. Сначала было изучение правовой базы и базовых технологий (API взаимодействия с операторами); формирование ТЗ и разработка ПО заняли пять месяцев; в июне 2013-го началось тестирование, а уже в октябре, ровно через год после старта, система перешла в режим промышленной эксплуатации. На первом этапе мы не форсировали расширение объема ЭДО, нужно было убедиться в его надежности и произ-

водительности. А с июля 2014 г. началось активное продвижение этого решения в сеть контрагентов, что потребовало как доработки системы на нашей стороне, так и помощи контрагентам по подключению к ЭДО со стороны их ИТ-решений.

Для ИТ-подразделения компании весь этот проект был, конечно, связан с повышением нагрузки не только потому, что нужно было внедрять новые технологии, но и в связи с их сопровождением. Как я уже говорил, в целом по стране ЭДО находится, наверное, еще на начальном этапе становления, идет регулярное обновление разного рода нормативных требований, на которые мы должны оперативно реагировать.

Но бизнес компании вполне очевидно выиграл. Резко сократился объем печати документов, который до этого рос довольно быстрыми темпами. В частности, мы перестали закупать принтеры. То же самое можно сказать об архиве документов — поддержка его бумажного варианта требовала все больших затрат. Хотя, пожалуй, главные эффекты заключаются в ускорении бизнес-процессов, в повышении их надежности. Кроме того, поскольку у нас довольно большие объемы обмена электронными документами, мы смогли получить от наших операторов ЭДО очень неплохие скидки.

PC Week: Как повлияла реализация внешнего обмена электронными документами на автоматизацию внутреннего документооборота?

С. Т.: В минимальной степени, поскольку в нашей компании фактически с момента ее возникновения внутренний документооборот выполнялся в электронном виде. Более того, мы и раньше общались с нашими контрагентами в электронном виде, все документы передавались в нужных им форматах (наша среда поддерживает около трехсот форматов документов для самых разных систем, используемых партнерами). Но тогда этот механизм имел сугубо информационную функцию, он работал в параллель с потоком бумажных документов, которые обеспечивали юридическую значимость деловых операций. Переход на юридически значимый ЭДО позволил исключить бумажный контур.

Хотя полностью уйти от бумажных документов все же пока не получается. Но такой задачи как некой самоцели и не было — нам нужно было повысить эффективность бизнес-процессов.

PC Week: Как проходил выбор операторов, как строятся отношения с ними?

С. Т.: У нас уже был опыт работы с операторами по сдаче налоговой отчетности в электронном виде, он помог нам при переходе на электронное взаимодействие с контрагентами. Мы ориентировались на знакомых нам партнеров, хотя, конечно, изучили их возможности по обмену документами с компаниями (технологии сдачи налоговой отчетности и обмена документами с контрагентами — это все же существенно разные вещи). Главные требования к про-

вайдерам состояли в том, чтобы у них были представительства во всех регионах страны, единое ценообразование для всех наших филиалов, а также возможность интеграции их решений с нашей ИТ-системой. В результате мы выбрали сервисы нескольких операторов, в том числе два основных — “Диадок” (“СКБ Контур”) и СБИС (“Тензор”).

PC Week: Поскольку вы имеете дело с несколькими операторами, можно сделать вывод, что проблема роуминга, работы с контрагентами, подключенными к другим операторам, до сих пор не решена. Насколько эта проблема существенна для вас?

С. Т.: Проблема такая есть, но для нашего бизнеса она пока не очень важна. Операторы говорят нам, что в принципе могут реализовать роуминг, но это требует некоторых дополнительных затрат. Пока получается, что нам проще использовать “монооператорскую” схему, два оператора — это вполне нормально для нас, при этом обеспечен географический охват всей нашей партнерской сети. Но можно предположить, что в будущем потребность в роуминге все же возникнет. И тут есть два основных момента.

Первое: наша отрасль находится на начальной стадии внедрения внешнего ЭДО. Подавляющее число аптек до сих пор его просто не использовали, поэтому они могут подписаться на услуги оператора, которого мы им предлагаем. Но по мере того, как на такое взаимодействие будут переходить другие дистрибьюторы, число задействованных операторов может расти.

Мы сами сталкиваемся с подобной проблемой при работе со своими поставщиками, среди которых есть и иностранные, использующие другие методы обмена документами. Но проблема автоматизации обмена документами с поставщиками для нас не очень актуальна, поскольку их число все же не столь велико, как количество наших потребителей. Тут мы пока можем продолжать работать в бумажном варианте.

PC Week: Разговоры о роуминге идут уже давно, мы регулярно слышим обещания решить эту проблему в ближайшее время, но реальный прогресс пока не очень ощущается. Почему так происходит?

С. Т.: На нашем примере видно, что рынок находится скорее в начальной стадии формирования, когда главными игроками являются оптовые продавцы. На этом этапе роуминг нельзя считать задачей номер один, то есть четко выраженного требования к этому механизму со стороны пользователей пока нет. Соответственно и операторам нет смысла обеспечивать такое взаимодействие между собой. В этот вопрос мог бы вмешаться регулятор, выпустив нужные нормативные требования, но он тоже занимает сейчас нейтральную позицию, возможно, понимая, что проблема ещё “не созрела” до нужной степени актуальности.

PC Week: С какими трудностями вы столкнулись в своем проекте за более чем трехлетний срок?

С. Т.: Основной проблемой было то, что мы были фактически первопроходцами. Среди трудностей нужно в первую очередь отметить несовершенство законодательства, необходимость в существенной и постоянной доработке наших собственных ИТ-систем, а также низкий уровень развития ЭДО в России, боязнь предприятий и конкретных людей работать без бумаги. Пришлось потратить много усилий на продвижение этой идеи как в собственной компании (речь идет о рядовых сотрудниках, руководство всё отлично понимало, оно и инициировало проект), так и у контрагентов. Если бы начали проект сейчас или год назад, всё было бы намного проще, так как рынок уже понимает эту тему намного лучше, чем в 2012-м.

PC Week: Но если бы такие компании, как ваша, не начали эту работу, то, возможно, сегодня понимание было бы таким же, как три года назад, и вам все равно пришлось бы выступать в роли первопроходцев.

С. Т.: Да, наверное, вы правы, кто-то должен быть первым. Но надо сказать, что мы были не одни, внедрением внешнего ЭДО тогда начали заниматься многие крупные коммерческие компании, в том числе наши конкуренты по дистрибуции лекарственных товаров.

PC Week: Насколько я понимаю, переход вашей компании на ЭДО еще далек от 100%?

С. Т.: Да, переход на ЭДО — это процесс, который пока не закончен. В нашей компании по плану во всех филиалах до конца текущего года его доля должна быть не менее 50%. Какие-то отделения уже вышли на этот показатель, у нас, в московском филиале, по состоянию на март достигнут уровень 45%, а ровно год назад было 20%, то есть динамика весьма оптимистичная.

PC Week: Основная трудность заключается в неготовности ваших контрагентов?

С. Т.: Я не стал бы использовать слово “неготовность”, лучше сказать — для них такой переход пока или сложен, или не очень нужен. Кому-то придется вносить серьезные коррективы в свои бизнес-процессы и ИТ-системы, кто-то работает не вполне “в белую” и не нуждается в повышении прозрачности. Хотя есть, конечно, и недопонимание возможностей ЭДО.

PC Week: Как вы видите развитие своей системы ЭДО?

С. Т.: Нужна проработка вопросов юридической значимости документооборота. Пока мы в основном имели дело с аспектом соответствия нормативным требованиям, но есть и другая сторона — решение юридических конфликтов, в том числе и в суде. Нельзя сказать, что у нас много таких конфликтов, но система должна быть выстроена так, чтобы мы могли использовать электронные документы в подобных разбирательствах. Самый простой вопрос — в каком формате и в каком виде мы должны представлять нужные документы в суд? Нужно анализировать отраслевой опыт, изучать судебную практику...

Банки на пороге новой технологической революции

Российские банки стали в свое время лидерами по применению передовых информационных технологий. И хотя сегодня все они оснащены автоматизированными банковскими системами, приложениями для взаимодействия с клиентами, оценки рисков и рядом других, жизнь ставит перед ними новые задачи. Банки становятся поставщиками гибко настраиваемых банковских продуктов и сервисов, опирающихся на самые передовые информационные технологии. Руководители крупнейшей отечественной кредитной организации — Сбербанк России — все чаще не без основания называют себя ИТ-компанией с банковской лицензией. Сегодня уже никого не удивляет, что финансовые сервисы начинают предоставлять мобильные операторы и провайдеры интернет-услуг. Появление таких инновационных технологий, как blockchain и SmartContracts, привлекает внимание крупнейших банков и ставит новые задачи перед ИТ-компаниями. О современном состоянии ИТ в российских банках, наиболее вероятных тенденциях их развития и решениях, предлагаемых компанией «Техносерв Консалтинг», рассказал заместитель генерального директора, директор по продажам **Алексей Катрич**.



Алексей Катрич

накопить опыт для безрискового перевода банковских данных и систем в облака.

Наряду с технологическими вызовами российские кредитные учреждения также сталкиваются с вызовами, обусловленными влиянием экономического кризиса и вероятными санкционными рисками. В чем специфика этих вызовов?

Ключевая специфика этих вызовов проявляется в необходимости выбора для внедрения между ПО из открытого государственного реестра и доступными иностранными продуктами, а также перевода банков на открытую архитектуру и организации взаимодействия с FinTech-компаниями. При этом перед ними стоит задача оптимизировать не только ИТ-расходы, но и все поддерживающие деятельность банка процессы: от запроса клиента до проводки по счету.

Как сегодня изменились требования к системам дистанционного банковского обслуживания (ДБО)? На кого они в основном ориентированы и в какой мере существующие на российском рынке ДБО-решения удовлетворяют современным требованиям многоканального обслуживания?

Задача внедрения системы ДБО преобразовалась в три ключевых бизнес-решения: цифровое отделение банка (Digital branch), предоставление банковских услуг в смежных бизнес-областях (White Label Banking), создание параллельного цифрового банка в интернет-пространстве (Dual Brand). Лидеры рынка систем ДБО предоставляют функционал для работы с любыми сегментами клиентов как по видам деятельности, так и по социальным группам. Большинство основных игроков банковского сектора уже создали облачные сервисы по услуге ДБО. Наша компания также имеет в реестре продуктов подобный облачный сервис.

Расскажите подробнее о решениях, которые ваша компания предлагает для банковских структур. В чем их особенность?

Работа с банками и финансовыми организациями — одно из приоритетных направлений деятельности нашей компании. И прежде всего отмечу, что ключевые предложения «Техносерв Консалтинг» подготовлены как отдельные, не зависящие от платформы продуктовые решения и переведены в облака. Заказчик при этом сначала выбирает принцип реализации бизнес-процесса под задачи банка, а затем уже принимает решение по платформе, на которой он будет построен.

Системы и услуги, которые мы предлагаем, сфокусированы на повышении эффективности деятельности финансовых учреждений и оптимизации ключевых направлений развития бизнеса. Они позволяют автоматизировать различные банковские процессы, включая следующие:

- единый фронт-офис;
- контакт-центр;

- корпоративные и розничные продажи;
- программы лояльности;
- дистанционное банковское обслуживание;
- целевые (в том числе онлайн) маркетинговые кампании;
- работа с проблемными активами Collection;
- корпоративное и розничное кредитование;
- управление лимитами;
- управление рисками;
- управление документооборотом (договорной, кадровый, ОРД);
- управление персоналом;
- административно-хозяйственная деятельность;
- бюджетирование;
- управление финансами;
- управление имуществом;
- казначейство;
- электронный архив;
- управление корпоративной базой знаний.

В целом же наша компания предлагает банкам единую стратегию, нацеленную как на усиление бизнес-модели B2C с помощью решений Digital Branch и Dual Brand, так и на расширение B2B-бизнеса в других индустриях с помощью решения White Label Banking с максимальным использованием инноваций и решений FinTech-индустрии. Тем самым банк превращается в глобальную платформу предоставления финансовых услуг на основе модели Banking-as-a-Platform.

Сегодня все чаще говорят о необходимости цифровой трансформации предприятий. Банки, очевидно, имеют шанс возглавить этот процесс?

Действительно, сегодня банки фокусируются на создании параллельного цифрового бренда (Dual Brand) в интернет-пространстве для четкой сегментации услуг среди разных групп клиентов. Создание цифрового офиса (Digital Branch) становится общепринятым стандартом, аналогично появлению в свое время банкомата рядом с кассовым узлом в отделении банка. Постепенный уход финансовых транзакций из банков в FinTech-компанию стимулирует создание открытой банковской B2B-платформы с возможностью подключения внешних игроков для создания новых финансовых продуктов и клиентских каналов.

Поясните, в чем суть упомянутой выше технологии SmartContracts. Какие задачи решаются с ее помощью?

Функционал SmartContracts (так называемых умных контрактов) позволяет автоматизировать конкретный бизнес-процесс компании и настроить искусственный интеллект для принятия базовых решений при выполнении этого бизнес-процесса. В безрисковых бизнес-процессах данный функционал совершит революцию, подобную той, что произошла с заменой ручного труда на электрические станки.

Главным триггером здесь стало появление криптографических решений, исключающих подделку документов в цифровом пространстве. А тогда почему бы не разместить ПТС автомобиля, личный паспорт и другие документы с уникальной открытой цифровой подписью в социальной сети и перестать пользоваться сложной системой нотариальных процедур?

В данном случае вы говорите о технологии blockchain. В какой мере она готова к практическому применению? Какие преимущества сулит эта технология и ведет ли ваша компания работы в данном направлении?

Наша компания активно развивает данную тему и является экспертом в том, что касается blockchain. Можно с уверенностью утверждать, что уже в ближайшие месяцы

технология blockchain обеспечит революционный прорыв в оптимизации бизнес-процессов на всех уровнях компаний, позволив заменить людей, занимающих сегодня определенные функциональные должности, интеллектуальными роботами и упростив персонализацию транзакций благодаря использованию уникальных идентификаторов на каждом документе и открытых реестров.

Возьмем, к примеру, функции нотариуса. Его офис является по своей сути реестром хранения записей и службой верификации подлинности документов. В результате переноса всех документов в систему blockchain мы получим идентичный реестр с уникальным для каждого цифрового документа идентификатором, исключающим возможность подделки и обеспечивающим однозначную проверку владельца данного документа. Хранение копий документов во множестве распределенных узлов сети исключает их потерю в случае пожара, утраты или неработоспособности одного из узлов. Наличие открытого реестра документов с уникальными идентификаторами позволяет отказаться от нотариальных копий, которые при распространении документов замещаются электронной ссылкой. При этом SmartContracts, или простейшие роботы, могут выполнять основную работу по приему документов и размещению записей в реестре. Подобным же образом можно заменить выполняющих формальные функции работников в самых разных сферах, а используемые там документы перевести в цифровое пространство.

Важно отметить, что с учетом существующей информации о нас в социальных сетях 99% документов не имеют грифа «конфиденциально». Это позволяет выложить большую часть такой информации в открытый доступ и сократить массовое дублирование данных во всем мире, систематизировать информацию в открытых источниках и исключить огромное число бесполезных бизнес-процессов во всех областях нашей жизни.

Надо быть готовыми к тому, что нас ждет массовый перевод некавалифицированного труда в облачное пространство и его автоматизация на основе технологии blockchain и SmartContracts, а высвобожденные человеческие ресурсы будут направлены на более интеллектуальные задачи. Это потребует серьезного обучения и повышения квалификации персонала, ведь если простейшие операции можно будет возложить на SmartContracts, то сама собой исчезнет необходимость в тех, кто ранее, образно говоря, перекладывал бумагу с места на место. Мир освободится от огромного бюрократического пласта и вернет людей к производству реальных физических или интеллектуальных продуктов.

Внедрение новых технологий всегда сопряжено и с появлением новых угроз информационной безопасности, что особенно актуально для банковских учреждений, которые всегда были объектом пристального внимания киберкриминала. Значит, надо готовиться и к усилению защитных редутов?

Платой за интеграцию внутренних банковских процессов и систем в мировую социальную сеть и информационное пространство стало постоянное усложнение кибератак со стороны криминальных структур. Сами банки в одиночку уже не способны бороться с данным вызовом, и в дело вступают компании, специализирующиеся в сфере информационной безопасности. Важно также исправно выполнять требования регулятора по ее обеспечению. Профилактика и постоянное обучение правилам ИБ всего персонала банка — такое же необходимое дело, как и ежегодное медицинское обследование.

ИБП APC Back-UPS BX650LI-GR: защита и стабилизация питания с минимальными затратами

ВЛАДИМИР РОМАНЧЕНКО

Традиционно ИБП небольшой мощности, такие как, например, APC Back-UPS BX650LI-GR, позиционировались в качестве решения для защиты питания офисных ПК и позволяли в случае внезапного отключения или сбоя в электросети избежать потери данных и при необходимости обеспечить штатное выключение оборудования. Однако времена меняются, и сейчас на смену громоздким и жадным до электричества десктопам повсеместно приходят компактные экономичные ПК, моноблоки и системы “два в одном”, а в некоторых случаях и вовсе мобильные и портативные устройства с собственной батареей. Теперь в случае сбоя электроснабжения порой важнее обеспечить резервное питание офисному беспроводному маршрутизатору или другим необходимым для работы устройствам.

То же самое справедливо и в домашних условиях, где резервирование питания коммуникаций, NAS или систем жизнеобеспечения “умного дома” может оказаться более целесообразным, нежели, например, домашнего развлекательного центра.

Во всех этих ситуациях уже упомянутый нами ИБП APC Back-UPS BX650LI-GR производства Schneider Electric, с которым мы имели возможность ознакомиться непосредственно, может стать хорошим выбором, позволив обеспечить надежное питание сразу нескольких устройств при небольших затратах.

APC Back-UPS BX650LI-GR относится к категории ИБП линейно-интерактивного типа и имеет выходную мощность 650 В·А (325 Вт). Выполнен он в классическом для подобных устройств корпусе из ударопрочного ABS-пластика чёрного цвета. Небольшие габариты (142×101×300 мм) и масса (4,4 кг) устройства позволяют разместить его так, чтобы оно не мешало и не бросалось в глаза. Но при этом следует позаботиться о том, чтобы ИБП был легко доступен — время от времени вам, вероятно, потребуется взглянуть на светодиодный индикатор состояния или воспользоваться размещенной рядом с ним на передней панели кнопкой для включения или перепрограммирования устройства, а также для отключения тревожного сигнала в случае перехода ИБП на резервное питание.

К сети ИБП APC Back-UPS BX650LI-GR подсоединяется через несъемный силовой кабель, заведенный с тыльной стороны корпуса. Здесь же расположены две компьютерные евророзетки (Schuko) для подключения защищаемого оборудования, а также классический предохранитель. С помощью ключа-разъема яркого желтого цвета подключается внутренняя батарея ИБП (во время хранения и транспортировки ИБП она отключена для

предохранения от разряда и преждевременного старения).

Благодаря наличию встроенного автоматического стабилизатора (AVR), обеспечивающего ступенчатую регулировку выходного напряжения, модель APC Back-UPS BX650LI-GR будет весьма эффективна при нестабильном напряжении электросети. При колебаниях входного напряжения в пределах от 180 до 270 В она обеспечит номинальное выходное напряжение (230 В) без перепада на питание от батареи. В стандартном режиме этот ИБП также фильтрует шумы и защищает оборудование от всплесков напряжения с энергией до 160 Дж.

ИБП Back-UPS BX650LI-GR снабжен одной герметичной свинцово-кислотной батареей необслуживаемого типа APCRBC110 с загущенным электролитом и защитой от утечек. Конструкция ИБП не предусматривает самостоятельной замены батареи пользователем, но благодаря встроенной системе самодиагностики ИБП своевременно обнаружит и автоматически оповестит о необходимости замены батареи. В таком случае рекомендуется обратиться в сервисный центр APC.

Заявленная производителем ёмкость батареи составляет 75 В·А·ч, типичное время полной зарядки — от четырех до шести часов (при первом включении



Внешний вид ИБП APC Back-UPS BX650LI-GR

ASUS Zenfone MAX: максимальная автономность, сбалансированные возможности

ВЛАДИМИР РОМАНЧЕНКО

Среди пользователей современных смартфонов на базе ОС Android найдется немало таких, кто увеличению производительности своего устройства предпочел бы продление времени его автономной работы от батареи. Если в течение дня смартфон используется активно, хочешь или не хочешь, а приходится снижать яркость экрана, отключать временно неиспользуемые радиоинтерфейсы и GPS, ограничивать число фоновых процессов и запущенных приложений... Кардинальный же вариант — приобрести устройство с более емкой батареей. Например, ASUS Zenfone MAX, у которого в этом смысле сегодня на рынке немного конкурентов, особенно если речь идет об устройствах известных брендов.

Действительно, если одни модели могут похвастать высочайшей производительностью или максимальной плотностью пикселей на экране, то у Zenfone MAX главное достоинство — это встроенный литий-полимерный аккумулятор ёмкостью 5000 мА·ч, благодаря которому смартфон, видимо, и получил своё название. В результате заявленное производителем время автономной работы устройства в режиме разговора составляет 37,6 ч, в режиме ожидания — до 914 ч. Мой личный опыт эксплуатации Zenfone MAX показал, что разрядить его до нуля при активном использовании с раннего утра до поздней ночи практически невозможно, даже если оставить включенными все беспроводные интерфейсы и модуль GPS. А в случае неэкстремального

сценария использования Zenfone MAX способен продержаться без подзарядки несколько суток.

Понятно, что за такую “живучесть” приходится чем-то платить. В данном случае это прежде всего немаленькая масса — 202 г. Хотя она не рекордная (есть смартфоны и потяжелее!), но внутренний карман пиджака смартфон оттягивает ощутимо. Толщина корпуса у него тоже немаленькая (габариты устройства — 77,5×156×10,5 мм), но визуально смартфон воспринимается более тонким благодаря 4-мм металлической окантовке по всему периметру, служащей не только для эстетических целей, но также для механического укрепления шасси.

В целом внешний вид Zenfone MAX традиционен для линейки Zenfone: плавные закругленные углы, глянцевый ламинат передней панели, тыльная крышка из “мягкого” на ощупь матового пластика, который не выскальзывает из руки. (Есть также версии с текстурированной под кожу крышкой белого или черного цвета.) Крышка съемная, а вот размещенный под нею аккумулятор, покрывающий более половины видимой площади, — к сожалению, несъемный (заменить его, безусловно, можно, но для этого придется обратиться в сервис-центр). Здесь же, под крышкой, располагаются слоты для флэш-карты MicroSD

ёмкостью до 64 Гб и двух SIM-карт формата micro-SIM (работают в попеременном режиме), устанавливать и извлекать которые можно без труда — батарея этому никак не мешает.

Установленный в Zenfone MAX процессор — Snapdragon 410 MSM8916 с тактовой частотой 1,2 ГГц — оче-

видный компромисс в пользу все той же автономности. Это первый 64-рядный процессор Qualcomm на четырёх ядрах Cortex-A53 и со встроенным 450-МГц графическим контроллером Adreno 306. По нынешним меркам его производительность никак не назовешь рекордной. Скорее это достойный середнячок со сбалансированными мощностью и энергопотреблением, весьма популярный и у многих других производителей мобильных устройств.

С учетом главного целевого преимущества смартфона вполне оправданным представляется применение в нем экрана на базе IPS-матрицы с разрешением 1280×720 пикселей (а не Full HD и тем более не WQHD). Факт остается фактом — даже при размере экрана 5,5 дюйма по диагонали, как в данном случае, этого разрешения вполне достаточно для большинства приложений, но при этом экран потребляет меньше энергии и обходится дешевле. К плюсам экрана



Смартфон ASUS Zenfone MAX с упаковкой

рекомендовано заряжать устройство не менее 10 ч). Средний срок службы батареи при типичном режиме эксплуатации составляет порядка 3—5 лет.

При переходе в режим питания от батареи встроенный преобразователь Back-UPS BX650LI-GR генерирует напряжение ступенчато-аппроксимированной синусоидальной формы с действующим значением порядка 230 В. Типичное время переключения ИБП в аварийный режим питания от батареи при рабочей частоте сети 50 Гц составляет примерно 4 мс, максимальное — около 6 мс. В аварийном режиме при полной нагрузке заряда батареи хватает примерно на 1,1 мин, при меньшей нагрузке это время соответственно увеличится.

ИБП Back-UPS BX650LI-GR — это простое в эксплуатации устройство, обеспечивающее стабилизацию и защиту питания подключенного оборудования в автоматическом режиме. Оно не предусматривает использования управляющего ПО PowerChute, но тем не менее ряд базовых функций управления и оповещения с помощью звуковых сигналов и светодиодной индикации можно настроить кнопкой на передней панели. Различное сочетание прерывистых или постоянных звуковых и визуальных сигналов оповещает об изменениях режима работы, перегрузке, перегреве, переходе на питание от батареи, слишком малом заряде батареи или ошибке зарядного устройства. Таким образом, от пользователя потребуются только внимательно ознакомиться с инструкцией по эксплуатации, а впоследствии не пропустить сигналы, информирующие о том, что устройство по каким-либо причинам не может выполнять свои функции и нужно принять те или иные меры, чтобы быть уверенными — питание вашего оборудования надежно защищено.

Zenfone MAX также относится к большому запасу яркости (до 450 нит) и широкие углы обзора (до 178°). Экран заламинирован по технологии ASUS TrueVivid Full Screen Lamination и защищен стойким к царапинам стеклом Corning Gorilla Glass 4 с олеофобным покрытием, а в режиме повышенной чувствительности позволяет управлять устройством и в перчатках.

Смартфон Zenfone MAX имеет 2 Гб оперативной памяти LPDDR3 и 16 Гб встроенной памяти, что приемлемо для многих пользователей. А набор интерфейсов у него вполне современный: Wi-Fi 802.11n с поддержкой Wi-Fi Direct; Bluetooth 4.0; радиомодем UMTS/LTE с поддержкой сетей GSM 900/1800/1900, 3G, 4G LTE, LTE-A Cat. 4. Также имеется полный набор средств для навигации, включая поддержку GPS, ГЛОНАСС, BeiDou и функцию A-GPS.

Встроенная основная 13-Мп камера смартфона снабжена пятиэлементным объективом с диафрагмой f/2.0 и дополнена двухцветной вспышкой. Она поддерживает запись MPEG4-видео в качестве до 1080p/30 кадров в секунду и 720p/60 кадров в секунду, а в режиме фотосъемки позволяет делать снимки при низкой освещенности с полным доступом к ручным настройкам экспозиции. Пользователю также предлагается ряд интересных творческих режимов для автоматического создания GIF-анимаций, панорам, миниатюр и т. д., а благодаря малому времени лазерной автофокусировки (0,03 с) вы не упустите хороший кадр. Фронтальная 5-Мп камера для селфи, видеозвонков и видеоконференций поддерживает функцию автоматического повышения качества изображения при плохом освещении.

Функционирует устройство под управлением уже не новой Android 5.0, но дополненной удобной фирменной оболочкой ZenUI 2.0 образца 2015 г. В предустановленной прошивке уже при-

“Терн”: от BI к углубленной аналитике

Компания “Терн”, ведущий поставщик аналитических решений на российском ИТ-рынке, отмечает в этом году свое 25-летие. Она одной из первых в нашей стране начала развивать направление бизнес-анализа и за прошедшие годы приобрела более 500 клиентов. Долгое время компания была единственным партнером таких известных вендоров, как Business Objects и KXEN. После поглощения их корпорацией SAP “Терн” получила высший партнерский статус лидера мирового рынка ERP-систем. Год назад ею было заключено партнерское соглашение с одним из лидеров рынка углубленного бизнес-анализа — Tibco Software. На прошедшей недавно в Москве очередной конференции “Терна” был представлен весь спектр решений, предлагаемых “Терном” своим заказчикам. О современном состоянии рынка бизнес-аналитики, особенностях нынешней экономической ситуации в России и стратегии развития “Терна” рассказывают генеральный директор компании **Екатерина Лозовая** и региональный менеджер Tibco Software в России **Игорь Бабич**, также принявший участие в прошедшей конференции.



Екатерина Лозовая

Здесь все более востребованы технологии Big Data и средства быстрой обработки больших массивов в оперативной памяти.

ИГОРЬ БАБИЧ: Аналитика сегодня существует не сама по себе — это, как правило, важная часть более широкого ИТ-решения. Количество используемых на предприятиях информационных систем растет, их необходимо друг с другом соединить и интегрировать, обеспечив общим аналитическим инструментарием, и с его помощью принимать решения о покупках или продажах, маркетинговых акциях, тарифных планах и т. д. Есть целый ряд задач, которые система Tibco Spotfire решает лучше всех. Представим себе, что в нашем массиве данных наблюдаются некие сильные “выбросы”, не укладывающиеся в рамки статистической погрешности. Руководители бизнеса хотели бы как можно быстрее обнаруживать такие выбросы, понимать, с чем они связаны (будь это результат маркетинговой акции или вероятного мошенничества), и принимать правильные управленческие решения. Во многих компаниях востребованы задачи бизнес-аналитики по построению “портрета” клиентов и прогнозированию их оттока.

На протяжении многих лет ваша компания предлагает российским заказчикам инструменты традиционного BI (SAP Business Objects) и углубленной аналитики (KXEN). Есть ли в арсенале “Терна” средства для реализации облачных аналитических сервисов, мобильных решений и обработки больших данных? Каков спрос на подобные решения в нашей стране?

Е. Л.: За последние три года спрос на них вырос колоссально. Компании все чаще размещают данные и аналитические сервисы для их обработки в облаке. Недавно мы завершили такой проект в российском подразделении англо-шведской фармацевтической компании AstraZenica, в рамках которого аналитическая система Business Objects раз-



Игорь Бабич

вернута на платформе СУБД Oracle в облаке Amazon Web Services. Для интеграции исходных данных из восьми источников (включая IMS Health) применяется ETL-инструмент Informatica, а в качестве клиентов служат как стационарные, так и мобильные устройства. Аналогичная архитектура используется и головным офисом международной AstraZenica. Облачные решения для российских компаний требуют более тщательной проработки вопросов безопасности и защиты данных. Следствием этого является определенная осторожность отечественных заказчиков, но, думаю, в недалеком будущем она уйдет: технологические средства и нормативная база для этого уже имеются.

Спрос на мобильные решения со стороны клиентов “Терн” тоже очень велик, и он растет с каждым годом. Работа на мобильном устройстве в определенных ситуациях очень удобна и практически не требует дополнительного обучения. Как ни странно, первыми повышенный интерес к мобильным решениям проявили организации из госсектора: подобные решения требовались руководителям таких организаций для контроля текущей деятельности и оперативной работы с документами. Сейчас наибольший спрос наблюдается со стороны банков, телеком-операторов, ритейла. Менее активны промышленные предприятия, особенно те, что опасаются утечки конфиденциальной информации.

В последние годы руководством страны взят курс на импортозамещение и более широкое использование СПО. В какой мере для решения указанных задач подходят программные средства вашего относительно нового партнера — компании Tibco Software?

И. Б.: В портфеле Tibco Software отдельные продукты категории Open Source есть только в линейке купленной нами в 2014 г. компании Jaspersoft. Мы не считаем, что в корпоративном сегменте будущее за этой

моделью создания приложений. Если говорить о ценовом факторе, то довольно часто бесплатной бывает только базовая версия ПО, а важные для корпоративного применения функции продаются за деньги. И прежде чем делать ставку на Open Source в плане импортозамещения, нужно тщательно проанализировать все достоинства и недостатки подобных продуктов, а также риски, связанные с их применением в долгосрочной перспективе. Не исключено, что в каких-то случаях аналитические решения Open Source окажутся вполне приемлемыми для России.

Е. Л.: Насколько я понимаю, импортозамещение не сводится к полной замене зарубежного ПО. Ведь допускаются и комплексные импортозамещающие решения, если стоимость используемых в них зарубежных компонентов не превышает определенного процента. Скажем, мы предлагаем сегодня своим заказчикам такое OEM-решение “Терн-Аналитика”, в котором наряду с лицензиями на проприетарное ПО Business Objects и Tibco Spotfire они получают разработанные в “Терн” и учитывающие российскую специфику отраслевые модели хранилищ данных, семантику, цепочки загрузок ETL, преднастроенные отраслевые отчеты и информационные панели, услуги по сопровождению внедренной системы и обучению пользователей. На решение получен государственный сертификат. Не менее важно то, что наши специалисты, внедряющие “Терн-Аналитику”, хорошо разбираются в отраслевой и регуляторной специфике бизнеса отечественных компаний. По сути в “Терн-Аналитике” сосредоточен весь опыт нашей многолетней деятельности на местном рынке. Заказчикам безразлично и то, что лицензии продуктов, входящих в состав “Терн-Аналитики”, обходятся им существенно дешевле.

Не дублируют ли друг друга BI-решения разных поставщиков, имеющиеся в портфеле “Терна”? Как вы позиционируете их для своих заказчиков?

Е. Л.: Скорее все эти аналитические решения дополняют и взаимно обогащают друг друга. Вот характерный пример: специалисты “Терна” разработали ПО для обеспечения взаимодействия Business Objects и Tibco Spotfire. С его помощью гиперкуб Business Objects с той или иной выборкой данных легко передается в Tibco Spotfire, где происходит более углубленный анализ такой выборки с использованием статистического анализа или методов прогнозирования на основе временных рядов, кластеризации, регрессии и т. д.

И. Б.: Один из наших клиентов в ОАЭ даже использует Spotfire для анализа в реальном времени данных, собираемых с датчиков газовой турбины, с тем чтобы заранее прогнозировать вероятные проблемы и осуществлять профилактические ремонты, не дожидаясь выхода турбины из строя.

▶ существует ряд полезных утилит (в частности, Power, ZenLink, ASUS Sync, Kids Mode, ASUS Splendid) и приложений (File Manager, Trend Micro Security, Quick Memo, One Hand Mode и What’s Next), а также программ для творческих задач (PhotoEffects, SnapView, ZenCircle, PhotoCollage, MiniMovie и др.). Преимуществом ZenUI 2.0 также является поддержка ряда полезных функций, таких как, например, вывод смартфона из режима сна двойным постукиванием по экрану и настройки для удобного использования устройства одной рукой. Для тех же, кто стремится использовать новейшие версии мобильных ОС, подчеркнем, что Asus включила ZenFone Max в перечень моделей, операционная система которых во II кв. 2016 г. будет обновлена до Android 6.

После ежедневного использования на протяжении пары недель в качестве основного смартфона для работы и развлечений ASUS Zenfone MAX оставил весьма положительные впечатления. Выглядит аппарат достойно, в руке лежит хорошо.

Производительности процессора и графического адаптера ASUS Zenfone MAX вполне достаточно для повседневной работы с почтой, документами и приложениями, а также для просмотра видео и простых казуальных игр. Его аккумулятор обеспечивает завидную для любого Android-устройства автономность. Кстати, смартфон можно использовать и для подзарядки в походных условиях других мобильных устройств — производитель это тоже предусмотрел.

Переход...

◀ ПРОДОЛЖЕНИЕ СО С. 10

PC Week: Здесь явно возникает тема хранения электронных документов. Как оно реализуется у вас сегодня?

С. Т.: Это довольно болезненный вопрос. Пока архив находится у наших операторов, они несут ответственность за него. Но нас такой порядок не очень устраивает — мы хотели бы иметь собственный архив, который имел бы соответствующую юридическую значимость. Решение этого вопроса — также одна из приоритетных для нас задач.

PC Week: Можно ли ожидать каких-то решительных действий со стороны регулятора — Федеральной налоговой службы, которые изменят ситуацию на рынке ЭДО?

С. Т.: ФНС уже более пятнадцати лет является главным инициатором и драйвером перехода на электронные формы делового взаимодействия, и, думаю, в недалеком будущем от нее вполне можно ожидать перевода ЭДО из возможного варианта в обязательный, как она проделала уже с налоговой отчетностью. У ФНС есть очень большой интерес к этому, ведь переход на электронные форматы позволяет не только снизить собственные трудозатраты, но и, что намного важнее, повысить собираемость налогов, улучшить прозрачность деловых процессов и перейти на качественно новый уровень контроля за ними.

PC Week: Спасибо за беседу.

Информационные технологии как инструмент выживания банков

ЕЛЕНА ГОРЕТКИНА

Нынешний год не обещает быть легким для российских банков. Остаются прежние проблемы в виде санкций, нехватки капитала, роста просрочки и повышенных отчислений в резервы, к ним добавляется более жесткое регулирование. Так, агентство Moody's ухудшило прогноз падения российского ВВП с 1,5 до 2,5% и прогнозирует, что Центробанк РФ отзовет лицензии у каждого десятого банка.

В таких условиях банкам предстоит трудная борьба за выживание, успешность которой во многом определяется эффективностью рабочих процессов. Важную роль в поддержке последних играют ИТ. Какими будут приоритеты банков в области информатизации в этом году? Какие решения может предложить сегодня ИТ-индустрия? На эти и другие вопросы отвечают эксперты, представляющие поставщиков ИТ-продуктов для финансового сектора и системных интеграторов.

Новая реальность — новые задачи

Несмотря на экономический кризис, банки не отказываются от развития своих ИТ-систем, но их приоритеты меняются. Впрочем, многие эксперты стараются избежать слова «кризис», считая, что оно всем уже надоело и к тому же не очень уместно говорить об этом, когда правила игры относительно стабильны, пусть и не позитивны.

По их мнению, финансовая сфера, как и многие другие отрасли экономики, живет в новой реальности и уже осознает это. «Задачи можно сформулировать так: быстро, еще быстрее и недорого. Проблемы не сильно трансформировались относительно ситуации в канун кризиса, они просто стали требовать более быстрых и эффективных решений», — считает Александр Сиркин, директор по развитию бизнеса компании IBS.

С ним согласен Юрий Корешков, руководитель управления по работе с банками Центра программных решений компании «Инфосистемы Джет», который отметил, что сейчас мы все чаще говорим о новой реальности и пора к этому привыкнуть. В ИТ-сфере тоже начинается новая реальность, для которой характерны две тенденции: во-первых, фокус на снижение стоимости владения ИТ-системами, в том числе желание сэкономить на классической организации ИТ-сервисов; во-вторых, стремление к повышению гибкости ИТ как на уровне бизнес-приложений, так и на уровне инфраструктуры за счет внедрения новых технологий разработки, управления изменениями, развития новых, более гибких и удобных сервисов для клиентов и т. п.

При этом многие банки переходят на режим максимальной экономии. «Они рассматривают вложения в информатизацию под лупой, давая ход только проектам, жизненно важному его бизнеса или повышающим его эффективность. На сомнительные или необязательные задачи бюджеты не выделяются. Даже рост мощностей для санации, апгрейд или дополнительный клиентский сервис анализируются с позиции необходимости», — пояснил Андрей Завада, директор по продажам ГК ХОСТ.

Это связано с тем, что ИТ-бюджеты большинства российских банков сократились на 20—30%, прежде всего из-за падения курса рубля. Лишь в некоторых небольших частных банках, исчисляющих ИТ-бюджеты в валюте, расходы на ИТ практически не снизи-

лись. По оценке Алексея Шалагинова, директора по отраслевым решениям департамента ИТ и ЦОД компании Huawei в России, в 2015-м ИТ-расходы российских банков упали по сравнению с 2013-м почти вдвое, до уровня немногим более 1 млрд. долл. В текущем году роста инвестиций в ИТ в банковской сфере не предвидится, лишь в 2017-м, при удачном стечении обстоятельств, может быть небольшой рост. Восстановления же ИТ-расходов в банках до уровня 2013 г. не следует ожидать ранее 2020 г.

«В таких условиях развитие ИТ в банковской отрасли представляется достаточно проблематичным. Следовательно, первоочередной задачей является оптимизация расходов на ИТ-обеспечение и превращение банковских ИТ-систем из обслуживающих в элемент генерации ценности», — считает Алексей Шалагинов.

Клиентский рынок не растет, поэтому между банками идет ожесточенная борьба за имеющихся клиентов. Чтобы сохранить своих и переманить чужих, им надо предлагать не только что-то «очень вкусное», но и быть в этом первыми. Поэтому резко сократилось время на выпуск релиза любой системы или продукта — с месяцев до недель. При этом цена не должна быть высокой, так как лишних денег ни у кого нет и низкая себестоимость системы или услуги актуальна как никогда.

Однако зачастую сокращение расходов влечет за собой снижение качества продукта. Банки это понимают. По словам Натальи Педчик, директора по работе с ключевыми клиентами подразделения IT Business компании Schneider Electric, в условиях кризиса наряду со снижением затрат на внедрение и эксплуатацию возрастают требования к уровню надежности и безопасности банковской информатизации. В связи с этим растет тенденция к централизации, стандартизации и обеспечению масштабируемости банковской ИТ-инфраструктуры, цель которой — оптимизировать стоимость владения и повысить скорость внедрения новых услуг.

В русле мировых ИТ-тенденций

Хотя рост мирового ВВП замедляется, банки всего мира наращивают инвестиции в ИТ. По прогнозу IDC, в 2016-м банковские ИТ-расходы составят 275 млрд. долл., а затем будут ежегодно расти на 4,5% в течение пяти лет. При этом IDC отмечает, что наиболее сильно на ИТ-бюджеты банков влияют основные компоненты цифровой трансформации, такие как облачные и мобильные технологии, Big Data и аналитика (BI).

В нашей стране современные технологические тренды тоже актуальны, так как, несмотря на все проблемы, банкам нужно оптимизировать расходы. Так, Александр Сиркин считает, что облака и аутсорсинг услуг или процессов позволяют снизить затраты на собственные структуры на десятки процентов, а иногда и в разы.

Что касается мобильности, то по общему мнению экспертов, она уже давно не является каким-то модным трендом. Это суровая реальность и обязательное требование клиентов. Нравится это банкам или нет, но они идут в Сеть, так как за этим будущее. Как отметил Алексей Шалагинов, сейчас для банковской отрасли наиболее актуально повышать мобильность бизнеса и представлять услуги в режиме онлайн, прежде всего через мобильные сети. По прогнозу Алексея Шалагинова, в ближайшие два-

три года среднегодовой рост расходов на банковскую «мобилизацию» составит 10—12%.

При этом банки применяют разные подходы. У многих из них есть собственные разработки, а кто-то предпочитает покупать готовые приложения. «Но в целом основные игроки понимают, что мобильные приложения — не дань моде, а очевидная потребность. При постоянном увеличении их функционала среди ключевых требований на первом месте остаются простота использования и безопасность», — констатирует Константин Савченко, руководитель отдела поддержки и развития продаж корпоративного ПО компании Ахофт.

Поскольку мобильные услуги уже не являются особым конкурентным преимуществом, банкам приходится уделять больше внимания изучению других потребностей клиентов и двигаться в сторону повышения персонализации услуг. Пользователи оставляют в цифровой среде огромное количество информации. Но как извлечь из нее пользу для бизнеса? Здесь на первый план выходят технологии Big Data и BI, которые способны значительно повысить отдачу от банковских продуктов.

Правда, отметил Константин Савченко, некоторые компании еще только стоят на пороге осмысления предстоящей работы, однако практически все понимают, что данные, которые, по сути, сейчас «лежат под ногами», являются необходимыми для роста прибыли, более качественной работы с клиентами, обеспечения внутренней и внешней безопасности.

Однако, по мнению Алексея Шалагинова, реальные внедрения «больших данных» требуют больших инвестиций, а это пока проблематично. Тем не менее он полагает, что несмотря на общий тренд снижения ИТ-расходов, затраты на BI и Big Data будут расти в ближайшие два-три года быстрее других инвестиций в финансовые технологии в целом.

В числе других передовых технологических трендов отметили так называемые видеобанкоматы, которые способны предоставить гораздо больший спектр услуг, чем обычные банкоматы, и применение Интернета вещей, например для отслеживания производственного цикла клиентов или для платежных сервисных устройств, которые сами совершают финансовые транзакции.

Таким образом, банки по-прежнему идут в авангарде освоения технологий. Однако, как справедливо заметил Андрей Завада, важно не то, что они используют, а то, как используют, насколько грамотно и гармонично эти решения вписаны в цикл банковских операций: «Технологии — не волшебная палочка, а просто инструмент. Компьютер используют и для отправки ракет в космос, и для лайков в соцсетях».

С этой точки зрения эксперты рекомендуют использовать перечисленные технологии вместе, поскольку они сильно взаимосвязаны между собой и в совокупности могут способствовать повышению эффективности. Например, у любого банка есть огромное количество данных, которые необходимо хранить, а следовательно, приходится увеличивать издержки на аппаратные ресурсы. Если же перенести эти данные в облака, это позволит оптимизировать затраты на их хранение, сэкономив на закупке и обслуживании оборудования. Обработка их с помощью технологий машинного обучения сокращает время, а применение BI-инструментов позволяет делать раз-

Наши эксперты



АНДРЕЙ ЗАВАДА,
директор по продажам,
ГК ХОСТ



АЛЕКСЕЙ КАТРИЧ,
заместитель генерального
директора, «Техносерв
Консалтинг»



ЮРИЙ КОРЕШКОВ,
руководитель управления
по работе с банками,
Центр программных
решений компании
«Инфосистемы Джет»



НАТАЛЬЯ ПЕДЧИК,
директор по работе
с ключевыми клиентами,
подразделение IT Business
компании Schneider
Electric



КОНСТАНТИН САВЧЕНКО,
руководитель отдела
поддержки и развития
продаж корпоративного
ПО, Ахофт



АЛЕКСАНДР СИРКИН,
директор по развитию
бизнеса, IBS



РУСТЕМ ТУРСУМБАЕВ,
архитектор систем ИБ,
ГК «Компьюлинк»



АЛЕКСЕЙ ШАЛАГИНОВ,
директор по отраслевым
решениям департамента
ИТ и ЦОД, Huawei
в России

личные аналитические выборки и представления обработанных данных, а затем на их основе через мобильный банкинг целенаправленно предлагать клиентам новые продукты и услуги. Каждый шаг на данной цепочке по-своему увеличивает эффективность банковской деятельности.

Комплексный аутсорсинг — лед тронулся

В мире усиливается тенденция передачи части или всех ИТ-операций на аутсорсинг профессиональным провайдерам ИТ-сервисов ради оптимизации затрат и рисков. До последнего времени российские банки с опасением относились к такой возможности. Но сейчас в связи с новой реальностью такое положение начинает меняться.

По мнению экспертов, многие коммерческие банки уже переходят на аутсорсинг, хотя и осторожно. Так, Андрей Завада отметил, что банки остаются консерваторами в отношении безопасности и не любят давать другим доступ к своей инфраструктуре: «В некоторых наших

► сервисных контрактах прямо прописано, что работы проводятся под наблюдением специалиста банка».

Тем не менее лед тронулся. Если раньше банки просто отмахивались от идеи аутсорсинга, то сейчас картина другая. Так, по мнению Юрия Корешкова, кризис повернул банки в сторону сервисных моделей, ориентированных на поддержку процессов, не относящихся к профильной деятельности банка.

Правда, считает Александр Сиркин, о победе комплексного аутсорсинга говорить еще рано, но банки все чаще отдают на аутсорсинг поддержку ИТ-систем и, что самое главное, получают от этого прямую финансовую выгоду без потери уровня сервиса. Все это вместе с учетом опыта развитых финансовых систем других стран дает основания полагать, что комплексный аутсорсинг не за горами.

Распространению аутсорсинга способствует и ситуация на ИТ-рынке, где в последнее время появилось несколько компаний, предоставляющих ИТ-услуги, в частности в области безопасности. «Например, услуга SOC является для многих единственным способом получить качественный анализ информационных событий, не инвестируя большие деньги в инфраструктуру и специалистов. Такая тенденция будет и дальше развиваться, так как количество и качество атак растет, а значит, обслуживание ИТ- и ИБ-систем за счет собственных ресурсов для многих заказчиков будет обременительным», — уверен Константин Савченко.

Импортозамещение — не самоцель

Относительно развития импортозамещения в банках мнения экспертов разделились. Одни считают, что ситуация меняется, правда, многое зависит от типа систем и задач. «АБС и процессинговые системы и так были российскими, а что касается углубленной аналитики, рисков, антифрода и ряда других областей, где критично наличие сложных математических моделей, алгоритмов и других разработок, то таких отечественных систем де-факто нет и создать их за несколько месяцев или даже пару лет крайне сложно», — пояснил Александр Сиркин. Поэтому здесь быстрого прорыва не случилось и ждать его не стоит. Зато в области инфраструктурных решений на рынке довольно быстро появились отечественные вычислительные платформы, которые вполне успешно конкурируют с дорогими западными продуктами.

По мнению других экспертов, общий курс на импортозамещение пока не оказывает заметного влияния на информатизацию банков, хотя сама по себе эта тема и вызывает у них интерес. Например, в центр компетенций ГК ХОСТ по свободному ПО уже выстроилась очередь из желающих посмотреть работу решений вживую. «Но от интереса до реальных проектов пока далеко. Банки только сравнивают плюсы и минусы перехода на отечественные продукты или свободное ПО, считают совокупную стоимость владения, оценивают риски», — поделился опытом Андрей Завада.

Такого же мнения придерживаются и Наталья Педчик, которая отметила, что хотя банки серьезно рассматривают стратегию импортозамещения, в том числе и в сфере ИТ, но на крупных инвестиционных проектах предпочитают внедрять оборудование известных, проверенных мировых производителей.

В перспективе, считает Константин Савченко, тема импортозамещения будет переживать несколько циклов: от восторженных идей заменить все на «наше» до осмысления абсурдности этой затеи и поиска локальных ниш и сегментов, в которых мы сможем преуспеть или хотя бы не быть аутсайдерами: «Все мы знаем удачные примеры российских решений, которые заказчики выбирали осознанно по итогам сравнения с отечественными

ми и зарубежными аналогами. Хочется верить, что банки и другие компании по-прежнему смогут руководствоваться коммерческой целесообразностью, а не местом происхождения решения».

Таким образом, эксперты считают, что стратегия импортозамещения и импортозависимости не является самоцелью. Она должна рассматриваться только в рамках достижения общей цели снижения операционных и стратегических рисков, связанных с ИТ и ИБ, таких как риски неконтролируемого внешнего деструктивного воздействия на банковские ИТ. Поэтому оптимальным является рассмотрение каждого случая в отдельности, когда при реализации информационных систем и ИТ-инфраструктуры банковской организации учитывается вся совокупность рисков.

Open Source в банках — плюсы и минусы

Сейчас доминирующей моделью в области ИТ становится Open Source. По данным компании Black Duck, полученным в результате опроса 1300 компаний из разных стран мира, 65% организаций использует открытый софт для разработки, а 55% — применяет в своей ИТ-инфраструктуре. Правда, неясно, сколько среди них банков. Ведь традиционно финансовый сектор с некоторой осторожностью относится к открытому ПО.

Однако в России интерес к Open Source подогревается нашими национальными особенностями, такими как общий тренд на импортозамещение и значительное подорожание западного проприетарного ПО. По мнению Андрея Завады, многие банки уже используют Open-Source-разработки в ИТ-ландшафте, причем и в системной, и в прикладной частях.

С ним согласен Алексей Шалагинов, который отметил, что Open Source оказывается достаточно привлекательным для большого числа ИТ-директоров, в том числе и из банковской сферы: «Внедрение открытых решений, например Sugar CRM, в некоторых российских коммерческих банках уже привело к сокращению ИТ-расходов более чем в три раза по сравнению с использовавшимися ранее проприетарными решениями».

По его мнению, к другим преимуществам такого подхода относится ускорение некоторых операций (например, по обслуживанию клиентов), уменьшение затрат на обучение персонала и новые возможности для перекрестных продаж в банках.

Юрий Корешков тоже с оптимизмом смотрит на перспективы Open Source, считая, что в ближайшее время стратегия замены зарубежного ПО на российские разработки и Open Source будет набирать обороты: «Банки уже начали строить свои ИТ-системы на основе решений и компонентов с открытым кодом, стараясь найти возможность отказаться от дорогостоящей поддержки зарубежных продуктов».

Однако у Open Source есть не только сильные стороны. Так, при оценке возможности использования открытых решений не следует забывать о проблеме уязвимости такого ПО. В случае проприетарных решений известно, кто отвечает за устранение проблем, а при использовании Open Source все такие риски возложены на банковские организации или компании, осуществляющие внедрение.

Кроме того, следует учитывать и скрытые расходы по созданию неоптимальных решений, но максимально кастомизированных для сложившейся в организации текущей ситуации. «Все сильные и слабые стороны перехода на решения стека Open Source еще не просчитаны. Это аналог задачи, которую банки до сих пор так и не решили: что лучше — внедрить иностранную систему, воплощающую международный опыт, или российскую с максимально проработанной локальной спецификой», — отмечает Алексей Катрич, заместитель генерального дирек-

тора компании «Техносерв Консалтинг».

Возможно, поэтому, несмотря на все перечисленные выше проблемы в банковской информатизации, особого бума в отношении открытого софта пока не наблюдается. «Крупные российские банки с осторожностью относятся к Open-Source-решениям и не стремятся использовать их в своей деятельности», — констатирует Наталья Педчик.

Но в перспективе такое отношение может измениться. На это есть причины, которые привел Константин Савченко: «Модель Open Source эволюционирует, появляются новые игроки, растет кооперация, возникают альянсы крупных производителей, расширяются сегменты присутствия — все это позволяет быть уверенными в перспективности модели Open Source, в том числе в весьма конкурентной банковской среде».

Спасение от хакеров

Банковский сегмент традиционно является целью атак со стороны злоумышленников. Только за период с октября 2015 г. по март 2016-го российские банки, по данным ЦБ, потеряли 2 млрд руб. из-за хакерских атак. И несмотря на развитие законодательства в области ИБ и на меры, которые принимают сами банки, ситуация не улучшается.

По мнению некоторых экспертов, данные ЦБ — лишь верхушка айсберга. На самом деле потери гораздо больше. Рустем Турсунбаев, архитектор систем ИБ ГК «Компьюлинк», объяснил это тем, службы безопасности банка легко проверяют транзакции на большие суммы, но не могут отследить среди миллионов операций нелегитимные транзакции на маленькие суммы, потому эти данные не попадают в статистику.

Что касается причин плачевной ситуации с ИБ, то, по мнению экспертов, их немало, и одна из них связана с самими банковскими ИТ. Ведь для оперативного и прозрачного взаимодействия с пользователями современный банк использует систему «банк — клиент» в виде веб-портала, доступ к которому может получить каждый. Эти сайты взаимодействуют с серверами, в том числе осуществляющими финансовые транзакции и расположенными в сети банка. Данная взаимосвязь и является одним из возможных способов доступа к материалам банка.

Немаловажную роль играет прословутое человеческий фактор: «Все чаще хакеры используют технологию фишинга, рассылая информационные письма якобы от имени ЦБ и регулятора, а во вложениях находятся зараженные файлы, при открытии которых на компьютерах сотрудников банков начинается подспудная вредоносная деятельность», — отмечает Алексей Шалагинов.

Еще одна причина, по мнению Алексея Катрича, заключается в том, что уровень подготовки специализированных хакерских компаний сегодня значительно превосходит возможности банков содержать специализированные подразделения для противодействия атакам.

Такой же точки зрения придерживается Андрей Завада: «Вместе с уровнем защиты растет и уровень атак, и злоумышленники выигрывают эту гонку. Какой бы комплексной не была защита, в ней найдутся «дыры». Чаще всего слабым звеном оказывается человек. Это подтверждают и удачные атаки с помощью вируса Buhtrap».

Недофинансирование обучения сотрудников также играет на руку хакерам. «Зачастую приобретаются системы за сотни тысяч или миллионов долларов, а их эксплуатация осуществляется без должной подготовки кадров. В решении этого вопроса есть существенный потенциал для улучшения защиты компаний», — считает Константин Савченко.

В частности, эксперты рекомендуют банкам применять хорошо зарекомендовавший себя опыт борьбы с подобным

явлением в Австралии, где для всех сотрудников банков и госорганов введены правила «ИТ-гигиены», включающие примерно 40 элементарных действий по ИБ. Оказалось, что реализация только первых шести пунктов перечня уже позволяет сократить ущерб на 90%. Нелишне будет перенять этот опыт и в России вкупе с более интенсивным применением ИБ-систем.

Кроме того, стоит также обратить внимание на технологию распределенной верификации блоков транзакций блокчейн. Эта технология отличается тем, что в ней практически невозможно провести злонамеренную транзакцию, включая и почтовую рассылку. Она будет сразу же обнаружена, и ее источник будет верифицирован с точностью до IP-адреса. По словам Алексея Шалагинова, опыт использования блокчейн сейчас пристально изучают ведущие российские банки.

Могут пригодиться и услуги компаний, специализирующихся в сфере ИБ: банки должны следовать первоочередным мерам противодействия и защиты информационной контура банка, а профессиональные компании — производить онлайн-охрану и превентивный аналитический мониторинг информационных объектов банка. «Постоянное участие специального оборудования, искусственного интеллекта и опытных специалистов дает возможность предотвратить потенциальные угрозы взлома и финансовые потери», — считает Алексей Катрич.

Но главным, уверен Рустем Турсунбаев, является то, что меры по повышению эффективности защиты банковской сферы должны быть комплексными: начиная с построения правильной безопасной архитектуры системы, обеспечения круглосуточного мониторинга работы ее компонентов и использования специализированных антифрод-систем и заканчивая систематическим повышением уровня знаний обслуживающего персонала.

Кибербезопасность...

◄ ПРОДОЛЖЕНИЕ СО С. 9

Причем фирма может быть не виновата. Все может делаться без ее ведома.

PC Week: Как выглядит организационная структура обеспечения кибербезопасности в РЖД?

Б. М.: Основным госрегулятором выступает ФСТЭК РФ. В ОАО «РЖД» создан и работает Экспертный совет по кибербезопасности, возглавляемый старшим вице-президентом ОАО «РЖД» — главным инженером компании. Экспертный совет определяет основные направления работы Центра кибербезопасности ОАО НИИАС. Кроме этого есть аккредитованный ФСТЭК орган (центр) по сертификации ОАО НИИАС, а также аккредитованные на безопасность информации испытательные лаборатории. И еще пул из 10–15 фирм, с которыми мы давно сотрудничаем и чья компетенция не вызывает у нас сомнения.

PC Week: Какие нужно предпринимать меры для противодействия возможным кибератакам?

Б. М.: Нужно развивать отечественное производство, осуществлять легендерование и централизацию закупок. Желательно иметь альтернативных поставщиков комплектующих и ПО для критических компонентов МПСУ и соответственно возможность альтернативной закупки, прежде всего в странах Таможенного союза и БРИКС. Ну и необходимо обязательно обеспечивать входной контроль, тестирование комплектующих и ПО. Сейчас об этом практически забыли, а в советские времена входной контроль был 100%-ным. Но и сегодня есть организации, которые этим занимаются.

Индустриальный Интернет в энергетике России

НИКОЛАЙ НОСОВ

Сейчас у нас много говорят и пишут о необходимости перехода к новой экономике, основанной на использовании киберфизических систем и технологий Интернета. Энергетика — одна из самых перспективных областей внедрения Индустриального Интернета вещей (Industrial Internet of Things, IIoT). Что делается в энергетике в области IIoT сегодня? И что будет делаться завтра? Попробуем разобраться.

ИНТЕРВЬЮ Инициативы по реорганизации у нас в стране идут, как правило, сверху. Поэтому начнем с одного из ключевых ведомств. На наши вопросы ответил Евгений Грабчак, директор департамента оперативного контроля и управления в электроэнергетике Министерства энергетики РФ.

PC Week: Для чего нужен Индустриальный Интернет государству в целом и вашему ведомству в частности?

ЕВГЕНИЙ ГРАБЧАК: Государству и Минэнерго России как ответственному за госфункцию по развитию отрасли интересно обеспечить необходимый уровень автоматизации, который позволил бы всем получить свои преимущества от ее внедрения. Для нас это мониторинг и аналитика. Государство не собирается вмешиваться в деятельность субъектов, но по результатам аналитики может вносить изменения с точки зрения законодательной базы и давать стратегические посылы для развития отрасли. Энергетика относится к стратегическим отраслям, влияющим на национальную безопасность, и нам нужны ее оптимизация, унификация и более понятная логистика производственных процессов.

PC Week: Энергетический комплекс состоит из сбытовых, генерирующих и транспортных компаний. Вы контролируете все три составляющие?

Е.Г.: Мы контролируем энергетику в целом. В сбытовых компаниях госучастия нет, оно есть в магистральном транспорте. Если речь идет о 110 кВт и выше, то это стратегическое предприятие и здесь 100%-ное государственное участие. В генерации электроэнергии мы участвуем через крупные государственные холдинги, такие как Газпромэнергохолдинг и “Интер РАО” для тепловых станций; “РусГидро” — в сфере выработки электроэнергии через гидроэлектростанции и т. д.

PC Week: У каждого участника энергорынка будет свой Индустриальный Интернет?

Е.Г.: С точки зрения рациональности нужно делать единую вертикально интегрированную систему с горизонтальными уровнями. У всех разные задачи — внутри сетей, внутри генерации, внутри сбыта. Но взаимодействие этих трех субъектов тоже ставит нам разные задачи по оптимальности режимов загрузки, по экономической эффективности, по управлению активами на макроуровне. Все компании имеют свои системы автоматизации и свои системы управления активами, которые позволяют им проводить собственную оптимизацию. Наше общее понимание сейчас разрознено и не увязано. Индустриальный Интернет в классическом варианте в электроэнергетике кое-где реализован как на макро- (на уровне управляющих компаний), так и на микроуровне. Пример микроуровня — цифровые подстанции, которые полностью обвязаны и за которыми можно и нужно наблюдать в реальном времени. И имеется система управления активами, которая пока только может своевременно собирать информацию по состоянию своих подстанций и сигнализировать оператору, когда и какой элемент цифровой подстанции нужно поменять.



Евгений Грабчак

PC Week: Что вы собираетесь делать в этом направлении?

Е.Г.: Совместно с Роснано и Ростелекомом формируем национальный проект по Индустриальному Интернету на основе пилотного проекта развития системы удаленного мониторинга и диагностики парогазовых установок. У любого оборудования есть свой жизненный цикл, и его можно отслеживать с помощью датчиков. Нам, как получателю, хотелось бы оптимизировать все ремонтные программы. И получить некую унификацию жизненного цикла оборудования, чтобы вовремя формировать заказ на поставку запчастей. Это позволит унифицировать логистические цепочки поставки, на основе пула компаний создать единую базу аварийного запаса, которая могла бы формироваться и пополняться не в зависимости от потребностей одного предприятия, а от потребностей всех компаний, расположенных рядом.

Информация о состоянии оборудования могла бы поступать в единый информационный центр, чтобы уже там искать свободную запчасть, которую можно было бы поставить оперативно и с минимальным логистическим плечом доставки.

PC Week: А что это дает государству?

Е.Г.: Здесь есть польза не только для компаний, но и для государства. Мы можем прогнозировать спрос на запчасти в целом по отрасли и передавать эту информацию в Минпромторг России. Мы формируем отраслевой заказ и имеем понимание по производителям основных элементов — когда и какой из них нужно произвести, к какому сроку, как его доставить и как эксплуатировать. Это позволит выстроить рыночную модель функционирования производителей российского оборудования, которой сейчас нет. Пока же наши производители говорят, что хотят производить, участвовать в импортозамещении, но просят гарантированного заказа. А это длинные деньги, нужны кредиты, нужна бизнес-модель. Если они не знают, будет ли рынок, то не могут инвестировать производство.

“Обвязав” всё датчиками, мы сможем анализировать — в каких случаях какое оборудование более работоспособно. Энергосистема построена на резервировании. Всегда есть вторая линия, обеспечивающая загрузку. Распределением потоков занимается системный оператор, у него есть модель распределения, которая зависит, например, от аварийных режимов. Но эта модель не интеллектуальная.

Если же у нас будет интеллектуальная модель, использующая исходные данные, данные о планируемой нагрузке и ее интенсивности, о планируемых выводах оборудования, то мы сможем оптимизировать загрузку станций с учетом затрат,

оптимизировать стоимость доставки электроэнергии для конечного потребителя и добиться минимизации стоимости электроэнергии на конечном рынке.

Индустриальный Интернет в нашем понимании помог бы провести большую оптимизацию в электроэнергетике и существенно снизить операционные затраты.

PC Week: Расскажите подробнее, какую роль IIoT мог бы сыграть в оптимизации ремонтных работ.

Е.Г.: Сроки планового ремонта в паспорте на газовую турбину определяются исходя из номинальной загрузки. Например, она должна быть загружена на 60—70% времени и тогда по паспорту будет работать десять лет. Тепловая генерация создана специально для срезания пиков и провалов потребления. Поэтому в реальности загрузка может сильно отличаться от той, что заложена производителем. С помощью Индустриального Интернета можно делать диагностику и исходя из реального положения вещей продлевать ресурс эксплуатации.

PC Week: Насколько подход “ремонт по состоянию” соответствует нашему текущему законодательству?

Е.Г.: Пока законодательно делать это нельзя. Но мы работаем в данном направлении, выпустили методологию о ремонте по техническому состоянию, которую сейчас законодательно закрепляем. Собственник сможет провести диагностику и самостоятельно продлить ресурс.

PC Week: А как еще может быть использована статистическая информация, собираемая в рамках систем IIoT?

Е.Г.: У нас много разнообразного вспомогательного оборудования: трансформаторы, системы подачи топлива, даже соединительные муфты. У каждого устройства свой ресурс и своя наработка. Если мы всё “обвяжем” датчиками и будем мониторить ситуацию, то сможем набрать статистику и провести анализ с целью оптимального выбора узлов и уменьшения ОПЕХ. Сможем понять, как собрать конструктор объекта в целом из разных узлов с минимальной стоимостью жизненного цикла.

Можно также получить информацию о наработке устройств и о стоимости жизненного цикла как единицы оборудования, так и комплекса в целом. Сможем брать данные о поведении турбины в качестве исходных для разработки собственных турбин. У нас, к сожалению, нет конструкторских бюро с серьезной аналитикой, и все попытки создания отечественных газовых турбин большой мощности пока не увенчались успехом.

PC Week: Сейчас вы используете западные газовые турбины большой мощности. Но у них ведь уже налажен сбор информации с датчиков?

Е.Г.: Да, налажен. Но вся информация уходит в дата-центры за рубежом. Они ею не делятся. У них есть сервисные контракты на эксплуатацию, которые стоят огромных денег. Стоимость жизненного цикла отечественных разработок на отечественном оборудовании как минимум на порядок ниже. Более того, когда западные компании поставляют нам оборудование, там помимо скрытых закладок есть декларируемые возможности по удаленному мониторингу и оказанию воздействий. Это представляет угрозу для национальной безопасности. Электростанции на газовых турбинах стоят в крупных городах и дают порядка 20 ГВт электроэнергии. Производители, конечно, дорожат своей репутацией, но если, например, американское правительство скажет General Electric отключить наши газовые турбины, то они их отключат. А у нас на вырабатываемой ими электро-

энергии вся оборонка и промышленность. И что мы будем делать? Все структуры взаимосвязаны. Мы не сможем с помощью только атомных и гидроэлектростанций управлять всей системой. Все маневровые мощности вырабатываются на газовых турбинах. Нашу энергосистему просто парализует.

PC Week: И что тут можно сделать?

Е.Г.: Мы можем разработать законодательно-нормативную базу, которая позволит внедрять инновации, связанные с Индустриальным Интернетом. А, кроме того, через советы директоров компаний с госучастием внедрять эту идеологию. Например, через утверждение концепции развития систем управления активами, что мы сейчас делаем в ПАО “Россети”.

PC Week: Вы уже разработали концепцию развития Индустриального Интернета в энергетике? Есть ли у вас соответствующая дорожная карта?

Е.Г.: Такой концепции у нас пока нет, и в этом основная проблема. Когда мы запускаем Индустриальный Интернет в критически важной отрасли, нам нужно понимать последствия, в первую очередь в плане безопасности. Сейчас оборудование в наших сетях на 80% — аналоговое. И с ним внешние злоумышленники — преступники, хакеры, зарубежные спецслужбы — ничего не сделают. Как работало, так и будет работать. Но эволюция идет, и даже с точки зрения оптимизации нужно переходить на цифру, делать единую сеть, единую базу. И обеспечивать межмашинное взаимодействие в рамках Индустриального Интернета.

Дорожной карты, естественно, тоже нет. До недавнего времени всё это даже не называли Индустриальным Интернетом — называли системой управления активами. И только в нынешнем году решили заниматься этим очень серьезно. Мы уже создали рабочую группу из энергетиков. Но к работам нужно привлечь Минкомсвязи и Минпромторг, чтобы создать единую целостную концепцию. А еще предстоит Индустриальный Интернет связать с пользовательским Интернетом вещей.

PC Week: Какие элементы IIoT уже работают в нашей энергетике?

Е.Г.: После аварии на Саяно-Шушенской ГЭС были проведены модернизация и реконструкция. В декабре прошлого года введена в промышленную эксплуатацию система группового регулирования активной мощности — ГРАМ. Это, по сути, взаимодействие машин между собой и систем с машинами, автоматическое регулирование загрузки гидроагрегатов в зависимости от проходящих в энергосистеме процессов. Есть параметры качества электроэнергии, один из них — частота 50 Гц. ГРАМ позволяет на основании частоты, которая получается в энергосистеме, и балансов мощностей полностью автоматически решать, сколько воды нужно пропускать через гидроагрегаты. Фактически это и есть Индустриальный Интернет. Вышла из строя тепловая станция — тут же больше воды пускается на лопатки и больше вырабатывается электроэнергии.

И еще у нас много крупных подстанций, на 110 кВт, без персонала, которые работают на основе межмашинного (M2M) взаимодействия и удаленного доступа. Пока удаленные переключения осуществляет диспетчер, но в перспективе, с внедрением Индустриального Интернета, будет реализовано автоматическое переключение режимов работы, которое обеспечит оптимальное распределение энергии и выбор оптимального пути её доставки от подстанции до ко-

ЭКОНОМЬТЕ ПРОСТРАНСТВО, СОХРАНЯЯ ПРОИЗВОДИТЕЛЬНОСТЬ!

Мини ПК Ak-Systems
на базе процессора Intel® Core™ i5.

Мощный компьютер в компактном
корпусе для высоких корпоративных
потребностей.

Intel Inside®, значит
производительные решения.



Процессор: Intel® Core™ i5-4460

Память: DDR3 1333/1600 МГц,
поддержка двухканальной памяти до 32Гб (8Гб x 4)

Графика: Intel® HD Graphics 4600

Аудио: Realtek ALC892, 7.1 channel HD-Audio

Порты ввода/вывода: USB 3.0 x 4, USB 2.0 x 8,
разъем для микрофона и наушников,
HDMI, DVI-I, eSATA

Размеры: 33,2 x 21,6 x 19,8 см



- ▶ **Адаптивная производительность процессора** обеспечивает выполнение сразу нескольких ресурсоемких задач.
- ▶ **Уменьшенное энергопотребление** при максимальной производительности.
- ▶ **Высокое качество графики** и работа с двумя Full-HD мониторами без дополнительной графической карты.
- ▶ **Размер корпуса** составляет всего лишь 1/3 часть от стандартного формата.



125362, Москва, Строительный проезд,
дом 7а, корпус 28

E-mail: sales@ak-systems.ru

Позвони представителю: +7 (495) 374-9388

www.ak-systems.ru

“Мы готовы предложить в России два десятка сценариев Интернета вещей”

НИКОЛАЙ НОСОВ

SAP является одним из лидеров ИТ-рынка и, в частности, рынка Интернета вещей (IoT). О взглядах компании на рынок IoT и на его перспективы, о том, что уже создано в этой области и что нас ждет в ближайшем будущем, нам рассказал Андрей Биветски, генеральный директор SAP Labs в СНГ.

PC Week: Можно ли утверждать, что Интернет вещей уже стал мейнстримом в мире?

АНДРЕЙ БИВЕТСКИ: Пока нет, но в недалеком будущем обязательно станет. Сейчас слишком много разных стандартов. Виден вектор развития и огромные перспективы для бизнеса. Но всё же IoT еще находится в начальной стадии. Мы считаем, что это самое перспективное направление в горизонте следующих трех-пяти лет.

PC Week: На недавней конференции по вопросам развития Промышленного Интернета в нашей стране президент Siemens в России Дитрих Миллер сказал, что, например, в Германии “поезд” IoT тронулся еще десять лет назад. Мы действительно так сильно отстаем?

А. Б.: Давайте посмотрим, что такое Интернет вещей. Датчики собирают информацию, которая через интернет-каналы отправляется в центр, где данные обрабатываются. Десять лет назад уже был Интернет, были датчики, базы данных и аналитические системы. А вот чего тогда не было, так это баз данных in-memo, а также платформ для анализа этих данных в реальном времени и предиктивной аналитики. То есть данные собирали и отправляли, на их основе можно было принимать решения, но отсутствовали технологии и платформы, чтобы собирать их в мощных облаках с правильными протоколами на промышленной основе, отсутствовали системы машинного обучения, которые позволяли бы не просто взять данные, а мгновенно принять бизнес-решение и запустить транзакцию. И я не думаю, что у России здесь есть серьезное отставание.

PC Week: Как организовано внедрение IoT в нашей стране?

А. Б.: Президент РФ несколько месяцев назад дал поручение сформировать маршрутную карту развития Промышленного Интернета вещей в России. Есть Фонд развития интернет-инициатив (ФРИИ), есть специальные учреждения, которые занимаются развитием IoT. Кроме того, “Ростелеком” вышел с предложением создать Национальный консорциум Промышленного Интернета вещей с привлечением лидеров рынка, производителей инфраструктурных решений, датчиков, разработчиков ПО и протоколов. На сегодняшний день ресурсов и знаний достаточно, чтобы российские компании внедряли на своих предприятиях сценарии IoT.

PC Week: Есть ли у вашей компании свои рекомендации для России?

А. Б.: Наш подход несколько иной. SAP в мире сейчас имеет порядка 30 сценариев IoT, реализованных в пяти-шести отраслях, и эти сценарии мы активно несем в массы. И предлагаем “приземлить” их в разных странах. У нас есть платформа и набор инструментов, есть понимание, опыт, и мы планируем до конца 2016 г. локализовать в России как минимум двадцать сценариев в трех-четырех отраслях.

PC Week: Есть ли у вас маршрутная карта для различных отраслей промышленности?



Андрей Биветски

А. Б.: Чтобы что-то построить в Интернете вещей, нужен конструктор. Сенсоры на российском рынке имеются. Интернет тоже есть, но “Ростелеком”, МТС, “Билайн”, “МегаФон” и другие операторы должны быть готовы к тому, что с приходом Промышленного Интернета возникнут совершенно новые требования к мощности каналов и к стандартам. Даже в потребительском Интернете вещей существует 10–15 крупных протоколов, а в Промышленном Интернете их десятки. Для нас, как производителей, маршрутная карта заключается в том, что мы работаем со всеми протоколами, потому что непонятно, какой из них победит и будет ли некий общий стандарт. Кроме того, чтобы наш Интернет вещей был безопасным, мы подписали меморандум-соглашение о сотрудничестве между SAP СНГ и “Лабораторией Касперского”.

Итак, у нас есть датчики, защищенные протоколы и решение SAP HANA Cloud Platform. Это не просто база данных in-memo, это удобная платформа разработки для стартапов и независимых софтверных вендоров. Развитие экосистемы — главная часть нашей маршрутной карты. Мы “не добежим” до каждого предприятия, мы дадим двадцать базовых сценариев, а дальше будут работать наши партнеры, специализирующиеся на конкретных отраслях.

PC Week: На недавнем Форуме SAP в Москве было заявлено, что “Ростелеком”, стремящийся возложить развитие Промышленного Интернета в России, разворачивает вашу облачную платформу IoT. Означает ли это, что “Ростелеком” уже сделал выбор национальной платформы Интернета вещей в вашу пользу?

А. Б.: Тут не идет речь о монополизации. Представляете, какой это большой рынок? IDC считает, что до 2020 г. его объем в мире будет расти на 79% в год и достигнет 9 трлн. долл. Самая большая часть этого пирога придется на программное обеспечение и на сервисы, в том числе инфраструктурные, — потому-то это интересно “Ростелекому” и другим провайдерам. А самый маленький кусочек из этих девяти триллионов достанется производителям датчиков. И на этом огромном, новом и быстрорастущем рынке будет много игроков.

PC Week: Кто сможет лучше всех монетизировать IoT?

А. Б.: В первую очередь для Интернета вещей нужна инфраструктура, такая как, например, наш совместный с “Ростелекомом” дата-центр. С другой стороны, если телеком-провайдеры, такие как “МегаФон” или “Билайн”, будут

не только расширять свои каналы связи и переходить на протокол IPv6, что совершенно необходимо для IoT, но ещё научатся монетизировать поток данных Интернета вещей, который идет через них, то огромная часть выручки достанется и им. Мы же, как провайдер ПО, будем работать со всеми.

PC Week: Что мешает переходу к Интернету вещей в России? Нужны ли здесь какие-то законы?

А. Б.: Внедрению Интернета вещей мешают не законы. В России есть много предприятий, которые еще не дозрели с точки зрения цифровой экономики. Даже многие крупные компании пока ещё занимаются базовыми вопросами: переводят ключевые бизнес-процессы на ERP, интегрируют склады, бухгалтерию, путевые листы. Естественно, им надо сейчас решить основные проблемы, сделать производство прозрачным. Сначала все должно пройти фазу интегрированного автоматизированного предприятия. А после этого они смогут заняться и Интернетом вещей.

PC Week: Что общего и каковы различия между потребительским и Промышленным Интернетом вещей? У какого из этих направлений больше перспектив в России?

А. Б.: Думаю, пойдет и тот, и другой.

Общее у них — конструкция. В обоих случаях есть датчики, интернет-каналы, системы анализа и принятия решений.

Что касается различий, то для потребительского IoT важно, чтобы было недорогое и был дружелюбный пользовательский интерфейс. А для промышленного — важнее безопасность и непрерывность. Например, сейчас многие автомобили работают на протоколе telnet, который должен быть надежно защищен. Кибербезопасность здесь — главное правило.

Еще один значимый момент — производительность. Если говорить о потребительском Интернете вещей, то речь идет о нескольких датчиках. А если вы имеете дело с двумя-тремя тысячами животных, снабженных датчиками, то это совсем другие объемы информации. Или возьмите прокатный стан или подвижной состав, генерирующие терабайты данных.

И еще в Промышленном Интернете важна масштабируемость, когда платформу можно тиражировать на увеличивающееся производство, например с одного прокатного стана на десять.

PC Week: SAP предлагает централизованную систему. Информация от множества датчиков собирается в одном месте — в облаке. В то же время многие аналитики, например из IBM, прогнозируют переход Интернета вещей к децентрализованным системам. Кто прав?

А. Б.: Эти подходы друг другу не противостоят. Всё зависит от решаемых задач.

Германия является идеологом Индустрии 4.0, где машины и станки общаются друг с другом через Интернет вещей и работает разветвленная модель. Некоторые задачи, скажем, предиктивного технического обслуживания (predictive maintenance), надо однозначно решать централизованно в облаке. А в производственных межмашинных процессах есть сценарии, когда системы могут договориться и без централизации. Например, когда друг с другом общаются конвейеры или их части.

PC Week: Чем сейчас занимается ваше подразделение SAP Labs в СНГ в области Интернета вещей?

А. Б.: В этом году мы фокусируемся на нескольких отраслях для IoT.

Во-первых, медицина. У нас сейчас идет большой пилотный проект для одного из металлургических предприятий — медицинские кресла для предсменных осмотров. Если перед началом работы нужно проверить несколько сотен рабочих, то устоявшаяся во всем мире практика такова: врач или несколько врачей проводят осмотр, замеряют различные параметры и принимают решение о допуске к работе. Технологии Интернета вещей смогут заменить этих врачей.

Во-вторых, сельское хозяйство. Например, квадрокоптеры-пастухи. Пастухам необязательно бегать за крупным рогатым скотом. Можно собирать информацию со спутников, но на сегодняшний день качество снимков с них невысоко, и к тому же в удаленной сельской местности нет быстрого Интернета. Мы в SAP Labs в Москве разработали сценарий, в котором дроны собирают информацию с датчиков, которая передается в облако, обрабатывается и принимается решение. Кроме того, возможно также контролировать воровство и появление диких животных.

В-третьих, сценарии Интернета вещей можно использовать для мониторинга выращивания определенных культур, осуществлять контроль за удобрением почвы. Это еще один интересный сценарий — умный трактор, который не только вспахивает землю, но и одновременно собирает информацию с датчиков и отправляет ее в базу данных in-memo. После ее обработки принимается решение об оптимальном удобрении полей. Эту систему можно подключить к классическому ERP-решению и выдавать заказы на закупку удобрений, выписывать накладные, вызывать грузовик, который всё это привезет.

PC Week: А что с другими отраслями? Например, с металлургией или железнодорожным транспортом?

А. Б.: В России SAP разработала очень интересный сценарий по прогнозированию качества металлургических слывов. Когда кусок металла выходит из печи, он покрыт слоем шлака. Простыми методами невозможно определить его качество. Это дорогостоящий процесс.

Наши коллеги совместно с заказчиком разработали другую процедуру. На линии розлива стали устанавливаются сенсоры, которые посылают информацию с каждого шага производства: о входных параметрах разливаемой стали, о функционировании линии. Система позволяет с высокой вероятностью предсказывать качество полученного сляба без необходимости проведения дополнительного контроля качества (без удаления шлака). В данном случае на 25% снижается стоимость затрат на контроль качества. Только на одной линии крупного производства это порядка 100 млн. руб. в год!

Также у нас есть предложение и для железнодорожников. В Канаде есть крупная железнодорожная компания Canadian Pacific. Классическое техническое обслуживание делается по двум показателям. Первый — дистанция: через каждые 200 км находится станция техобслуживания, через нее проходит состав, проверяются необходимые параметры, и состав едет дальше. Второй — время: гарантийное обслуживание проводится в заданные сроки, а регулярное — в зависимости от пройденного пути. Сбор и обработка информации с датчиков позволяет перейти к обслуживанию по состоянию.

PC Week: Спасибо за беседу.

Виталик Бутерин и "Сколково" поддерживают блокчейн-стартапы

НИКОЛАЙ НОСОВ

17 мая в Москве прошла пресс-конференция с участием Виталия (по канадскому паспорту — Виталика) Бутерина, который покинул Россию в шестилетнем возрасте вместе с родителями. Два года назад, когда ему было 19 лет, он разработал блокчейн-платформу нового поколения Ethereum ("Эфириум"), и сейчас капитализация его проекта составляет миллиард долларов. Партнерами Ethereum являются более 40 крупнейших банков мира, включая Goldman Sachs, Credit Suisse, Barclays и JP Morgan, и крупнейшие ИТ-компании, такие как Microsoft.

"Первой реализацией технологии блокчейн был биткойн, придуманный и выпущенный Сатоши Накамото в 2009 г. Изначально эта технология была разработана для поддержки транзакций по криптовалюте. Некоторое время спустя люди стали понимать, что биткойн и блокчейн — разные вещи. Блокчейн как технологию, на которой основан биткойн, можно использовать для других целей. Идея Ethereum — сделать универ-

сальную платформу, своего рода децентрализованную операционную систему, для которой любой человек на мощном языке программирования может написать

свои правила, которые будут понимать и обрабатывать блокчейн, — рассказал Виталий Бутерин. — Конечно, есть сложности, такие как масштабируемость, защита конфиденциальной информации, связи между механизмами в блокчейн и внешнем мире, например, если есть контракт, зависящий от наступления события в реальном мире. Над этим работают, и если проблемы удастся решить, то через пять—десять лет мир будет выглядеть по-другому".

На мой вопрос, можно ли в Ethereum исключить использование криптовалюты и платить за проведение транзакций в фиатной валюте, например в рублях, он ответил, что для этого протокол должен иметь право рубли контролировать и выпускать. "Чтобы это реализовать, нужно сотрудничество с российским Центробанком. Такого уровня сотрудничества мы в ближайшие несколько лет не получим", — считает Виталий Бутерин.



Виталий Бутерин

Индустриальный...

◀ ПРОДОЛЖЕНИЕ СО С. 16

сального потребителя. Таково реальное и просматриваемое будущее. Пока это всё закрытые сети, но нам интересна обратная связь с конечным потребителем, так что в перспективе может быть выход в публичное облако. Но тут еще предстоит осмыслить и решить много вопросов.

PC Week: Как можно связать Индустриальный Интернет с пользовательским Интернетом вещей в энергетике?

Е. Г.: Энергетика в силу специфики технологических процессов всегда имеет каналы связи. Если взять компании, которые занимаются дистрибуцией электроэнергии, и убрать энергетическую составляющую, то получится самый крупный оператор связи в России. Связь нам необходима для обеспечения управления энергосистемой. Поэтому везде, где есть подстанции на 110 кВт, есть и канал связи, причем на 90% это оптоволоконно, которое позволяет передавать данные. Последняя миля — где-то есть, где-то её нет. В новых сетях есть везде. На каждой новой подстанции на 35 кВт имеется выход в Интернет.

Кроме того, существует PLC-технология передачи данных по электрическим сетям, то есть по сути мы можем добраться до любого прибора, который работает от розетки.

PC Week: А что вам даст факт применения Интернета вещей конечными пользователями?

Е. Г.: Для нас это интересно в плане учета электроэнергии, снижения её потерь и повышения

эффективности потребления, оптимизации операционных затрат с точки зрения снижения стоимости энергии и повышения экологической безопасности.

Например, есть автоматизированная система коммерческого учёта электроэнергии. Было бы интересно, чтобы пользователь мог зайти на сайт системы и сообщить, какая розетка у него дома должна работать, а какая нет.

Чем лучше мы будем понимать поведение потребителя, тем меньше требуется затрат на поддержание резервов мощности и тем более прогнозируемыми становятся затраты на ремонт, на поддержание инфраструктур и инвестиции в них. Огромные средства тратятся на создание новых сетей. При этом мощности мы сейчас используем на 60% — остальное простаивает. Так что польза получается и для нас, и для потребителей, которым могут быть интересны возможности Интернета вещей.

PC Week: Что вы думаете о концепции "умной" энергетики Smart Grid, получившей активное развитие на Западе?

Е. Г.: "Умный" город, солнечные батареи, Smart Grid (выдача электроэнергии от потребителя в сеть) — всё это у нас не работает и работать не будет по тем же принципам, что в энергосистемах других стран. Энергосистема европейского государства принципиально отличается от российской. Там много маленьких локальных систем, где нет жестких требований к функционированию резерва и нет разницы категорийности потребителей. У нас расстояния очень большие, производители электроэнергии и домовые хозяйства далеко разнесены друг от друга,

В настоящее время основной криптовалютой для подтверждения и проведения транзакций на платформе Ethereum является "эфир" (Ether), который по рыночной капитализации (1,06 млрд. долл.) уверенно занимает второе место в мире после биткойна (7,08 млрд. долл.). Курс эфира растет: с января по сегодняшний день он вырос в 15 раз (по отношению к доллару — в 20 раз), что отражает огромный интерес к Ethereum в мире.

Есть интерес к этой платформе и в России. Член консультационного совета Ethereum Владислав Мартынов анонсировал решение о создании Фонда поддержки разработчиков на платформе Ethereum совместно с Виталием Бутериным и Фондом "Сколково". Последний совместно с Ethereum организует отбор и акселерацию перспективных блокчейн-проектов и окажет поддержку в виде налоговых льгот и грантов, заявил вице-президент и исполнительный директор кластера информационных технологий Фонда "Сколково" Игорь Богачев. По его словам, создаваемый фонд поможет удовлетворить запрос бизнеса и государства в решении не только текущих, но и будущих задач, таких как микроплатежи в мире Интернета вещей, исполнение сложных смарт-контрактов, создание гибридных платформ и госреестров. Игорь Богачев сообщил, что планируется поддержка 20 команд разработчиков.

ВКРАТЦЕ

Hewlett Packard Enterprise отделяет сервисное подразделение

Hewlett Packard Enterprise (HPE) объявила о том, что её подразделение корпоративных сервисов будет выделено в самостоятельный бизнес и объединено с одним из крупнейших в мире системных интеграторов — Computer Sciences Corporation (CSC), сообщает Reuters. Таким образом, на рынке ИТ-сервисов возникнет крупный игрок с годовым оборотом 26 млрд. долл. Этот неожиданный шаг является очередным в серии мер, предпринимаемых CEO HPE Мег Уитман с целью оживить одну из старейших компаний Кремниевой долины. Он ставит точку на эксперименте HP, начавшемся в 2008 г. покупкой за 13,9 млрд. долл. сервисной компании EDS.

Половина объединенной компании будет принадлежать акционерам HPE. Последние также получат дивиденды на общую сумму 1,5 млрд. долл. Согласно условиям соглашения, CSC берет на себя 2,5 млрд. долл. долгов подразделения HPE Enterprise Services, выручка которого в прошлом финансовом году составила 19,5 млрд. долл., что на 10% меньше, чем

годом ранее. В рамках сделки с CSC подразделение было оценено в 8,5 млрд. долл.

Мег Уитман войдет в состав совета директоров компании, созданной в результате присоединения HPE к CSC. Руководить ею будет глава CSC Майк Лори. Сделку планируется закрыть к марту 2017 г. По словам финансового директора HPE Тима Стоунсайфера, расходы компании на отделение Enterprise Services составят 900 млн. долл.

После завершения сделки HPE сфокусируется на продаже облачных сервисов, серверов, систем хранения данных и сетевого оборудования. При этом компания сохранит некоторые сервисные операции, в том числе продолжит оказывать услуги технической поддержки пользователям софта и оборудования, сообщила Мег Уитман.

В официальном анонсе не сообщается о возможных увольнениях, но до этого HPE предупреждала, что к 2018 г. сократит 33 тыс. рабочих мест, в дополнение к 55 тыс., анонсированным ранее.

Аналитик IDC Кроуфорд Дель Прете считает, что сделка с CSC согласуется со стратегией Уитман по превращению HPE в более гибкую и прибыльную компанию. *Сергей Стельмах*

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

PC WEEK

 № 8-9
(907-908)

 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..... | 20 |
| <input type="checkbox"/> Asus..... | 2 |
| <input type="checkbox"/> Huawei..... | 5 |
| <input type="checkbox"/> RedSys..... | 9 |
| <input type="checkbox"/> AK-Systems..... | 17 |

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; или по факсу: +7 (495) 974-2260, 974-2263.

PC Week: Спасибо за беседу. □



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.

