ГАЗЕТА ДЛЯ КОРПОРАТИВНЫХ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И РЕШЕНИЙ

PC WEEK

СК ПРЕСС

18+

№ 15-16 (914-915) • 27 СЕНТЯБРЯ • 2016 • МОСКВА

http://www.pcweek.ru

Huawei делает ставку на облака

СЕРГЕЙ СВИНАРЕВ

КОНФЕРЕНЦИИ

Прошедший в г. Шанхае в начале сентября международный конгресс Huawei Connect 2016, собравший 18 тыс. участников из 120 стран, объединил в себе три проводившиеся прежде раздельно конференции Huawei — Cloud Congress, Network Congress и Developer's Congress. Как оказалось, в этом был прямой смысл. Судя по программным выступлениям высших руководителей компании, одним из главных направлений ее стратегии становятся облака. Объясняя этот шаг, исполняющий на ротационной основе обязанности CEO Кэнь Ху отметил, что к 2025 г. все компании в той или иной степени будут использовать в своем бизнесе облака, а 85% перенесут туда свои ключевые приложения. А кроме того, у Huawei есть полный набор компетенций и ресурсов для реализации современных облачных инфраструктур.

Кэнь Ху

Пленарное выступление Кэнь Ху, представлявшего новую облачную стратегию, изобиловало общими рассуждениями о создании "умного мира" (intelligent world), а также объединении компьютеров всей планеты и создании "цифрового мозга" в облаке, который, постоянно развиваясь, не будет подвержен старению. Но сегодня удивить кого-то общими сентенциями о пользе облаков довольно трудно: ведь о своей ориентации на них говорят все ведущие вендоры. В этой связи следует обратить внимание на те элементы стратегии, которые отличают Huawei от других игроков.

Компания делает акцент не на некие универсальные облачные решения, пригодные на все случаи, а на специфические для каждой отрасли решения, способные стать основой для столь модной сегодня цифровой трансформации бизнеса. В числе основных отраслей Huawei видит, в частности, госсектор, коммунальные услуги, финансовые учреждения, телекоммуникации, энергетику и СМИ. Очевидно, что строить в одиночку специализированные облачные инфраструктуры, учитывающие тонкие особенности каждого такого сегмента одной компании, пусть и такой большой, как Huawei, не под силу. И поэтому ставка делается на формирование глобальной экосистемы партнеров и заказчиков.

Примером такого сотрудничества можно считать разработку решения "Безопасный город" (Safe City), обеспечивающего визуализацию информации и координацию взаимодействия различных городских ведомств, отвечающих за безопас-

ПРОДОЛЖЕНИЕ НА С. 15

RECS'2016: государство как катализатор перехода на ЭДО

ЕЛЕНА ГОРЕТКИНА

В нашей стране государство уже давно играет важную роль в области автоматизации документооборота, выступая в двух ипостасях: с одной стороны, в качестве заказчика, а с другой — в роли регулятора рынка, тем самым способствуя переходу бизнеса и госструктур на электронные рельсы.

Но на этом пути остается еще немало проблем и задач. О некоторых последних инициативах государства, направленных на их решение, шла речь на сентябрьской конференции Russian Enterprise Content Summit (RECS) 2016, организованной еженедельником PC Week.

Пленарное заседание RECS'2016

На пути к единой информационной среде

Информатизация госуправления привела к тому, что у государственных органов скопилось огромное количество информации о гражданах и объектах. Однако эти информационные ресурсы остаются разрозненными и слабо связанными между собой. При этом каждая госорганизация использует свой формат, что затрудняет обмен данными, а также негативно отражается на их достоверности и качестве.

Для решения этой проблемы в июне этого года было принято постановление правительства РФ № 487 о создании в нашей стране "Единой информационной среды". Над этим сейчас работает Федеральное казначейство РФ.

Предполагается, что реализация этого постановления позволит решить две ключевые задачи: во-первых, данные в государственных ИС (ГИС) будут актуальны, достоверны и связаны между собой, а во-вторых, в любой момент времени они будут доступны всем госорганам.

"Работа предстоит большая", — считает Дмитрий Коновалов, заместитель начальника управления систематизации

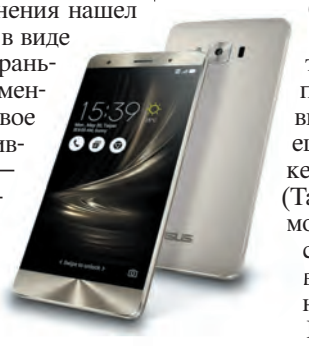
ПРОДОЛЖЕНИЕ НА С. 6

В НОМЕРЕ:

ASUS Zenvolution пришла в Россию

ИГОРЬ НОВИКОВ

Компания ASUS представила в Москве обновленное семейство мобильных Zen-продуктов для эры облачных вычислений, объединяющее в единой целое компьютеры, смартфоны, робототехнику, Интернет вещее, виртуальную и дополненную реальность. Принцип объединения нашел концептуальное отражение в виде серии продуктов, которые раньше относились к разным сегментам рынка. Новое продуктовое предложение ASUS, получившее название Zenvolution, — это смартфоны серии ZenFone 3, ноутбуки серии ZenBook 3, устройства "2 в 1" Transformer 3 Pro, трансформеры Transformer 3 и умные часы ZenWatch 3.



Zenfone 3 Deluxe

Когда-то давно ASUS была известна на ИТ-рынке прежде всего своими бюджетными моделями. Однако затем компания сменила стратегию и, используя ранее накопленный опыт, сделала ставку на выпуск флагманских продуктов. Новая стратегия принесла успех. Как заявила Анжела Сю, региональный директор ASUS в странах СНГ, Балтии и России, компания занимает сейчас первое место на рынке ультрабуков в России, продажи смартфонов ZenFone в России уже второй год растут на 60%, а три модели ее смартфонов входят в список Top-10 российского онлайн-рынка (по данным GFK на июль 2016 г.). Вице-президент ASUS Эрик Чен назвал российский рынок одним из наиболее приоритетных для компании.

Строго говоря, третье поколение мобильных гаджетов и компьютеров ASUS, представленное в Москве, впервые было анонсировано еще в начале лета на выставке Computex 2016 в Тайбэе (Тайвань). Однако нынешний момент для их вывода на российский рынок неслучаен: в начале осени традиционно начинается подъем продаж.

Концепция новой продуктовой линейки Zenvolution выстроена на предоставлении пользователям максимальной скорости работы, которая достигается за счет оснащения моделей топовыми процессорами: для смартфонов — это процессоры Qualcomm вплоть до Snapdragon 821 и ОС Android 6.0 с фирменным интерфейсом ZenUI; для трансформеров и ноутбуков — процессоры Intel Core i7 и ОС Windows 10. Вторая характерная особенность Zenvolution — это фирменный дизайн, который доработан компанией для создания максимального удобства при повседневном применении.

"На мой взгляд, будущее за устройствами, которые будут не только быстро работать, но и оснащены богатым набором функций. Этот набор свойств в итоге создает то, что называется "удовлетворенность пользователей", — заявил в интервью для

Эрик Чен

PC Week Эрик Чен. — ASUS делает сейчас многое в этом направлении. Новые продукты компании отражают выбранную ею стратегию".

По его словам, главным в новой линейке устройств стало раскрытие скрытых

ПРОДОЛЖЕНИЕ НА С. 4

ASUS®
В ПОИСКАХ НЕВЕРОЯТНОГО

ПРОДУКТ ГОДА 2016

от 69 990 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 исключительная производительность.

intel inside™ CORE™ m

* спецификации отличаются в зависимости от модели

ПРИСОЕДИНЯЙТЕСЬ К НАМ В СОЦИАЛЬНЫХ СЕТЯХ:

VK.COM/**ASUS** FACEBOOK.COM/**ASUS.RU** TWITTER.COM/**ASUS_RUSSIA** INSTAGRAM.COM/**ASUS_RUSSIA**

СОДЕРЖАНИЕ

№ 15-16 (914-915) • 27 СЕНТЯБРЯ, 2016 • Страница 3

НОВОСТИ

ЭКСПЕРТИЗА

ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ

УПОМИНАНИЕ ФИРМ В НОМЕРЕ

БЛОГОСФЕРА PCWEEK.RU

Всегда ли возвращаются инвестиции в IoT?

Сергей Свинарев,
pcweek.ru/iot/blog

В только что выпущенном отчете Russia Internet of Things Market 2016—2020 Forecast IDC прогнозирует, что в течение 2016—2020 гг. рынок Интернета вещей (IoT) будет ежегодно увеличиваться в среднем на 21,3% и к концу указанного периода достигнет 9 млрд. долл. В основном за счет трех отраслей — производства, транспорта и энергетики, на них приходится более 50% общего объема российского рынка IoT. Немного отстает от них государственный сектор, реализующий программы, которые условно можно отнести к категории “умных городов”.

Почему условно? Давайте по порядку. В отчете IDC есть еще одна цифра, которая, с одной стороны, радует, а с другой — вызывает беспокойство. Констатируется, что в этом году российские организации инвестируют в IoT свыше 4 млрд. долл., включая затраты на оборудование, программное обеспечение, услуги и связь. Вероятно, в этой сумме есть и некая доля государственных инвестиций. Но насколько эффективно они работают? Все мы видим, к примеру, что запущена система отслеживания движения общественного транспорта и на остановках прекрасно функционируют электронные табло, оповещающие пассажиров об ожидаемом времени прибытия того или иного маршрута. Удобно, не спорю. Но этим использование данной системы и ограничивается. В то же время я регулярно наблюдаю у себя в районе, как к остановке чуть ли не гуськом подходят два-три автобуса с одним и тем же номером. Естественно, после этого интервал ожидания следующего увеличивается колоссально. Причем происходят данные события не в часы пик и в районе, где особых пробок не наблюдается. Казалось бы, почему не использовать данную систему не только для оповещения, но и для управления движением общественного транспорта? Мне кажется, потому что у многих госпроектов цели не экономические, а имиджевые. А следовательно, о возврате инвестиций здесь думают в последнюю очередь.

Microsoft свернет производство Lumia-смартфонов к концу года

Сергей Стельмах,
pcweek.ru/mobile/blog

Похоже, Microsoft осознала бесперспективность противостояния Windows Phone с iOS и Android — оно лишь перемалывает ресурсы, которые можно было бы использовать в других сферах бизнеса. Эту информацию подтверждает анонимный сотрудник Microsoft, сообщивший изданию WinBeta, что к концу года Microsoft окончательно свернет выпуск смартфонов линейки Lumia.

Косвенно желание завершить выпуск аппаратов Lumia подтверждается и регулярным снижением Microsoft цен на фирменную продукцию с Windows Phone/Windows 10 Mobile, которое стало за последний год вполне привычным явлением для поклонников бренда. Очевидно, что Microsoft действительно распродает неактуальные для неё модели из серии Lumia.

Ещё одним подтверждением служит то, что из списка фирменной продукции, предлагаемой интернет-магазином Microsoft, и вовсе исчезла строка с упоминанием Lumia, на месте которой появился раздел Education Store.

Но Microsoft не уходит из смартфонного бизнеса и, как известно, работает над новым смартфоном. И первым таким устройством, слухи о котором многократно появляются в прессе, должен стать Surface Phone. По последней информации, Microsoft переносит его запуск, который, по слухам, должен был состояться в конце 2017-го, на 2018 г. Учитывая, что выход SP имеет столь отдаленную перспективу, говорить о нем рано.

Тем временем поддерживать экосистему Windows 10 Mobile (чтобы ко времени выхода мифического SP о ней не забыли) будут партнеры Microsoft. В настоящее время список таких партнеров невелик, однако новинки вроде бизнес-смартфона HP Elite X3 демонстрируют значительный потенциал платформы. Также известны планы компании о выпуске в 2017 г. следующего обновления Windows 10 Mobile под кодовым названием Redstone 2.

Социальные сети — новое кибероружие?

Владимир Безмалый,
pcweek.ru/security/blog/

Пора признать, что Facebook, LinkedIn и Twitter не могут защитить сами себя, не говоря уже о вашей информации.

Киберпреступники атакуют пользователей практически в каждой социальной сети. Очень часто сегодня в новостях мелькают заголовки о взломах учетных записей знаменитостей, однако это не более чем верхушка айсберга. Проблема на самом деле куда глубже. Большинство организаций просто не осознает их существование.

Неумение организовать безопасность компаний в социальных сетях приводит к серьезным рискам как для брендов, так и для руководителей соответствующих организаций.

Обратимся к статистике. По данным Cisco, наиболее часто мошенничество в том или ином виде распространялось в 2015 г. через Facebook. По заявлению ФБР, мошенничество, связанное с общением в социальных сетях, увеличилось в четыре раза за последние пять лет, а по сведениям компании PricewaterhouseCoopers, каждое восьмое предприятие пережило событие, связанное с нарушением безопасности из-за атаки в социальных сетях.

По сообщению Facebook, в 2015-м до 2% учетных записей пользователей являются мошенническими, а это около 31 млн. Twitter и Linkedin оценивают эту цифру в 5%. В социальных сетях на сегодня нет надежной системы идентификации и учета двойных или просто фальшивых учетных записей.

Несмотря на это, социальные сети все еще пользуются наибольшим доверием среди онлайн-каналов. Как показывают результаты исследования, потребители легко доверяют средствам социального общения, куда больше, чем любым другим каналам онлайн. Все это автоматически делает социальные сети находкой для злоумышленников. Атакующие сегодня могут легко управлять пользователями и выполнить множество распространенных кибератак и афер, включая различные методы социальной инженерии, организацию мошеннических продаж, фишинг и т. д.

Однако и это не все. Уже довольно давно социальные сети и данные в них используются в разведывательных целях. Такими были атаки через Linkedin и Twitter. Например, утечка данных из Пентагона летом 2015-го, в ходе которой почтовый сервер управления безопасности с учетными данными 4200 сотрудников не работал в течение двух недель, а точный объем украденных данных так и не удалось определить.

Да, социальные сети не могут создавать новые угрозы, но существенно усиливают угрозы существующие. Что это значит для вас? Прежде всего то, что специалисты по безопасности должны понимать, что социальные сети — опаснейший канал возможного нарушения безопасности. Вам необходимо оценить ваши социально значимые активы и постоянно их контролировать. Помните, что средства социального общения все еще развиваются. Подготовьтесь к возможным атакам, которые несомненно появятся в ближайшее время.

ИБ-ошибки, настойчиво повторяемые персоналом

Валерий Васильев,
pcweek.ru/security/blog

По данным PwC за 2014 г., количество ИБ-инцидентов растет в среднем на 66%, а ущерб от одного взлома (опять же в среднем) составлял (в 2014-м) без малого 6 млн. долл. И это без учета взломов, скрываемых от общественности. Ведь пропущенный взлом — удар по репутации.

Как утверждает информационный ресурс Security Innovation Europe, существенная доля взломов происходит из-за вредных (с позиции службы ИБ) привычек персонала, с которыми тот не хочет расставаться. Кратко опишем главные из них и подскажем средства противодействия.

Использование для работы небезопасных устройств. Главным источником таковых остается практика BYOD. Снизить связанные с этим риски можно, как считают в Security Innovation Europe, распространив ИБ-политики на используемые в служебных целях личные устройства. Помимо технических средств следует применять оргмеры, включающие ответственность за нарушение правил ИБ.

Слабая безопасность для мобильного доступа. Прежде всего ИБ-служба должна обеспечить жесткий контроль за мобильным доступом к чувствительным данным, предоставив его только тем, кому он реально нужен в работе, и своевременно закрывая утратившие актуальность доступы и привилегии в правах. Разумеется, нужно шифровать данные, вообще запретить хранение на мобильных носителях чувствительных данных и ввести (хотя бы) парольный доступ к мобильным устройствам. С это следует начать, а продолжение зависит от ИБ-политики компании.

Слабая парольная защита. Это общее больное место. Поможет двухфакторная аутентификация. Варианты могут быть самыми разными, включая набирающую популярность и технологическое разнообразие биометрию.

Записанные или распечатанные пароли. Эту практику следует запрещать и наказывать за нарушение. Если от записывания паролей можно защититься описанным выше способом, то от привычки записывать иную чувствительную информацию сделать это значительно сложней. Поэтому начинать нужно с оргмер.

Слабая защищенность от социальной инженерии. Тут первым делом, как наиболее доступное, нужно ввести регулярное обучение и информирование персонала. ИБ-служба должна выявлять (и прогнозировать — мыслить как злоумышленник) наиболее типичные для своей компании ухищрения злоумышленников и доносить эту информацию до сотрудников.

Умышленное отключение защиты. Корпоративная система ИБ должна быть выстроена так, что технически к таким возможностям получает доступ строго ограниченный состав специалистов. В целом же нужно вводить оргмеры — обучение и ответственность за нарушение ИБ-политики.

Появление теневых ИТ-средств. С несанкционированной установкой технических ИТ-средств и ПО следует бороться, возглавив ее: дать возможность персоналу доводить до руководства свои пожелания иметь на рабочем месте тот или иной новый ресурс и обсуждать его полезность. Зачастую можно пойти сотрудникам навстречу без ущерба корпоративной ИБ или предложить альтернативу, ИБ которой проще реализовать.

Большие данные, блокчейн и новая ИТ-платформа Сбербанка

НИКОЛАЙ НОСОВ

Сбербанк подтверждает свою репутацию "крупнейшей ИТ-компании с банковской лицензией". 20 сентября Андрей Иванов, старший управляющий директор — директор управления торгового финансирования и корреспондентских отношений Sberbank CIB, сообщил о завершении первого этапа работ по созданию ИТ-платформы Сбербанка для проведения сделок торгового финансирования.

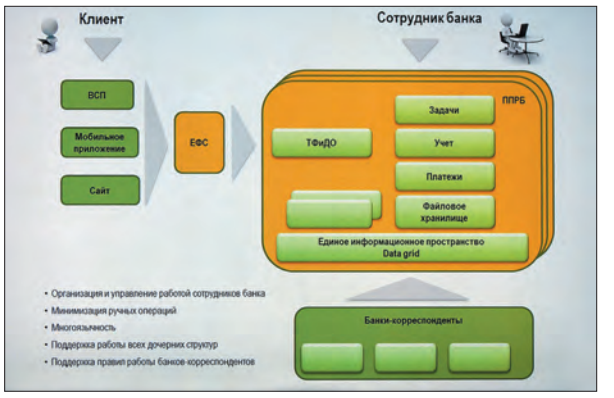

Андрей Иванов

Торговое финансирование — классическая область работы банка. Предположим, продавец и покупатель заключают сделку. Они имеют дело друг с другом впервые и работать по предоплате или по предпоставке не готовы. Тем более с малоизвестным зарубежным партнером. Нужен посредник, которому доверяют обе стороны. Покупатель обращается в банк с заявлением на открытие аккредитива на сумму, причитающуюся продавцу за отгруженный товар. Свидетельством о выполнении договора со стороны продавца могут быть, например, документы об отгрузке товара. Как только предмет сделки передан покупателю либо независимому перевозчику, продавец направляет в исполняющий в соответствии с условиями аккредитива банк предусмотренные документы. Банк покупателя осуществляет платеж по аккредитиву согласно полученным из исполняющего банка инструкциям. Все это занимает немало времени, требует большого количества труда и бумаг.

Для автоматизации всех этих процессов в конце 2015 г. в Сбербанке начались работы по созданию новой ИТ-платформы. Сейчас, по окончании первого этапа, запущена в промышленную эксплуатацию часть системы, автоматизирующая внутренний учет ряда операций торгового финансирования.

Летом следующего года, по окончании второго этапа, системой смогут воспользоваться клиенты. У них будет индивидуальный личный кабинет по всем продуктам торгового финансирования, в котором можно будет заключать сделки не отходя от своего компьютера. Им будет представлен полный сервис по взаимодействию с банком по соответствующим продуктам. От предварительных консультаций по заключению договоров в области внешней торговли, консультирования по правильной формулировке платежных статей, по особенностям соблюдения валютного контроля и валютного законодательства РФ до консультирования по структурированию как экспортных, так и импортных сделок торгового финансирования.

Клиенты получат возможность через личный кабинет подбирать себе иностранных партнеров на внешнем рынке, получать рекомендации по различным юрисдикциям, по учету логистических



Архитектура платформы торгового финансирования

аспектов, таможенных и валютных особенностей различных юрисдикций стран мира. Клиенты получат полную информацию о статусе их операций с продуктами торгового финансирования — аккредитивов, гарантий, контргарантий, инкассо и всех других продуктов, которыми располагает Сбербанк, включая автоматический расчет всех платежей по продуктам в режиме онлайн.

Более того, планируется уведомлять клиента о важных событиях по тем или иным продуктам. Личный кабинет будет напоминать ему о погашении задолженностей, что особенно важно, когда у клиента открыто большое количество аккредитивов, о выплате процентов, о поступлении или непоступлении товара, о растаможке. Система дает возможность уйти от бумажных носителей и является еще одним шагом на пути полного перехода к электронному документообороту.

Программа по развитию глобальной платформы торгового финансирования реализуется на базе и во взаимодействии с основными стратегическими платформами банка — Платформой поддержки развития бизнеса и Единой фронтальной системой. Завершить проект планируется в середине 2018 г.

"В российском финансовом секторе аналогичной разработки пока нет", — отметил Андрей Иванов.

На третьем этапе работ планируется развернуть системы Big Data, которые помогут анализировать глобальные данные о мировых торговых потоках и пре-

ПРОДОЛЖЕНИЕ НА С. 6

ASUS...

ПРОДОЛЖЕНИЕ СО С. 1

возможностей, заложенных в новые технологии. Говоря о смартфонах, это — расширенная графика, для трансформеров и ноутбуков — минимальные весовые характеристики и тонкий дизайн при премиальной графике и достаточном запасе питания для функционального использования в течение всего рабочего дня.

"Долгое время при продаже мобильной техники мы старались сделать ставку на более низкие цены, чем у конкурентов, стремясь завоевать симпатии рядовых покупателей, — рассказал Эрик Чен. — Однако около двух лет назад мы серьезно переработали стратегию. Теперь мы предлагаем рынку технику, которая отличается самыми передовыми технологическими достижениями и идеальна с точки зрения дизайна. В этом году мы сделали еще один шаг в этом направлении. Хотя цены на наши устройства подросли, но мы продолжаем следовать выбранному принципу, предлагая рынку продукты по наименьшей цене в своем диапазоне и дополняя их передовыми характеристиками".


Анжела Сю

Рассматривая линейку Zenvolution, действительно можно отметить полноценный набор гаджетов и мобильных компьютеров.

ZenFone 3 Deluxe

Это первый в мире смартфон с новым флагманским процессором Qualcomm Snapdragon 821. Он изготавливается по наиболее совершенной на сегодняшний день для мобильных систем 14-нм технологии FinFET Low Power Plus. Благодаря росту частоты с 2,2 до 2,4 ГГц производительность нового процессора выше, чем у предыдущей модели 820, на 10%, что обеспечивает ZenFone 3 Deluxe 20%-ное преимущество в тестах Antutu на производительность перед Samsung Galaxy S7 и Apple iPhone 6.

Главные достоинства нового процессора лежат в области графики. Модель Deluxe поддерживает камеру с разрешением до 28 Мп, видеозапись высокого разрешения в формате 4K Ultra-HD и расширенные функции автофокусировки по нескольким технологиям: лазерная, фазовая и следящая.

Когда-то давно ASUS начинала свое продвижение на ИТ-рынке, занимаясь выпуском материнских плат. Они отличались премиальными характеристиками и предназначались пользователям, которые хотели получить максимум возможного. Этот подход был сопряжен с риском неустойчивой работы, однако ASUS сумела тогда обогнать конкурентов, добившись высокой надежности несмотря на экстремальные режимы разгона.

Прежний опыт теперь находит применение в нынешних моделях ASUS. ZenFone 3 Deluxe оснащен беспрецедентным объемом памяти: 6 Гб быстрой двухканальной оперативной памяти LPDDR4 с полосой пропускания 29,8 Гб/с. Она обеспечивает ту самую надежность, которая выражается для пользователей в возможности очень быстрого переключения между приложениями. Даже "тяжелым" приложениям "нетесно" в таком объеме памяти. Нетесно и пользовательским данным — аппарат располагает накопителем на 256 Гб.

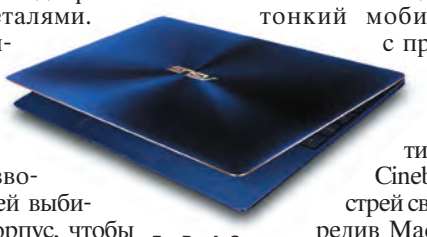
Алексей Нистратов, менеджер по техническому маркетингу ASUS в странах СНГ, Балтии и России, особое внимание обратил на работу новой модели Deluxe с графикой. Камера PixelMaster использует сенсор Sony IMX318 с разрешением 23 Мп, который позволяет получать профессиональное качество при фотосъемке. Шестиэлементный объектив Largan камеры обеспечивает хорошую светосилу (f/2.0), оптимальную для съемки в неподготовленных условиях. Благодаря защите сапфировым стеклом достигнута долговечность объектива, необходимая для качественной съемки.

Особая гордость ASUS — это расширенная сверхскоростная технология Tri-Tech следящей фокусировки, уникальная в своем роде. Впервые в мире инженеры компании объединили вместе три технологии наведения камеры смартфона на резкость — лазерную, фазовую и следящую. Лазерная автофокусировка подходит для съемки в темное время суток или в помещениях с плохой освещенностью. Время фокусировки составляет всего 0,03 с, за которое лазер успевает измерить расстояние до выбранного объекта, а механизм управления линзами — подстроиться для создания оптимального кадра.

Фазовая автофокусировка — это традиционный способ настройки резкости, он эффективно работает при съемке на открытом воздухе, и ASUS сохраняет его в своих продуктах.

Третий тип автофокусировки — следящая. Она позволяет выделять объекты, движущиеся в кадре, и сохранять их резкость вне зависимости от приближения или удаления.

Большое внимание уделено дизайну. Его особое изящество подчеркивается технологическими деталями. Традиционно пластиковый корпус смартфона ассоциировался у пользователей с бюджетностью модели. Поэтому производители топовых моделей выбирают металлический корпус, чтобы подчеркнуть статусность модели. Однако разработчикам приходится идти на компромисс: применение компактных внутренних антенн возможно только в сочетании со специальными пластиковыми вставками в корпусе гаджета, но они необходимы для надежного выделения радиосигнала. Инженеры ASUS сумели найти решение этой проблемы: новый ZenFone 3 Deluxe обладает стильным, полностью металлическим корпусом без диэлектрических вставок на задней крышке.


ZenBook 3

Еще одна техническая новинка для смартфонов — применение двойного микрофона: один — для считывания голоса/звука, другой — для выявления фоновых искажений и шумов. Эта технология раньше встречалась на профессиональном звуковом оборудовании (микрофонах, диктофонах, наушной гарнитуре). Инженеры ASUS нашли возможность теперь реализовать ее в своих флагманских моделях.

ZenBook 3

Zenvolution рассматривается компанией ASUS не просто как набор продуктов. Это — подготовка пользователей к цифровому будущему, когда выбор устройства для работы продиктован условиями его использования, прикладными задачами, объемами информации. Как отметил Эрик Чен, достоинство линейки Zenvolution состоит в том, что в ней представлены устройства сразу несколько типов: смартфон, умные часы, трансформер, ультрабук.

В сегменте мобильных настольных систем линейка Zenvolution представлена премиальным высокопроизводительным ультрабуком ZenBook 3, построенным на базе процессора Intel Core i7 в корпусе толщиной 11,9 мм. Эксперты сразу назвали ZenBook 3 "конкурентом MacBook и MacBook Air, на котором работает Windows 10".

ZenBook 3 создавался как ультратонкий мобильный компьютер с премиальной производительностью. Благодаря процессору Core i7 и 16 Гб оперативной памяти на тестах Cinebench он оказался быстрей своих конкурентов, опередив MacBook Air в 1,07 раз, а MacBook в 1,5 раза.

Дисковая подсистема нового ультрабука выстроена на базе высокоскоростного твердотельного накопителя с интерфейсом PCIe 3.0×4 и обладает емкостью 1 Тб. По тестам Intel ZenBook 3 превзошел конкурентов и по скорости подсистемы хранения: MacBook Air в 1,26 раза, а MacBook в 2,36 раза.

Главный вызов, который приняла на себя ASUS в новой модели, — это минимизация размеров. Ультрабук получился со сверхтонкими рамками для дисплея, а по толщине корпуса (11,9 мм) он превзошел конкурентов: MacBook на 9%, а MacBook Air на 30%.

Инженеры ASUS сумели создать и самую тонкую конструкцию крепления крышки ноутбука (всего 3 мм). Но при этом они обеспечили 20 тыс. гарантированных циклов закрывания при тестах шарнира на надежность.

В непростых условиях современного рынка мобильных систем ASUS показала, что готова бороться за позиции лидера и может потеснить не только конкурентов в сегментах Windows и Android, но и Apple. Свои амбиции "совершить революцию" компания не скрывает.

Моноблок ASUS Zen AiO ZN240IC для бизнеса и творчества

ВЛАДИМИР РОМАНЧЕНКО

ПЕРВЫЙ ВЗГЛЯД

Настольный ПК Zen AiO ZN240IC, представленный в этом году компанией ASUS, представляет собой моноблочную систему класса “достал из коробки, включил и работай”. Новинка является логичным развитием выпущенной в конце прошлого года премиальной линейки моноблоков Zen AiO Pro. Вычислительный модуль, сенсорный 24-дюймовый монитор и стерео акустика, интегрированные в одном корпусе, не требуют настройки и избавляют рабочий стол от излишних проводов.

Внешний вид комплекта ASUS Zen AiO ZN240IC с клавиатурой и мышью

Zen AiO ZN240IC выполнен в корпусе из алюминиевого сплава серебристо-серого (Quartz Gray) оттенка. Фирменный дизайн Zen AiO включает такие неизменные элементы, как литая металлическая подставка, тонкая шлифовка тыльной панели и стилизованная шлифовка концентрическими окружностями в нижней части лицевой панели. Подставка обеспечивает только наклон моноблока, но небольшая масса системы (всего 7,3 кг) позволяет развернуть её даже одной рукой.

Моноблок оснащён современным 23,8-дюймовым дисплеем с разрешением Full HD (1920×1080) на базе IPS-матрицы с сенсорным вводом. Экран обладает высокой контрастностью и очень большим запасом яркости, так что блики от глянцевой поверхности всегда можно нейтрализовать дополнительными настройками и выбором подходящего рабочего места.

После близкого знакомства с удобным сенсорным вводом устройства остается только сожалеть, что настольные системы с сенсорными экранами до сих пор так и не стали массовым явлением. И это несмотря на широкое распространение ОС Windows 10, отлично с этим справляющейся. Благодаря ежедневному использованию смартфонов мы уже привыкли пользоваться сенсорным экраном. Возможность такого ввода на экране десктопа во многих случаях позволяет значительно увеличить производительность труда. А функции других манипуляторов, в первую очередь мыши, ее не заменяют, но отлично дополняют.

Как и более ранние устройства серии Zen AiO, модель ZN240IC оснащена компактным внешним блоком питания, рассчитанным на рабочее напряжение 19 В и ток 4,74 А. Примерно такими же БП оснащаются мощные ноутбуки ASUS.

Моноблок располагает действительно мощной аппаратной платформой, включающей 4-ядерный процессор Intel Core i5-6200U шестого поколения с тактовой частотой 2,3 ГГц и 4 Гб оперативной памяти DDR4 в двух слотах SODIMM с возможностью расширения до 16 Гб. Помимо интегрированной в процессор графической подсистемы, возможностей которой более чем достаточно для большинства офисных и деловых приложений, ZN240IC также содержит дискретную графическую видеокарту Nvidia GeForce 940MX, обеспечивающую высокую производительность при работе с ресурсоёмкими приложениями, при просмотре фильмов или в играх.

Интерфейсы расположены на тыльной стороне ASUS Zen AiO ZN240IC

Операционная система и критичные приложения устанавливаются на твердотельном накопителе Liteon CV1-CC128 ёмкостью 128 Гб (OEM Plextor). Для хранения данных предусмотрен 2,5-дюймовый жесткий диск Toshiba MQ01ABD100 ёмкостью 1 Тб с интерфейсом SATA 3 Гбит/с, 8 Мб буферной памяти и скоростью вращения шпинделя 5400 об./мин. Это не самый быстрый современный накопитель, но его характеристики полностью соответствуют характеру офисной нагрузки.

В плане интерфейсной обвязки моноблок может служить образцом того, как действительно следует проектировать современные десктопы. Беспроводные интерфейсы представлены современными Wi-Fi 802.11ac/b/g/n и Bluetooth 4.0. В распоряжении пользователя также есть четыре порта USB 3.0 и два порта новейшего стандарта USB 3.1 со скоростью обмена данными до 10 Гбит/с. Помимо этого есть выход HDMI, проводное подключение LAN 10/100/1000 Мбит/с, аудиоразъемы для микрофона и наушников, а также слот безопасности для замка Кенсингтона.

Все порты расположены с тыльной стороны устройства, так что кабели легко убираются с глаз и не портят внешний вид системы. К сожалению, там же расположен ридер для флэш-карт SD, и это не очень удобно — искать узкий слот на тыльной стороне на ощупь. Всё же картридер был бы более уместен на лицевой стороне.

Концепция “система из коробки”, в которой выполнен ASUS ZN240IC, предусматривает наличие таких компонентов, как 1-Мп цифровая HD-камера и цифровой микрофон (встроены в окантовку экрана для удобного ведения видеоконференций), а также встроенная стереофоническая аудиосистема мощностью 2×3 Вт. В рамках этой же концепции в комплект поставки ASUS ZN240IC входят фирменные беспроводная клавиатура и мышь. Особенно приятное впечатление произвела полноформатная клавиатура, клавиши которой стилизованы под “ноутбучное” исполнение. Очень удобно при частой смене стационарного рабочего места на портативный ПК и обратно.

Моноблок поддерживает трансляцию мультимедийного контента с различных мобильных устройств. Благодаря приложению ASUS ZenSync систему можно превратить в цифровую базовую станцию для обмена файлами, а накопитель компьютера при этом сможет играть роль персонального облачного хранилища с интернет-доступом из любого места в любое время.

СК ПРЕСС PC WEEK

Учредитель и издатель
АО «СК ПРЕСС»

Издательский директор
Е. АДЛЕРОВ
Издатель группы ИТ
Н. ФЕДУЛОВ
Издатель
С. ДОЛЬНИКОВ
Директор по продажам
М. СИНИЛЬЩИКОВА
Генеральный директор
Л. ТЕПЛИЦКИЙ
Шеф-редактор группы ИТ
Р. ГЕРР
Ведущий эксперт группы ИТ
С. КОСТЯКОВ

Редакция

Главный редактор
А. МАКСИМОВ
1-й заместитель главного редактора
И. ЛАПИНСКИЙ
Заместитель главного редактора
О. МЕЛЬНИК
Научные редакторы
В. ВАСИЛЬЕВ,
Е. ГОРЕТКИНА,
С. СВИНАРЕВ,
П. ЧАЧИН
Обозреватели
С. ГОЛУБЕВ, А. КОЛЕСОВ,
С. МАКАРОВ, Н. НОСОВ
Специальный корреспондент
В. МИТИН
Корреспонденты
О. ЗВОНАРЕВА,
М. ФАТЕЕВА
Тестовая лаборатория
А. БАТЫРЬ
Ответственный секретарь
Е. КАЧАЛОВА
Литературные редакторы
Н. БОГОЯВЛЕНСКАЯ,
Т. НИКИТИНА
Фотограф
О. ЛЫСЕНКО
Художественный редактор
Л. НИКОЛАЕВА
Группа компьютерной верстки
С. АМОСОВ, А. МАНУЙЛОВ
Техническая поддержка
К. ГУЩИН, С. РОГОНОВ
Корректор
Л. МОРГУНОВСКАЯ
Тел./факс: (495) 974-2260
E-mail: editorial@pcweek.ru

Отдел рекламы

Руководитель отдела рекламы
С. ВАЙСЕРМАН
Тел./факс:
(495) 974-2260, 974-2263
E-mail: adv@pcweek.ru

Распространение

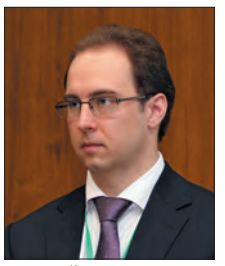
АО "СК Пресс"
Отдел распространения, подписка
Тел.: +7(495) 974-2260
Факс: +7(495) 974-2263
E-mail: distribution@skpress.ru
Адрес: 109147, Москва,
ул. Марксистская, д. 34, к. 10,
3-й этаж, оф. 328

Газета зарегистрирована Комитетом РФ по печати 29 марта 1995 г.
Свидетельство о регистрации № 013458.
Отпечатано в ООО "Доминико",
тел.: (495) 380-3451.
Тираж 35 000.
Цена свободная.
Использованы гарнитуры шрифтов "Темза", "Гелиос" фирмы TypeMarket.

RECS'2016...

ПРОДОЛЖЕНИЕ СО С. 1

и классификации информации в социально-экономической области Казначейства РФ. Прежде всего нужно определить, где формируется каждый эталонный набор данных, ведь сейчас нет эталона даже для ФИО. Концепция Казначейства состоит в том, что эталонными будут считаться данные, сформированные в базовых ресурсах первично (для ФИО это ЗАГС), а дублирующими — их дополнительные правовые статусы, например, в ФМС — ФИО гражданина, в ФНС — ФИО гендиректора и т. д.


Дмитрий Коновалов

В результате обмен данными между ГИС должен существенно упроститься за счет исключения всех дублирующих данных. "В обмене останутся только эталонные данные, т. е. ФИО нужно будет брать только из ЗАГСа, а не из ЕГРЮЛ, Росреестра и т. д.", — пояснил Дмитрий Коновалов.

При этом вместо дублирующих данных будут использоваться только идентификаторы, присвоенные им в соответствующих информационных ресурсах. Эти идентификаторы будут связаны в единой информационной среде ГИС. "Поддерживать актуальность связей идентификаторов существенно проще, чем всего массива данных, но этого достаточно для обеспечения актуальности и достоверности самих данных в ГИС, — считает Дмитрий Коновалов. — И к тому же не нужно будет централизованно хранить все данные. Это дорого и небезопасно. Достаточно хранить только идентификаторы и связи, а сама информация будет находиться в базах данных, которые формируются госорганами в соответствии с их полномочиями. Причем каждый госорган может получить нужную информацию на основе единой модели данных".

Реализация "Единой информационной среды" рассчитана на три года. Уже запущены три проекта: первый связан с разработкой ПО для этой ГИС, второй — с формированием модели данных всех информационных ресурсов федеральных органов исполнительной власти, а третий касается приведения нормативно-правовых актов об информационных ресурсах в соответствие с вышеупомянутым постановлением правительства.

Планируется, что ГИС начнет работать с 1 января 2019 г. и будет контролироваться Минфином, Минэкономразвития и Федеральным казначейством. С этого времени утратят силу постановление правительства о базовых государственных информационных ресурсах и изменения в него, а все госорганы будут выпускать данные в соответствии с постановлением № 487.

И тогда, выразил надежду Дмитрий Коновалов, удастся справиться с проблемой достоверности и актуальности информации в государственных реестрах и регистрах, оптимизировать обмен данными, сократить затраты на ИТ и к тому же создать Big Data — огромный информационный ресурс для аналитики.

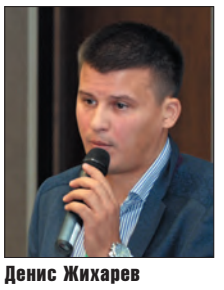
Время покажет, получится ли решить все эти задачи за счет создания еще одной глобальной государственной информационной системы.

ФНС об устранении препятствий на пути к ЭДО

Когда в начале 2000-х Федеральная налоговая служба России начала принимать налоговую отчетность в электронном виде, ее примеру последовали другие госорганы, и это дало толчок для развития межорганизационного электронного документооборота (ЭДО) в нашей стране. В прошлом году доля передаваемых в ФНС налоговых показателей в электронном виде достигла 91,7%, а в этом году ожидается 93%.

Однако, несмотря на такие достижения, еще остается ряд причин, затрудняющих массовое распространение ЭДО. В качестве таких причин Денис Жихарев, консультант отдела интернет-проектов Управления информационных технологий ФНС, назвал увеличение количества формализованных документов, отсутствие возможности направления документов любому контрагенту, невзирая на то, у какого оператора ЭДО он обслуживается, и вопрос хранения юридически значимых электронных документов.

В связи с этим при поддержке Агентства стратегических инициатив, а также на основе предложений и требований бизнес-сообщества был сформирован план мероприятий по совершенствованию налогового администрирования, который затем был утвержден ведомственными приказами. В соответствии с этим планом были подготовлены форматы электронных документов для передачи товаров и результатов услуг при торговых операциях, счетов-фактур и т. д.


Денис Жихарев

Кроме того, ФНС провела работы по представлению неформализованных документов, утвердив за последнее время более 40 форм таких документов.

И наконец, план совершенствования налогового администрирования содержит требования по организации взаимодействия контрагентов, т. е. роуминга. "На этом сильно настаивал бизнес, и в этом году мы начали работу в данном направлении", — сказал Денис Жихарев.

В результате были внесены изменения в существующие нормативные документы, регулирующие порядок предоставления счетов-фактур в электронной форме, и теперь операторы ЭДО обязаны давать организациям возможность взаимодействия с любым контрагентом. В апреле этого года вышел соответствующий приказ ФНС, согласно которому до 1 октября операторы ЭДО должны предоставить ФНС документы, подтверждающие реализацию роуминга.

В качестве основной схемы в ФНС выбрали способ взаимодействия через роуминговый центр. "На сегодняшний день это наиболее приемлемая схема", — сказал Денис Жихарев, добавив, что на данный момент три оператора ЭДО получили паспорта о присоединении к сети доверенных операторов, а документы ряда других операторов находятся на рассмотрении в ФНС. Предполагается, что скоро порядка десяти операторов будут удовлетворять новым требованиям.


Анатолий Миклашевич

Еще остаются вопросы, которые предстоит решить в ближайшее время. Один из них связан с хранением электронных юридически значимых документов и электронной подписи. Ведь электронный документооборот невозможно организовать без электронной подписи. Собственно говоря, ее появление и стимулировало переход на ЭДО. Но сроки действия электронной подписи и сертификата ее ключа ограничены, поэтому пока неясно, как при длительном хранении обеспечить подтверждение того, что документ легитимен.

По словам Дениса Жихарева, существуют два способа хранения юридически значимых документов, каждый из которых имеет плюсы и минусы. Первый предусматривает автоматическое переподписание документов после окончания срока действия предыдущего ключа электронной подписи. Здесь преимуществом является простота, а недостатком то, что юридическая значимость документа подтверждается не изначальной электронной подписью. Второй способ связан с проставлением метки времени в момент первичного подписания документа электронной подписью. В данном случае плюс состоит в том, что документ создается один раз и в любой момент может быть проверен, а минус — в необходимости специализированного ПО при подписании документа.

Успокаиваться рано

О том, что перечисленные проблемы необходимо решать, свидетельствуют данные ФНС, согласно которым, несмотря на стремительный рост популярности ЭДО, на бумаге (в сканированном виде) до сих пор передаются 10 млрд. счетов-фактур в год, а средствами юридически значимого ЭДО — лишь 100 млн., т. е. 1% от общего количества.

По мнению Анатолия Миклашевича, исполнительного директора ассоциации РОСЭУ, одна из причин такой ситуации связана с тем, что операторы ЭДО, преследуя свои коммерческие интересы, сдерживали процесс роуминга.

Ведь в РОСЭУ еще в 2012-м разработали отраслевой стандарт для обмена счетами-фактурами между операторами. "Тогда мы думали, что это станет катализатором бурного развития в области такого обмена, но прошло четыре года, а особой активности не наблюдается", — посетовал Анатолий Миклашевич.

Но теперь дело, возможно, сдвинется, поскольку ФНС, заинтересованная в том, чтобы избавиться от бумаги и сканированных документов, стала продвигать идею роуминга. Сейчас уже имеются два роуминговых центра — "1С" и Ростелекома, а операторы ЭДО, как отметил выше Денис Жихарев, активно занимаются перерегистрацией в ФНС. "Таким образом, процесс пошел, но пока еще не ясно, приведет ли это к бурному развитию ЭДО", — заметил Анатолий Миклашевич.

По его мнению, успокаиваться еще рано, т. к. несмотря на развитие законодательной основы для ЭДО, остается немало проблем, главной из которых является несовместимость форматов электронных документов, созданных в разных системах ЭДО: "Спасибо хоть, что унифицировано то, что относится к налогам. А остальное остается несовместимым, и как только начинается общение, системы не понимают друг друга. Нужна стандартизация форматов документов".

Большие данные...

ПРОДОЛЖЕНИЕ СО С. 3

доставлять эту информацию клиентам. Также система будет использоваться для внутренних нужд компании. "В рамках проекта Big Data мы будем отслеживать специфику развития нашего продуктового ряда", — объяснил Андрей Иванов.

Кроме того планируется использовать технологию блокчейн, которая позволит объединить в одну систему Сбербанк как банк, финансирующий сделки, со всеми сторонами сделки: продавцами, покупателями, таможней, налоговой инспекцией, санинспекцией, перевозчиками.

"Глобальная цель данной платформы простирается очень далеко. Это, в общем, создание с применением технологии блокчейн абсолютно новой экосистемы, которая сделает внешнюю торговлю абсолютно другой по сравнению с тем, что имеется сегодня",— сказал Андрей Иванов.

Как объяснил нам технический специалист Сбербанка, в настоящее время проводятся исследования возможности использования для этих целей блокчейн-платформы Hyperledger, хотя впоследствии выбор может быть изменен, т. к. существует большое количество проблем, которые мешают использованию этой платформы в промышленной эксплуатации.

Впрочем, как считает специалист, если к плюсам Open Source-решений, к которым относится Hyperledger, добавить плюсы промышленных разработок, которые будет вести сам Сбербанк, то в итоге можно будет решить существующие проблемы.

У новой Tele2 новая ERP-система

Начав работу на российском рынке в 2003 г. с запуска сети GSM в нескольких регионах, Tele2 прошла путь от небольшого регионального оператора до игрока федерального уровня. В марте 2013 г. шведский концерн **ИНТЕРВЬЮ** *Tele2 AB продал российское подразделение группе ВТБ. В феврале 2014 г. Tele2 и "Ростелеком" объявили об объединении мобильных активов на базе Tele2 и создании нового федерального оператора. Теперь Tele2 работает в 65 регионах России, включая Москву.*

Интеграция сотовых активов "Ростелекома" и активное строительство сетей 3G/4G в регионах потребовали значительных изменений в корпоративном управлении и приведения его в соответствие с новыми масштабами бизнеса. В 2014 г. руководством компании был инициирован проект внедрения SAP ERP на in-memory-платформе БД SAP HANA, завершенный в конце 2015 г. О целях и задачах проекта, об особенностях его реализации с финансовым директором "Tele2 Россия" ***Людмилой Смирновой*** *беседует обозреватель PC Week* ***Сергей Свинарев****.*

Людмила Смирнова

PC Week: Какова общая цель данного проекта и можно ли говорить о том, что внедрение ERP-системы в Tele2 завершено?

ЛЮДМИЛА СМИРНОВА: В качестве первоочередной стояла задача централизации всех функций финансового учета и управления в ОЦО — Общем центре обслуживания группы компаний (по сути — единой централизованной бухгалтерии). Наряду с финансовым контуром, который обеспечивает работу ОЦО, внедрение SAP ERP призвано автоматизировать и другие бизнес-процессы Tele2. Уже сегодня с помощью SAP ERP ведется управление процессами строительства, логистики и складскими операциями. В планах — управление процессами ремонта и технического обслуживания, более детального учета складских запасов, а также подключение к закупочному облачному сервису SAP Ariba. В более отдаленной перспективе возможно внедрение HR-модулей SAP, но окончательный выбор еще не сделан. За продажи у нас отвечает специализированная биллинговая система другого вендора.

Мы считаем, что внедрение в том объеме, что был запланирован, завершено. Совершенно очевидно, что такие системы, как SAP ERP, имеют большой потенциал развития. Я уже говорила о наших планах по внедрению ряда дополнительных модулей, а кроме того, на очереди переход на последние версии средств анализа и отчетности SAP BW, PCM (Profitability and Cost Management) и BPC (Business Planning and Consolidation), формально не входящие в состав SAP ERP. Общая цель внедрения SAP ERP — полное обеспечение управления всеми рисками компании. Старые системы не позволяли делать это в полной мере, так как компания очень сильно выросла и увеличился объем контролируемых ею данных, а их качество в условиях разобщенности систем оставляло желать лучшего. Даже формирование ежемесячной отчетности требовало значительных усилий и затрат времени. Цена каждой ошибки становится неприемлемо высокой. Никаких формальных оценок ожидаемого экономического эффекта мы не делали, поскольку для нас очевидны выгоды от повышения качества управления и прозрачности бизнеса для менеджмента.

PC Week: Какие бизнес-приложения использовались для управления Tele2 до этого? Чем они не устраивали вашу компанию? Все ли они заменены модулями SAP ERP?

Л. С.: Мы приступили к внедрению в июле 2014 г. и на запуск первой волны, в рамках которой к системе подключались три с лишним тысячи пользователей из компаний группы, уже обращавшихся в то время к ОЦО, у нас ушло 12 мес. Вторая волна, завершившаяся в ноябре 2015-го, подразумевала окончание интеграции и переход на обслуживание ОЦО компаний, которые присоединились к Tele2 в результате сделки с "Ростелекомом". В октябре в SAP ERP были переведены последние подразделения, не охваченные по тем или иным причинам второй волной.

В компаниях первой волны до этого использовался продукт Scala вместе с решением для транзакционной обработки финансовых документов в ОЦО на платформе IBM FileNet. Система была слабо интегрирована, перенос информации из FileNet в Scala осуществлялся вручную, аналитики в обеих системах не совпадали. Для задач бюджетирования и финансового планирования использовалась платформа SAP BPC, в которой присутствовали свои аналитики. Все это было крайне неудобно для конечных пользователей, которым при заполнении документов приходилось держать в уме и правильно вводить три набора аналитик: бюджетных, документационных и учетных. Компании, пришедшие в Tele2 из "Ростелекома", применяли более широкий спектр продуктов: там были и Platinum, и Oracle, и "1С", и самописные решения. В рамках их интеграции в оргструктуру Tele2 предусматривался переход на единую систему учета и управления на базе одного, общего для всей компании продукта.

Хочу отметить, что наша система SAP ERP развернута в российском облачном ЦОДе SAP на платформе SAP HANA Enterprise Cloud (HEC): мы были первым облачным клиентом SAP в России.

PC Week: Какие системы Tele2 нуждаются в интеграции с SAP ERP?

Л. С.: Предстоит интеграция решения по формированию доходной части в ERP с биллинговой системой, уже осуществлена агрегация с электронным документооборотом на базе FileNet. Ввод документов и хранение их скан-образов ведется в FileNet, а их транзакционная обработка осуществляется в SAP ERP. Сейчас рассматривается новый проект по потоковому вводу и распознаванию печатных форм документов на платформе ABBYY, результатом которого станет исключение ручного ввода финансовых документов и автоматическая их передача в SAP ERP.

PC Week: Кто является генподрядчиком данного проекта? Сколько специалистов Tele2 было задействовано в нем?

Л. С.: Первые две фазы проекта были выполнены компанией Bearing Point, а для последующей поддержки и развития системы мы сформировали пул отечественных системных интеграторов, обладающих экспертизой по тем или иным функциональным модулям. На разных этапах число задействованных специалистов Bearing Point варьировалось (иногда одновременно работало более сотни человек). Со стороны Tele2 был один выделенный сотрудник, который занимался только этим проектом, и еще около 25 человек из разных подразделений совмещали это со своими основными обязанностями. В основном это были специалисты из департамента методологии, руководители ОЦО, сотрудники операционных подразделений. На местах был сформирован институт ключевых пользователей, которые приняли на себя всю основную нагрузку по запуску системы, когда к ней подключилось более 4000 пользователей из 65 региональных подразделений (весь штат Tele2 — 8000 человек). Их нужно было обучить, и для этого мы использовали видеолекции, веб-семинары, а также знания тех самых ключевых пользователей (их было около 150). Все это позволило всем подразделениям перейти на эксплуатацию системы в течение одного дня.

PC Week: Сказалось ли на бюджете проекта снижение курса рубля? Рассматривались ли в этой связи какие-либо "импортозамещающие" варианты?

Л. С.: Нет, не сказалось. Лицензии на ПО SAP мы покупали весной 2014 г., т. е. еще тогда, когда курс рубля был стабилен. Оплата услуг облачного ЦОДа по модели HEC также исчислялась исходя из стоимости оборудования по докризисному курсу рубля. Прайс-лист на услуги Bearing Point рублевый, и расценки внедренца на протяжении всего проекта не пересматривались. Поэтому вопросы импортозамещения для нас были неактуальны. В какой-то мере импортозамещением можно считать передачу сопровождения и развития системы отечественным системным интеграторам. Но особой экономии это нам не дает, поскольку расценки на услуги российских и западных SAP-консультантов примерно одинаковы (отличаются не более чем на 25%) и зависят в большей степени от уровня их экспертизы по тем или иным направлениям. Они сохранились на доинфляционном уровне 2014 г.

PC Week: Почему была выбрана редакция SAP ERP на платформе HANA? Какие ее особенности принимались во внимание в первую очередь? Рассматривались ли альтернативные варианты?

Л. С.: У Tele2, как компании-дискаунтера, всегда была корпоративная установка: никогда не запускать в эксплуатацию новые продукты первыми. Мы не из тех компаний, которые любят раньше других пробовать инновационные решения, находить их достоинства и недостатки, набивать себе шишки и зарабатывать бесценный опыт. Но в ИТ-индустрии развитие идет настолько быстро, что, начиная внедрять сегодня какое-либо решение, вполне может оказаться, что уже через пару лет оно устареет. Так у нас произошло с SAP BPC. Мы внедряли в 2011-м версию 7.5 на платформе СУБД MS SQL Server. Уже тогда была доступна более новая версия, но мы от нее отказались. Сейчас объявлено, что версия 7.5 перестает поддерживаться вендором. Сегодня мы внедряем новейшую версию BPC 10.1 на платформе HANA, которую кроме нас, мне кажется, во всем мире внедряет пока только Lufthansa. Проект очень сложный и требует дополнительной отладки процессов, в чем нам очень помогает служба поддержки SAP. Но мы можем быть уверены, что система послужит нам много лет.

Эти соображения мы имели в виду, делая выбор и в пользу SAP ERP on HANA. Мы отдаем себе отчет, что стратегически SAP делает ставку на платформу HANA и в отдаленной перспективе нам так или иначе пришлось бы переходить на эту инновационную in-memory-платформу. Но, кроме того, мы предъявляли повышенные требования к быстродействию системы при обработке больших массивов записей. В частности, у нас есть отдельные довольно сложные и объемные формы ввода информации, заполнение которых в старой системе сопровождалось длительными задержками.

PC Week: Чем объясняется развертывание SAP ERP в облаке HANA Enterprise Cloud (HEC) на базе российского ЦОДа SAP, а не в ростовском корпоративном ЦОДе Tele2?

Л. С.: Облачное развертывание позволило нам не приобретать дорогостоящие серверы с большим объемом оперативной памяти и иное оборудование. Они принадлежат поставщику облачных услуг и оплачиваются нами вместе с поддержкой в рамках подписки в соответствии с объемом используемых ресурсов. Сначала мы не совсем точно определили требуемый объем, и его пришлось быстро наращивать в ходе развертывания системы. Думаю, в своем ЦОДе нам сделать это в отсутствие экспертизы по платформе HANA было бы очень трудно. Если бы мы сами покупали лицензии и оборудование, то легко могли промахнуться в ту или другую сторону и ответственность за это ложилась бы полностью на нас. А в облачном варианте мы можем варьировать объемы задействованных программно-аппаратных ресурсов в любую сторону и платить только за то, что реально используем. Мне, как финансовому директору, также очень важно, что нам не нужно единовременно инвестировать большие суммы и денежный поток распределяется равномерно по календарным периодам. В целом все это приводит к снижению целого ряда рисков.

То, что в качестве облачного провайдера HEC мы выбрали российский ЦОД SAP, объясняется целым рядом причин технического и нормативного характера, а также тем, что этот ЦОД наполовину принадлежит нашему крупнейшему акционеру — "Ростелекому", что снимает для нас ряд рисков информационной безопасности. С учетом крайне невыгодного нынешнего валютного курса вариант аренды услуг HEC в зарубежном облачном ЦОДе даже не рассматривался. Возможное развертывание системы в нашем собственном ЦОДе имеет два важных недостатка: необходимость больших начальных затрат и отсутствие у специалистов нашего ЦОДа компетенций в области SAP HANA.

PC Week: Насколько велики объемы данных, которыми будет оперировать SAP ERP в Tele2? Все ли они находятся в БД HANA или какая-то часть останется в традиционных дисковых БД?

Л. С.: Используемые нами серверы имеют ОЗУ суммарным объемом 7 Тб. Мы в дальнейшем будем хранить все данные ERP-системы на HANA и полностью отказываемся от дисковых СУБД. Унаследованные данные за прошлые годы остаются в прежних системах в качестве архива и в SAP ERP не переносятся. Был лишь переходный период в середине 2015 г., когда после внедрения SAP ERP нам пришлось временно вести параллельную обработку данных в старой и новой системах. Для всех данных, необходимых для текущей оперативной работы, оперативной памяти HANA-серверов вполне достаточно. Предварительно нами проводился сравнительный анализ стоимости облачных конфигураций на базе HANA и SQL Server с учетом стоимости аппаратных компонентов, и оказалось, что они не очень сильно различаются.

PC Week: В настоящее время SAP продвигает новое поколение своей ERP-системы — SAP S/4HANA. Планирует ли Tele2 переходить на эту систему?

Л. С.: Мы присматриваемся к SAP S/4HANA, изучаем ее возможности и достоинства,

ПРОДОЛЖЕНИЕ НА С. 9 ▸

Обновление продуктов Schneider Electric для ЦОДов:
DCIM и комплексный контроль за состоянием среды и безопасности

Хранить информацию и размещать новые сервисы в рамках традиционной ИТ-инфраструктуры год от года становится сложнее. Большие данные органично перетекают в облака, предлагающие эффективный инструментарий и значительные компьютерные мощности для их обработки, а бизнес-заказчики для размещения своих сервисов и данных всё чаще выбирают специализированные ЦОДы — либо арендуя у провайдера необходимые вычислительные мощности, либо размещая на внешней площадке собственное оборудование.

Нагрузка на эксплуатационные и административные службы провайдеров непрерывно растет. Вместе с ростом сложности услуг растут ответственность и риски. Теперь необходимо не просто самим контролировать серверную и инженерную инфраструктуру, но и предоставлять информацию о её состоянии клиентам, обеспечивать различные уровни безопасности, управлять имуществом. Заказчики, делающие выбор в пользу операторских площадок, выдвигают повышенные требования относительно возможностей по удаленному мониторингу среды, качества и управлению своим имуществом.

Новая модель NetBotz 250

Со стороны службы эксплуатации площадки ошибки планирования и неоптимальное распределение ресурсов между имеющимися потребителями в условиях растущих нагрузок чреваты их выходом из строя и нарушением контрактных обязательств. Часто невозможность проактивно или своевременно отреагировать на сбои в функционировании инженерных систем или на несанкционированные действия в ЦОДе может грозить ещё более ощутимыми материальными потерями. Для противодействия этим угрозам и снижения рисков уже предлагается обширный и проверенный инструментарий. В частности, компания Schneider Electric продолжает совершенствовать свой набор DCIM (Data Center Infrastructure Management), который служит для многостороннего мониторинга оборудования ЦОДов и решения большинства задач управления ресурсами. Решение органично охватывает всю инженерную и ИТ-инфраструктуру, упрощая решение множества задач, стоящих перед провайдерами услуг централизованного хранения и обработки данных.

Система активного мониторинга NetBotz

Любой серьёзный сбой в системах жизнеобеспечения ЦОДа, будь это внезапная протечка трубопровода, сниженное время автономной работы ИБП или несанкционированные действия, может привести к серьёзным потерям или катастрофическим последствиям для серверной инфраструктуры. Именно поэтому ответственные провайдеры услуг хранения и обработки данных так много внимания уделяют активному мониторингу всей имеющейся инженерной инфраструктуры. Для решения этих задач компания Schneider Electric предлагает масштабируемую систему активного мониторинга NetBotz, позволяющую организовать наблюдение за машинными залами, технологическим и ИТ-оборудованием.

NetBotz позволяет обезопасить физическую составляющую ЦОДа от разнообразных факторов риска, связанных с умышленным или спровоцированным естественными причинами физическим воздействием. Отслеживаются изменения климатических параметров, аварии на инженерных коммуникациях, доступ к стойкам, наличие и действие людей в помещениях и т. д. Новейший представитель этой линейки — монтируемый в стойку контроллер NetBotz 250, способный собирать информацию с 78 внешних датчиков (47 из которых могут быть беспроводными), поддерживающий до двенадцати модулей расширения (Sensor Pod 150, Wireless Sensor Pod и др.) и имеющий на борту встроенный контроллер СКУД и релейные выходы.

NetBotz 250 может использоваться самостоятельно, например, если необходимо оснастить мониторингом и контролем доступа отдельное помещение, телекоммуникационный узел или шкаф, т. к. имеет собственную сетевую консоль управления и веб-интерфейс. Контроллеры NetBotz поддерживают одноименную линейку разнообразных датчиков и аксессуаров и даже обладают возможностью работы в качестве самостоятельной системы мониторинга, с отправкой тревожных сообщений по электронной почте и SMS. В то же время, как подчёркивает производитель, максимальный эффект от внедрения мониторинга достигается при объединении всей сети NetBotz в централизованную систему мониторинга Data Center Expert.

Система мониторинга Data Center Expert входит в фирменное решение Schneider Electric, которое является лидером в так называемом классе DCIM-систем. Data Center Expert агрегирует данные от инженерного оборудования машинных залов и от сети NetBotz, за счёт чего обеспечивает службу эксплуатации единым инструментом мониторинга, что подразумевает оповещения, отчёты и разнообразные средства для проактивных действий, снижающих риски и минимизирующих тяжесть потенциальных аварий в случае их возникновения. Система уже “из коробки” имеет ряд необходимых в современном ЦОДе функций, которые зачастую отсутствуют в классических решениях типа BMS и SCADA — это, например, централизованное видеонаблюдение и контроль доступа к стойкам. К преимуществам системы относится то, что после внедрения масштабирование под новых клиентов или помещения совершенно не требует привлечения разработчиков. Затраты и время на расширение несопоставимо меньше, чем при использовании промышленных решений.

Платформа Schneider Electric StruxureWare для дата-центров

Средства мониторинга Data Center Expert и NetBotz являются модулями программной платформы StruxureWare for Data Centers, применяемой в ЦОДах для ведения процедур и регламентов, обеспечивающих высокую утилизацию и производительность ресурсов физической инфраструктуры, а также для снижения рисков и ошибок, возникающих в процессе эксплуатации. Благодаря своей модульной природе StruxureWare for Data Centers допускает адаптацию к потребностям ЦОДов любых масштабов с самыми разными требованиями к сложности организации процессов и надёжности. В результате одна такая платформа позволяет принимать обоснованные решения на всех уровнях компетенции — от установки дополнительного сервера (уровень специалиста ИТ-службы) до модернизации всего ЦОДа в целом (уровень владельца бизнеса).

Фреймворк StruxureWare for Data Centers образован модулями трёх типов, предназначенными для целей мониторинга, операционной деятельности и аналитики. Продуманная структура программной платформы предоставляет возможность различным группам специалистов на предприятии получать необходимую информацию для принятия решений. При этом каждая группа располагает доступом к данным в соответствии со своим уровнем компетенции и ответственности, а каждый сотрудник внутри неё оказывается обеспечен удобным интерфейсом для получения и анализа данных.

Версия StruxureWare Data Center Operation 8.0 обладает расширенной функциональностью для управления инженерной и ИТ-инфраструктурой

Новая версия Data Center Operation 8.0 имеет ряд новых функций. Например, платформа стала обеспечивать клиентов коммерческих ЦОДов собственным кабинетом для контроля ресурсов и управления имуществом, размещённым в ЦОДе коммерческого провайдера.

“Мы модифицировали платформу, чтобы удовлетворить потребности по крайней мере трёх категорий пользователей, — пояснил Андрей Ивашов, руководитель по развитию бизнеса (DCIM) компании Schneider Electric в регионе СНГ. — Во-первых, это менеджмент ЦОДа, которому важны реальные показатели затрат, утилизации и эффективности использования ресурсов. Во-вторых, операторы ЦОДа и инженеры. Для ускорения работ по инсталляции, аудиту и перемещению оборудования они смогут, например, воспользоваться веб-интерфейсом, доступным и на мобильных устройствах. И, в-третьих, это клиенты коммерческих площадок, которые теперь могут контролировать свои активы, расположенные на площадке оператора, через личный кабинет”.

Так, веб-клиент, интегрированный в StruxureWare Data Center Operation 8.0, позволяет использовать любой стандартный браузер (в том числе на мобильном устройстве) для таких задач, как инвентаризация, поиск оборудования, аудит, фиксация основных параметров потребления ресурсов и нагрузки. А клиенты благодаря созданному для них порталу получают оперативный доступ к аналитической информации о внутреннем состоянии ЦОДа (арендованных комнатах, секциях и стойках), доступной и потребляемой электрической мощности, температуре, влажности и прочих существенных для функционирования оборудования параметрах. Немаловажное новшество — предоставление клиентам доступа к панели с ключевыми показателями эффективности (KPI). Всё это позволяет коммерческому провайдеру предлагать дополнительные услуги на базе системы DCIM, гибко контролируя доступ клиентов к порталу в целом или к определённой информации.

Одна из ключевых областей компетенции Schneider Electric — высоконадёжное и стабильное электропитание для компьютерного оборудования. Не удивительно, что в StruxureWare Data Center Operation 8.0 особое внимание уделено планированию распределения питания (для постоянного и переменного токов) и контролю соответствующих рисков. “В новой версии появилось несколько ключевых функций, позволяющих учитывать распределение нагрузки на источники электроэнергии и взаимовлияние компонентов, а также проактивно контролировать уровень резервирования, — пояснил Андрей Ивашов. — Мы также анонсировали поддержку моделирования систем постоянного тока, что должно пригодиться операторам связи. Кроме того, через организацию регламентов новая версия системы позволяет повысить уровень утилизации ресурсов ЦОДа и сократить время на выполнение ряда работ. Эти и другие новые функции помогут уменьшить количество ошибок, влияющих на устойчивость инфраструктуры”.

Как утверждают в Schneider Electric, это первое на рынке решение DCIM, позволяющее в случае совместного использования в ЦОДе систем постоянного и переменного тока обеспечивать управление и планирование нагрузки для них через единый интерфейс.

Ещё одно важное новшество восьмой версии StruxureWare Data Center Operation — усовершенствованная модель энергопотребления, созданная на основе отзывов многочисленных пользователей прежних версий фреймворка. В этой модели модернизированы схемы контроля и прогнозирования доступной мощности в стойках. В результате появляется возможность на основе данных реальных измерений оптимальным образом загружать каждую стойку оборудованием, сокращая риски, связанные как с перегрузкой, так и с недоиспользованием ресурсов.

“Владельцы корпоративных и коммерческих ЦОДов сталкиваются с тем, что в силу высоких темпов развития технологий и бизнеса количество задач, стоящих перед эксплуатационной командой, увеличивается. Ограничения по численности этой команды и недостаток “умных” инструментов повышают риски при эксплуатации инфраструктуры, — говорит Андрей Ивашов. — Новая версия нашей платформы StruxureWare Data Center Operation становится более удобной для визуального контроля энергетических и физических зависимостей, а также для инвентаризации оборудования в ЦОДах. Это позволяет снизить риск человеческой ошибки при планировании и проведении изменений. Появился также функционал, который интересен коммерческим площадкам, это многопользовательская версия с порталом для клиентов. Таким образом, версия 8.0 становится операторским инструментом и поможет провайдерам расширить число предоставляемых услуг и повысить их качество”.

"Успехи Open Source объясняются взрослением ИТ-рынка"

Модель Open Source, которая еще десять лет назад считалась нишевым направлением и возможности использования которой корпоративными заказчиками подвергались сомнению многими экспертами, сейчас однозначно признана ключевой частью мировой ИТ-отрасли. В той или иной мере открытые методы разработки и продвижения ПО сейчас используют в своей работе практически все заметные ИТ-вендоры, при том что для многих успешных ИТ-компаний она стала основой их бизнеса. Общепризнанным фактом является и то, что именно Open Source — один из главных локомотивов создания и внедрения инноваций, в том числе в таких направлениях, как облака, мобильность, большие данные. Уже давно исчезло недоверие к открытому ПО у широкого круга клиентов, включая самые крупные компании мира. О роли Open Source в современном ИТ-мире и о возможностях участия России в развитии этого ИТ-направления с директором по маркетингу в регионе EMEA компании Red Hat ***Бренданом Макэрланом*** *беседовал обозреватель PC Week* ***Андрей Колесов****.*

PC Week: В чем причины успеха модели Open Source, в который мало кто верил полтора десятка лет назад?

БРЕНДАН МАКЭРЛАН: Фундаментальная причина в том, что развитие ИТ-рынка достигло в конце прошлого столетия такого уровня зрелости, когда для дальнейшего прогресса потребовались новые модели разработки и внедрения ИТ. И традиционная проприетарная модель уже не поспевала за новыми вызовами, не отвечала растущим требованиям постоянно расширяющегося круга пользователей.

До недавнего времени в широком общественном мнении применение Open Source связывалось с возможностью экономии денег при приобретении ПО. Наши расчеты и опыт наших заказчиков показывают, что снижение затрат действительно есть, причем оно весьма существенно. Есть и другие оценки, которые говорят, что с точки зрения совокупной стоимости владения Open Source не имеет заметных преимуществ перед проприетарными продуктами Однако открытое ПО позволяет перенести тяжесть финансовых затрат с капитальной составляющей на операционную, реализуя сервисную модель предоставления ИТ заказчикам (которая является фундаментом облачных схем использования ИТ), что очень важно для бизнеса, особенно — для развивающегося. А современная мировая экономика базируется именно на динамично развивающейся модели бизнеса.

И все же финансовые аспекты далеко не самые главные. Модель Open Source позволила вывести процесс создания ПО за рамки центров разработки вендоров. Какими бы крупными ресурсами ни обладали ИТ-гиганты вроде IBM, Microsoft и Oracle, их уже недостаточно для обеспечения динамики развития современных ИТ. Да, можно наращивать центры разработки компаний, но при этом возникают проблемы управления огромными коллективами. Нужны новые модели реализации крупных проектов, как раз их и предложила концепция Open Source. Более того, идея Open Source позволила вовлечь в процесс создания инноваций заказчиков. Конечно, многие предприятия и раньше имели свои отделы разработки ПО, но, во-первых, модель Open Source упростила модернизацию внедренных продуктов, а во-вторых, позволила реализовать обратную связь, дав возможность внутренним разработчикам в той или иной степени участвовать в создании открытого ИТ-продукта.

Брендан Макэрлан

PC Week: Что можно сказать о влиянии Open Source на разработчиков ПО и его пользователей?

Б. М.: Что касается разработки ПО, то тут все представляется довольно очевидным: именно Open Source является уже многие годы главной силой создания ИТ-инноваций. Не единственной, но — можно сказать с большой долей уверенностью — ведущей. И эта лидирующая роль только повышается. Практически все основные ИТ-тенденции последних лет — облака, мобильность, большие данные, IoT — или имели в своей основе открытые проекты, или же в существенной мере были связаны с ними. В первом десятилетии этого столетия прорывной технологией была виртуализация, развитие которой шло в основном в рамках проприетарной модели. Но в нынешнем десятилетии средства виртуализации развиваются при растущем участии Open Source. Примером этого являются, в частности, проекты OpenStack и Docker. Уже то, что Microsoft (и не только она) в своем бизнесе все шире использует открытые проекты и активно сотрудничает с сообществом Open Source, говорит само за себя.

Что касается заказчиков, то среди них популярность открытого ПО также быстро растет, но тут наблюдаются более сложные процессы. Поначалу для них основным мотивом использования Open Source была бесплатность такого ПО. Хотя многих как раз это и пугало, так как все отлично знают, где бывает бесплатный сыр. Но потом на передний план преимуществ стала выходить гибкость открытого ПО, которая крайне важна для динамически меняющихся условий бизнеса. И дело тут не только в возможности доработки и адаптации ПО под себя, но в большей гибкости управления финансовыми затратами. Перенос тяжести затрат с капитальной части на операционную позволяет оптимизировать расходы, на практике реализуя схему "по требованию", что особенно важно, если требования постоянно меняются, причем, как правило, в сторону роста.

PC Week: В последние годы мы видим еще одну важную роль ИТ-отрасли. Она выступает не только как поставщик собственно ИТ, но и как пример качественно новых бизнес-моделей, которые теперь все шире берут на вооружение компании традиционного бизнеса. Как в этом участвует движение Open Source?

Б. М.: Самым непосредственным образом! Сегодня новые бизнес-модели становятся даже более важными, чем технологии, хотя, конечно, мы понимаем их диалектическую взаимосвязь. И пример тут подает Open Source! Посмотрите: первыми методы открытого ПО взяли на вооружение ранее непримиримые противники — проприетарные вендоры. Сейчас мы видим, как подобные методы разработки новых систем начинают использовать предприятия телекома и банки. Нет сомнений, что распространение открытых моделей ведения бизнеса будет расширяться.

PC Week: Серьезным препятствием распространению Open Source для многих клиентов было и отсутствие привычного вендора, который так или иначе, но обеспечивал не только текущую поддержку программных продуктов, но и гарантированное их развитие в перспективе.

Б. М.: Эта проблема очень четко обозначилась на рубеже веков, и как раз ее решением стало появление Red Hat, а потом и других компаний, которые занялись профессиональным бизнесом на основе модели Open Source. Разумеется, нам тоже поначалу пришлось завоевывать доверие рынка, что особенно важно при работе с крупными корпоративными клиентами. Но лет десять назад наша компания стала признанным ведущим игроком этого рынка, и последние годы вопрос доверия к нашим продуктам и услугам вообще не стоит.

PC Week: Созданием открытого ПО занимаются как сообщества разработчиков, так и коммерческие компании вроде вашей. Как строятся отношения между ними?

Б. М.: Я уже сказал выше, что успех модели Open Source связан с переходом ИТ-рынка на новый уровень зрелости. Соответственно и сама эта модель является более сложной по сравнению с традиционной проприетарной. Если последняя ранее была как бы одноуровневой для изолированных друг от друга компаний-разработчиков, то сейчас она как минимум двухуровневая. Базовым уровнем разработки является сообщество, community. Здесь создается, если можно так сказать, классически открытое ПО, которым могут пользоваться все желающие, обычно совершенно бесплатно. Но применять такое ПО люди и организации могут исключительно на свой страх и риск, без сколько-нибудь гарантированной технической поддержки. Разумеется, ПО уровня community само по себе достаточно высокого качества, у него есть своя история, рыночный авторитет, вы можете рассчитывать на какую-то помощь со стороны независимых коллег. Но все же очень многим заказчикам такой несколько аморфный вариант ПО не подходит, особенно когда речь идет о его применении для критически важных задач предприятий. И вот тут появляются ИТ-вендоры, предлагающие свой вариант продукта, сформированный по собственным спецификациям (что-то добавлено, что-то исключено), за работоспособность которого они несут ответственность, в том числе в виде технической поддержки и оперативного обновления.

PC Week: В чем тогда различие между Red Hat и проприетарными вендорами, той же Microsoft?

Б. М.: Я бы тут выделил несколько моментов, они все важны и связаны между собой. Первый — мы изначально используем сервисную, а не лицензионную модель взаимоотношений с заказчиком. Мы берем деньги не за собственно ПО, а за его техническую поддержку. Это получается для клиента выгоднее в чисто финансовом плане, к тому же он получает более высокую гибкость в плане выбора нужного ему числа лицензий.

Второй момент — заказчик получает исходный код ПО, зачастую — и исключительно наших (а не от сообщества) модулей. Таким образом, он имеет возможность самостоятельно модернизировать ПО, расширяя его возможности и адаптируя под свои потребности. Да, на практике большинство заказчиков не притрагиваются к исходному коду, но даже для них его наличие очень важно, хотя бы просто потому, что они знают, что в случае необходимости могут воспользоваться им.

Третий по счету, но не по значимости, момент — это получение существенно более высокого уровня независимости от вендора. Об этом говорится давно, но в условиях усложнения политической обстановки в мире российские заказчики — а на их примере и клиенты в других странах — отлично поняли, что за общими разговорами скрываются серьезные реальные проблемы.

PC Week: Откуда берется ПО уровня community? У нас в стране у многих людей, кажется, бытует представление, что оно появляется откуда-то само собой, как некая манна небесная.

Б. П.: Разумеется, тут никаких чудес нет, что-то из ничего никогда не получается. В свое время, на начальном этапе, Open Source появилось как результат академических исследований и хобби энтузиастов. Эти две составляющие имеют и сегодня очень большое значение, но все же сейчас финансовой основой данного уровня разработки является то или иное участие коммерческого рынка (не только ИТ-вендоров, но и ИТ-заказчиков), в некоторых регионах мира, в частности в Европе, заметную роль играет государственное финансирование. Коммерческие компании участвуют в этом, занимаясь непосредственно разработкой программного кода и финансированием отдельных проектов (обычно — не разработки ПО, а для покрытия административных расходов). Но я хотел бы обратить внимание на то, что механизм работы сообщества Open Source построен так, чтобы свести к минимуму принцип "кто платит, тот и заказывает музыку", т. е. речь идет о действительно не зависимых от источников финансирования проектах.

PC Week: Спасибо за беседу.

У новой Tele2...

ПРОДОЛЖЕНИЕ СО С. 7

но конкретных планов перехода на этот продукт у нас пока нет. Если такое решение и будет принято, то произойдет это не раньше середины 2017 г. Наши эксперты из проектной команды отмечают, в частности, более дружественный пользовательский интерфейс SAP S/4HANA на основе технологии Fiori.

PC Week: Были ли заранее установлены какие-то критерии успешности данного проекта?

Л. С.: Tele2 не публичная компания, но мы проходим международный аудит — аудитором является Ernst & Yang. Для аудитора важна прозрачность отчетности и бизнес-процессов, и то, что они подкрепляются авторитетом системы SAP ERP, тоже имеет определенное значение.

Для нас успех заключается уже просто в том, что система работает и выполняет все необходимые функции гораздо лучше, чем старая. Все процессы функционируют без сбоев, отчетность выпускается своевременно и подтверждается аудиторами. Конечно, любое внедрение оставляет какие-то узкие места и требует их расшивки. Причина, как правило, в том, что мы при внедрении старались в максимальной степени использовать стандартные процессы, заложенные в SAP ERP. Это позволяет существенно снизить затраты на внедрение и ускоряет его. Однако некоторые процессы, например при планировании строительства, оказались чересчур сложными и трудозатратными. Теперь мы постепенно пересматриваем и корректируем реализацию таких бизнес-процессов в ERP-системе. У нас с этой целью инициирован отдельный проект SAP 2.0, который реализуется отечественными интеграторами, взявшими на себя сопровождение и развитие системы.

PC Week: Благодарю за беседу.

Как монетизировать ИТ-безопасность

ВАЛЕРИЙ ВАСИЛЬЕВ

ОБЗОРЫ

Российские организации и компании очень неохотно публикуют сведения об ИБ-инцидентах. Стремление не выносить сор из избы усложняет организацию консолидированного (в отраслевых и национальных масштабах) противодействия киберпреступности и реалистичную оценку последствий кибератак.

В таком отношении к инцидентам ИБ наша страна не является особенной. Так, Агентство ЕС по сетевой и информационной безопасности (European Union Agency for Network and Information Security, ENISA) отмечает, что в публиковавшихся до сего времени отчетах по Европе о потерях из-за кибератак данные редко бывают сопоставимы между собой ввиду сильного различия используемых для расчетов подходов и методов, часто имеющих значение только в конкретном контексте.

В ENISA считают, что нужны унифицированные и стандартизированные подходы, а некоторые эксперты предлагают определить единый метод измерений, чтобы исследование потерь от киберпреступлений в разных странах и отраслях стало более простым и эффективным. Предполагается, что одобренное Европарламентом новое законодательство, обязывающее компании сообщать о кибератаках, упростит решение этой задачи. Публичность данных об ущербах от ИБ-инцидентов поможет строить реалистичные модели угроз, даст возможность коллективными усилиями сообщества специалистов разработать методики оценки таких ущербов, а сами эти методики станут мощным инструментом в руках бизнес-руководителей и руководства корпоративных ИБ-служб для адекватного определения места информационной безопасности в каждой конкретной структуре, в планировании и обосновании бюджетов на ИБ.

В нашем обзоре мы обсудим, насколько расходы российских компаний и организаций на обеспечение ИБ адекватны реальным угрозам в этом отношении, что следует предпринять в плане формулирования нормативных требований, создания методик расчета расходов на ИБ, разработки современных ИБ-инструментов, организации ИБ внутри компаний, подготовки ИБ-специалистов, чтобы сделать эти расходы более соответствующими современному ландшафту ИБ-угроз и эффективными с точки зрения их окупаемости.

Расходы на ИБ: много, мало или достаточно?

Сбербанк оценил общий ущерб российской экономики от кибератак в 2015 г. в 600 млрд. руб., а Фонд развития интернет-инициатив — примерно в 200 млрд. Как видим, данные заметно разнятся. Одной из главных причин столь сильных расхождений в оценках эксперты считают сокрытие российскими компаниями сведений об инцидентах ИБ. Мотивация для этого очевидна: никто не хочет нести репутационные потери, которые в высококонкурентных рыночных сегментах (например, в кредитно-финансовом) весьма ощутимы.

Изменить ситуацию в лучшую сторону помогло бы закрепление в законодательстве норм, обязывающих публично объявлять о кибератаках и нанесенных ими ущербах. Именно по таким правилам уже не один год живут компании в США, а совсем недавно начали жить и в Евросоюзе.

Нужно сказать, что и в России ведущие игроки зрелых рынков (в качестве примера можно упомянуть ту же кредитно-финансовую отрасль) уже ощутили преимущества обмена информацией об инцидентах ИБ. Сначала это было неформальное общение между специалистами, а затем при ЦБ РФ был создан Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере — ФинCERT, ставший центром обмена информацией о кибератаках и о реагировании на них в кредитно-финансовой сфере.

И тем не менее, по данным исследовательской компании J`son & Partners, российский рынок ИБ в 2014 г. вырос на 13% и достиг 51 млрд. руб., что намного меньше приведенных выше оценок ущерба, причиненного кибератаками отечественным организациям и фирмам. В 2015-м расходы на ИБ, скорее всего, подросли, однако с учетом общей экономической ситуации они все равно не сравнятся с суммарным объемом нанесенного ущерба, даже если учесть высказываемые аналитиками соображения о том, что вложения в ИБ трудно выделить как независимые в отдельную статью расходов, поскольку чем дальше, тем четче реализуется на практике концепция встраивания функционала ИБ во все ИКТ-средства. В наиболее зрелых современных продуктах это реализуется начиная со стадии разработки, а в тех, которые имеют свою историю присутствия на рынке, — путём добавления такого функционала в готовое решение.

Анализируя развитие инвестиций в ИБ в нашей стране за последние полтора десятилетия, а также размышляя, с какими статьями корпоративных бюджетов чаще всего соотносятся затраты на ИБ, руководитель центра технологий безопасности компании IBS Дмитрий Романченко отмечает, что во многих российских компаниях процесс обособления ИБ-бюджета от бюджета на ИТ только начинается, и значительная часть (возможно, более 50%) фактических ИБ-бюджетов, скорее всего, пока еще растворена в ИТ-затратах.

В крупном и среднем бизнесе, по мнению г-на Романченко, действуют как минимум три значимых драйвера увеличения ИБ-бюджетов: недофинансирование сферы ИБ в прошлом, необходимость провести заново адекватную оценку ИБ-рисков с целью функционирования бизнеса сегодня и стремление соответствовать требованиям регуляторов.

В компаниях, зрелых в отношении ИБ (как правило, это представители крупного бизнеса), на взгляд г-на Романченко, меняется структура затрат на эту сферу: от базовых задач антивирусной защиты и защиты периметра они переходят к выстраиванию эшелонированной защиты ИТ-инфраструктуры и информационных систем, а также к построению комплексных систем управления доступом к информационным ресурсам. В целом же затраты на ИБ в крупном бизнесе если и не являются сегодня достаточными, то активно наращиваются.

В среднем бизнесе, по его мнению, ИБ-затраты жестко лимитируются и выделяются по остаточному принципу. Проекты ИБ здесь запускаются скорее как ответ на проверки и требования регуляторов, оценка реальных угроз в таких компаниях ограничена, что приводит к существенному недофинансированию ИБ.

Главный инженер ИБ-проектов ГК "Компьюлинк" Николай Зенин считает, что руководство российских компаний не стремится сокращать огромный разрыв между традиционно учитываемыми при планировании расходов на ИБ угрозами и теми рисками, с которыми сталкиваются ИБ-специалисты уже в ходе повседневной работы, поскольку учет актуальных угроз чреват кратным увеличением расходов на ИБ, в то время как финансовая отдача при этом не кажется очевидной. Зачем же тогда платить?

Тем не менее в некоторых сегментах в нашей стране в силу специфики перехода России к рыночной экономике концентрировались денежные средства и вырастали крупные корпорации, которые могли (а некоторые должны были из-за конкуренции) позволить себе внедрение передовых технологий и наем лучших специалистов. Это государственные монополии, банки, энергетические и добывающие компании, сети розничной торговли. Но и там, как указывает начальник отдела консалтинга НИП "Информзащита" Андрей Тимошенко, из-за их масштабов и территориальной распределенности ИБ-риски адекватно обрабатываются в основном в головных компаниях, а в филиалах и дочерних фирмах бюджетов на это может не хватать.

В целом в российских государственных организациях и органах власти защита информации, по мнению г-на Тимошенко, сводится к выполнению требований законодательства, которое развивается не так быстро, как технологии. Поэтому и бюджеты на ИБ выделяются с запозданием и в урезанном виде. Не хватает в госструктурах и квалифицированных кадров — большая часть специалистов, способных выполнить проект по созданию комплексной централизованной системы защиты информации для распределенной компании, приходится на долю крупных ИТ- и ИБ-интеграторов. В результате не все госорганизации успевают реагировать на актуальные угрозы ИБ.

Как бы то ни было, несмотря на кризисные явления в экономике страны, эксперты отмечают сегодня заметный рост ИБ-бюджетов в российских компаниях, что соответствует общемировым тенденциям. При этом, считает менеджер по развитию бизнеса "Лаборатории Касперского" Олег Глебов, предприятия все чаще сталкиваются с проблемой, когда даже самая передовая технология не дает необходимого уровня защищенности и требуется не столько наращивать инвестиции в ИБ, сколько перенаправлять их в нужные области.

Подходы к оценке необходимых затрат на ИБ

Совершенно очевидно, что проблема адекватной оценки необходимых затрат на ИБ стоит и перед российскими компаниями. При этом г-н Романченко выразил сомнение в том, что для достоверного количественного расчета таких затрат можно найти какие-либо инструменты. Он полагает, что такие средства могут существовать лишь для частных задач — защиты простых объектов при ограниченном наборе актуальных угроз ИБ. "На корпоративном же уровне, — заключает он, — задача обеспечения ИБ включает множество организационных и технических мероприятий, которые, в свою очередь, могут быть многовариантными в зависимости от вида бизнеса, состава актуальных угроз, ИТ-архитектуры и т. д., поэтому делать универсальный калькулятор или сложно, или бессмысленно". В то же время он указывает на то, что нормативные документы ФСТЭК, по сути, содержат пошаговую инструкцию по обеспечению ИБ и методику реализации системы защиты. ИБ-экспертам известны также примеры бюджетов реализованных ИБ-проектов, которые позволили обеспечить разные уровни ИБ в зависимости от многих факторов и выбора вендорских продуктов для объектов различного масштаба.

Выделяя систему управления информационной безопасностью в структуре обеспечения ИБ, начальник отдела продвижения и поддержки продаж компании RedSys Владимир Перминов как наиболее эффективный инструмент для расчетов затрат на ее построение признает международный стандарт ISO 27001. "Чтобы в процесс управления ИБ вовлечь руководство компании, ИБ-служба проводит оценку рисков, выявляя наиболее критичные процессы и активы предприятия, оценивая потенциальный ущерб от реализации ИБ-угроз, предлагая приемлемые для бизнеса варианты минимизации рисков. Такой подход позволяет ранжировать задачи ИБ по степени важности и адекватно оценивать необходимые для их решения ресурсы", — говорит он.

"Мы применяем различные способы расчета средств на ИБ, — говорит главный инженер проектов ИБ ГК "Компьюлинк" Николай Зенин. — Для одних руководителей убедительны расчеты сравнительных затрат, которые несет компания при передаче задач ИБ на аутсорсинг и при организации ИБ собственными подразделениями. Для других важны требования законодательства в области ИБ или обоснованность мер защиты на базе моделирования ИБ-угроз (исходными данными для этого может быть информация об анализе уязвимостей). Важно, чтобы основная мысль обоснования была простой и умещалась на одной странице".

Наши эксперты


ИВАН БОЙЦОВ, *ведущий менеджер по продукту, "Код безопасности"*


ОЛЕГ ГЛЕБОВ, *менеджер по развитию бизнеса, "Лаборатория Касперского"*


НИКОЛАЙ ЗЕНИН, *главный инженер проектов ИБ, ГК "Компьюлинк"*


МИХАИЛ КАДЕР, *заслуженный инженер, Cisco*


ВЛАДИМИР ПЕРМИНОВ, *начальник отдела продвижения и поддержки продаж, RedSys*


ВЛАДИМИР ПИСКУНОВ, *вице-президент по коммерческой деятельности, "Аквариус"*


ДМИТРИЙ РОМАНЧЕНКО, *руководитель центра технологий безопасности, IBS*


АНДРЕЙ ТИМОШЕНКО, *начальник отдела консалтинга, "Информзащита"*


ОЛЕГ ШАБУРОВ, *руководитель департамента ИБ, ГК Softline*


АНДРЕЙ ЯНКИН, *руководитель отдела консалтинга Центра ИБ, "Инфосистемы Джет"*

Обычно расходы на ИБ начинаются с решения применить тот или иной конкретный ИБ-продукт, а это зависит от потребностей, которые, как утверждает вице-президент по коммерческой деятельности компании "Аквариус" Владимир Пискунов, определяются моделями угроз, моделями нарушителя и моделями защиты. Он предлагает такой алгоритм действий. Для разработки упомянутых моделей следует провести аудит и вникнуть в бизнес- и технологические процессы предприятия. Это требует существенных затрат, которые прибавляются к затратам на ИБ. Для разработанных моделей нужно использовать готовые методики расчета и анализа ИБ-рисков — в разных отраслях есть уже устоявшиеся такие методики. На основании проведённого анализа формируются требования к ИБ-продукту, к услугам или инфраструктуре в целом, затем изучается рынок или объявляется тендер на выполнение этих требований, запрашиваются коммерческие предложения, определяется цена. Обязательно нужно учитывать амортизацию оборудования, стоимость обслуживания и перспективное развитие технологий, чтобы не купить откровенно неперспективный продукт.

Руководитель отдела консалтинга Центра ИБ компании "Инфосистемы Джет" Андрей Янкин рекомендует освоить методики расчета ROI и применять их к ИБ-проектам хотя бы частично (на основе оценки денег, сохраненных от нереализованных рисков), ввести систему метрик и KPI, которые позволят измерять эффективность ИБ в целом, а также отдельных проектов и сотрудников в частности. "Это даст возможность наладить контакт с бизнесом, а самим ИБ-специалистам сосредоточиться на главном. Такие расчеты делать непросто, — констатирует г-н Янкин, — как, впрочем, и для любых других направлений деятельности".

К инструментам расчета затрат на ИБ верхнего уровня следует отнести рекомендуемые г-ном Тимошенко системы относительно нового класса — "Управление предприятием, рисками и соблюдением нормативных требований" (Governance, Risk management and Compliance, GRC). В их основе лежит комплексный подход, позволяющий структурировать бизнес-процессы и автоматизировать их, интегрировать процессы управления ИБ-рисками в единую систему корпоративного риск-управления, внедрять контрольные процедуры и оценивать их эффективность, централизованно управлять планами по обработке рисков. Системы GRC позволяют агрегировать информацию о рисках, требованиях и контрольных процедурах и предоставляют возможность менеджменту принимать обоснованные и своевременные управленческие решения.

Самоокупаемость корпоративной ИБ — миф или реальность?

Как утверждает г-н Перминов, не более десятка российских компаний может похвастаться самоокупаемостью своих ИБ-служб: работая по сервисной модели, они предоставляют ИБ-услуги внутри компании на основе договорных ставок и SLA.

Судя по малому количеству таких компаний, ситуацию с самоокупаемостью корпоративной ИБ в нашей стране типичной не назовешь. Но и негативной, если судить по комментариям экспертов, она тоже не выглядит. И хотя мнения наших экспертов распределились по всей шкале от "да" до "нет", концентрируются они все же возле "да".

Андрей Тимошенко, относящийся к экспертам-скептикам, полагает, что самоокупаемость ИБ маловероятна, поскольку в структуре компаний это затратное подразделение и говорить здесь можно только о минимизации рисков и потерь. Однако и он считает, что в телеком-сегменте зарабатывать на ИБ можно. Зарубежная практика уже имеет реализованные кейсы по монетизации ИБ в телекоме, и российские компании, перенимая лучшие иностранные практики, тоже начинают формировать соответствующие пакеты ИБ-услуг.

"ИБ — поддерживающий сервис и не может быть самоокупаемым подобно тому, как не могут быть самоокупаемыми прокуратура, суды, законодательные органы, которые тем не менее способствуют организации жизни общества", — заявляет г-н Романченко. Вместе со своим коллегой Тимошенко он говорит только об оптимизации затрат на ИБ в корпоративном секторе за счет оптимального разделения ИБ-функций между собственной службой и профессиональными ИБ-компаниями, привлекаемыми на контрактной основе, или частичной замены инвестиций в собственную ИБ-инфраструктуру на эквивалентный сервис. Но к сожалению, предложений ИБ-сервисов должного уровня, которые гарантировали бы требуемый уровень SLA и возврат потерянных средств в случае ИБ-инцидентов, он в России не видит.

Публичность данных об ущербах от ИБ-инцидентов поможет строить реалистичные модели угроз, даст возможность коллективными усилиями сообщества специалистов разработать методики оценки таких ущербов, а сами эти методики станут мощным инструментом в руках бизнес-руководителей и руководства корпоративных ИБ-служб для адекватного определения места информационной безопасности в каждой конкретной структуре, в планировании и обосновании бюджетов на ИБ.

Оппонируя г-ну Романченко, г-н Пискунов приводит другую аналогию — с окупаемостью страховки на автомобиль. Решение, страховать или не страховать машину, принимает владелец, оценивая возможные риски и добиваясь в результате самоокупаемости страховки.

Не только телеком-операторы успешно монетизируют ИБ, считает заслуженный инженер компании Cisco Михаил Кадер. Все динамично развивающиеся компании смотрят на ИБ как на средство снижения расходов, добавления новых сервисов, повышения эффективности труда. В этом случае экономический эффект рассчитать можно, и такие компании говорят не о "самоокупаемости", а о получении прибыли за счет внедрения ИБ-решений.

Самоокупаемость ИБ становится реальностью, полагает г-н Зенин, если она интегрирована в основную деятельность компании. Для этого необходимо, чтобы обоснование ИБ-бюджетов содержало убедительные данные, в основе которых лежит, как правило, модель угроз по отношению к ИБ, а в концепции защиты компании должны быть прописаны аргументированные меры предотвращения актуальных угроз. Для того чтобы угроза была признана актуальной, рассматриваются характеристики вероятности ее реализации в инфраструктуре компании и уровень ее опасности — всё это индивидуально для каждой компании.

Реальностью, причем не отдаленной, считает самоокупаемость ИБ г-н Перминов. Основным препятствием для этого, по его мнению, является недостаточная квалификация ИБ-служб и отсутствие взаимопонимания с руководством. "Через два-три года сервисная модель отношений между бизнесом и департаментами ИТ и ИБ, которая доказала свою состоятельность на Западе, будет массово применяться и у нас", — полагает он.

Как повысить эффективность расходов на ИБ?

Чтобы бизнес начал заниматься эффективностью ИБ, ему необходим серьезный мотив. Сейчас, по мнению г-на Зенина, этому препятствуют три фактора:

— ИБ-риски не находятся в числе главных бизнес-рисков российских компаний;

— ИБ рассматривается руководством только как затратная статья;

— бюджеты ИБ не настолько велики, чтобы руководство заостряло на них внимание.

Для изменения ситуации необходимо ИБ представить бизнесу как самоокупающееся направление деятельности.

В поисках ответа на вопрос о повышении эффективности ИБ г-н Романченко рекомендует руководствоваться двумя критериями: во-первых, ИБ-инвестиции должны быть адекватны значимости актуальных для бизнеса угроз, а во-вторых, нужно просчитать фактически предотвращенный ущерб из-за случившихся инцидентов.

Наши эксперты выделили ряд направлений, в которых следует действовать для повышения эффективности ИБ.

Регулирование ИБ. Дополняя сказанное выше об отраслевом регулировании ИБ Центробанком РФ, г-н Тимошенко упоминает разрабатываемые этой организацией отраслевые документы, направленные на обеспечение ИБ в банковской сфере России. Такие документы создают системную основу для оценки и повышения эффективности расходов на ИБ в организациях банковской системы (несмотря даже на то, что, как показывают аудиторские проверки, ими пользуются далеко не все банки).

Наши эксперты высоко оценивают деятельность ФСТЭК РФ. Эта федеральная служба сегодня наибольшее внимание обращает на оперативное информирование профессионалов и устранение уязвимостей. "Новых нормативных актов от ФСТЭК специалистам ждать приходится несколько дольше, чем хотелось бы, зато документы получаются высокого качества и доступными для практического применения при определении ИБ-угроз и планировании мер защиты", — отмечает г-н Зенин, особо выделяя банк данных угроз безопасности ФСТЭК.

Наши эксперты полагают, что повышение штрафов за нарушение закона "О персональных данных" может существенно улучшить ситуацию с защитой ПДн, поскольку неадекватная ответственность в этой области по сути порождает "защиту от регулятора" и вовсе не способствует эффективной защите персональных данных.

"В то же время возможности повышать эффективность ИБ через регулирование, — отмечает ведущий менеджер по продукту компании "Код безопасности" Иван Бойцов, — ограничены тем, что при составлении своих требований регуляторы диктуют меры и способы обеспечения защиты, описывают возможные угрозы, не учитывая рыночной конкретики, не руководствуясь стоимостью ИБ-средств и экономической эффективностью их эксплуатации". Как раз сейчас страна пытается как-то приспособиться к одной из таких законотворческих новаций — так называемому закону Яровой.

Обучение и информированность. "Нет ничего легче, — утверждает руководитель департамента ИБ группы компаний Softline Олег Шабуров, — чем воспользоваться невежеством человека, его нежеланием выполнять разработанные правила или стремлением узнать что-то изначально закрытое от него. Поэтому простейшим способом повышения эффективности ИБ является работа с самым слабым в сфере ИБ звеном (по возможности исключая его из процесса обеспечения информбезопасности, т. е. полагаясь на технику)".

Бывает, что пользователям достаточно объяснить, какие бывают риски, к чему они могут привести и как правильно реагировать на те или иные ситуации. Заниматься этим нужно регулярно, что, кстати, соответствует мировому тренду: расходы компаний на обучение сотрудников и уровень их осведомленности в области ИБ в последние годы существенно растут.

Нелестно оценивают наши эксперты подготовку ИБ-специалистов в учебных заведениях. По наблюдениям г-на Тимошенко, почти каждому молодому специалисту требуется как минимум год дополнительной практической подготовки, прежде чем он начнёт выполнять свои обязанности самостоятельно. Эксперт считает, что вузы должны чаще привлекать к обучению опытных ИБ-практиков, а студентов отправлять на дипломные работы в высокотехнологичные компании, которые способны предложить им действительно интересные и полезные темы для исследований.

Требования к технологиям. Напомнив о том, что среднее время обнаружения взлома сейчас составляет около двухсот дней, г-н Кадер заявляет, что улучшать ситуацию неизбежно следует через развитие технической области, иначе отставание от злоумышленников приведет к дальнейшему росту "незаметных" вторжений.

Наши эксперты надеются, что разработчики ИБ-средств и ИКТ-оборудования будут развивать набирающую обороты практику сквозной ИБ, т. е. реализацию ИБ в условиях цифровизации жизни как одного из главных функционалов пользовательских продуктов.

Важнейшее значение для повышения эффективности ИБ приобретает возможность интегрировать между собой отдельные ИБ-средства и решения, с тем чтобы специалисты могли строить из них единые комплексы ИБ с централизованными управлением и обработкой данных. Это означает, что ИБ-вендоры "обречены" на совместные действия для создания таких комплексов.

На изменения в стратегии организации ИБ указывает г-н Глебов, отмечающий, что сегодня предприятия переключают своё внимание с превентивной защиты на построение процессов реагирования на ИБ-инциденты, а это требует дополнительных технологий и изменений, связанных с централизацией управления ИБ, обработкой больших данных, интеллектуализацией и автоматизацией в области ИБ.

Потребность в централизации управления ИБ, в консолидации ИБ-данных, в централизованной их обработке должна изменить положение службы ИБ в структуре компаний. По мнению г-на Пискунова, корпоративные службы ИБ и ИТ должны наконец-то стать единым целым, а глубокая интеграция информационной безопасности в ИТ позволит строить современную комплексную защиту.

Возможность унификации и консолидации ИБ-решений, где каждый элемент становится частью единой интегрированной экосистемы, не только выполняя свои задачи, но и качественно влияя на общую эффективность ИБ, является, по мнению г-на Глебова, одним из весомых показателей экономической обоснованности их внедрения. Такой подход позволяет как повысить ИБ, так и снизить общую стоимость владения решениями корпоративной информбезопасности.

Государственное регулирование в области безопасности производственных и технологических процессов

ВИТАЛИЙ СЕРГИЕНКО

Как правило, государственное регулирование тех или иных областей касается обеспечения безопасности граждан (собственно, такова основная функция государства). По этой причине все законодательные акты, обязательные для исполнения, направлены на противодействие угрозам аварий, которые могут повлечь за собой человеческие жертвы или нарушить обороноспособность страны, т. е. угрожают жизнедеятельности людей и сохранению государственности. Государство не вмешивается в такие тонкие материи, как повышение эффективности труда, улучшение качества продукции, рост прибыльности того или иного бизнеса. Имеющиеся нормативные акты в этих областях, как правило, носят рекомендательный характер или отдаются на откуп в министерства (отраслевые стандарты, нормы и правила) и саморегулирующиеся организации (нормативные документы СРО). Нормы обязательности исполнения таких требований сохраняются только в пределах определенной отрасли или СРО.

С учётом вышеприведенных оговорок безопасность технологических процессов в нормативных актах государственного или отраслевого значения рассматривается исключительно с точки зрения безопасности промышленной, т. е. охраны труда и соблюдения норм техники безопасности при проведении работ и эксплуатации технических средств.

Нормативная база защиты технологических процессов

В документах Роскомнадзора используются термины “требования к безопасности технологических процессов” (приказ Ростехнадзора от 22.11.2013 № 563 “Об утверждении федеральных норм и правил в области промышленной безопасности «Правила безопасности грузовых подвесных канатных дорог»”); “требования безопасности к технологическим процессам” (ПОТ РО-13153-ЦШ-877—02. Отраслевые правила по охране труда при техническом обслуживании и ремонте устройств сигнализации, централизации и блокировки на федеральном железнодорожном транспорте, утверждённые МПС РФ 19.02.2002, или постановление Госгортехнадзора РФ от 27.05.2003 № 41 “Об утверждении Правил промышленной безопасности резиновых производств”); “безопасность ведения технологических процессов” (приказ Ростехнадзора от 11.03.2013 № 96 “Об утверждении федеральных норм и правил в области промышленной безопасности «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств») и т. п.; причём используются они исключительно в области охраны труда и соблюдения техники безопасности при проведении работ. Аналогичную ситуацию можно наблюдать относительно термина “соблюдение (или контроль) технологической дисциплины”.

Какие-либо требования со стороны государства, как правило, сопровождаются указанием на должностное лицо, с которого в конечном итоге будут спрашивать за их неисполнение. Помимо очевидного “руководителя организации”, который является публичным физическим лицом, представляющим предприятие, и соответственно несет всю полноту ответственности за его деятельность или бездействие в целом, в большинстве регулируемых областей указывается и должностное лицо, ответственное за организацию выполнения устанавливаемых требований. Например, за нарушения в области бухгалтерского и налогового учета, из-за которых бюджет недополучил своей копеечки от деятельности организации, отвечать перед государством будет не только руководитель, но и главный бухгалтер. В рамках рассматриваемого вопроса нормативными актами определено, что понятия “безопасность технологических процессов” и “контроль технологической дисциплины” лежат в сфере ответственности главного инженера предприятия. Это подтверждается положениями “Квалификационного справочника должностей руководителей, специалистов и других служащих” (утверждён постановлением Минтруда России от 21.08.1998 № 37), в том числе в разделах квалификационных характеристик должностей в разного рода на опасных производствах (приказы Минздравсоцразвития России от 10.12.2009 № 977, от 10.04.2012 № 328н, от 23.04.2008 № 188 и др.).

Непосредственное исполнение мероприятий по контролю технологической дисциплины и техническому контролю качества выпускаемой продукции возлагается на работников технологических служб. Постановлением Минтруда РФ от 21.04.1993 № 86 “Об утверждении укрупненных норм времени на разработку технологической документации” определено, что на планирование и выполнение контрольных процедур для простейшего технологического процесса, в котором задействовано всего два или даже одно рабочее место, уже требуется как минимум два нормо-часа, а только на разработку методов технического контроля и испытания качества при массовом производстве (т. е. уже при изготовлении свыше тысячи единиц продукции) понадобится более недели рабочего времени. В современных условиях, когда конкурентная борьба диктует необходимость внесения изменений в выпускаемую продукцию за минимальные сроки, такие цифры совершенно неприемлемы.

Необходима автоматизация

Руководитель предприятия оказывается в непростом положении, когда из-за снижения качества продукции и простоя оборудования вследствие постоянно возникающих аварийных ситуаций либо из-за чрезмерно больших сроков перестройки технологических процессов и внедрения методов их контроля компания может утратить конкурентные преимущества.

Решить эти проблемы помогает автоматизация управления производственными и технологическими процессами, под которой в данном случае следует понимать внедрение широкого набора инструментов — от систем управления предприятием (ERP) и производством (MES, АСУП) до систем автоматизации отдельных производств (АСУ ТП) или даже отдельных операций (станок с ЧПУ).

К сожалению, в большинстве случаев возможности, предоставляемые АСУ ТП, используются в первую очередь для снижения сроков внесения изменений в производимую продукцию. Мероприятия по переключению процедур контроля её качества и соблюдению технологии на всех этапах производства катастрофически запаздывают. Довольно часто буквально через один-два месяца после поступления в продажу первых партий тех или иных продуктов выпускаются их новые версии, в которых изначально заявленные характеристики не просто декларируются, но реально обеспечиваются. Между тем первые версии оказывают весьма негативное влияние на потребительское доверие к торговой марке.

Под контролем государства

Государство тоже не остается в стороне от оценки новых рисков, связанных с внедрением средств автоматизации управления производством, особенно на объектах, имеющих критическую важность для сохранения основной государственной функции — обеспечения безопасности граждан. В “Основных направлениях государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации” (утв. Президентом РФ 03.02.2012, № 803) определен термин “безопасность автоматизированной системы управления критически важным объектом (КВО)” как такое “состояние автоматизированной системы управления КВО, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения ею целевых функций (штатный режим функционирования) при проведении в отношении ее компьютерных атак”. Разумеется, государство в первую очередь озабочено защитой от целенаправленного вредоносного воздействия на КВО, справедливо полагая, что задачи обеспечения выпуска заданного количества продукции заданного качества и в заданный срок будут решаться руководителями предприятий без напоминания с его стороны.

В тех случаях, когда государство выступает в роли потребителя какой-либо продукции и вопросы ее качества и соблюдения сроков производства начинают влиять на основную государственную функцию, в дело вступают нормы “добровольной” сертификации в области управления качеством. Добровольность этой процедуры заключается в том, что никто не заставляет ту или иную организацию предлагать свою продукцию государственным заказчикам, но если такое желание возникло, то извольте внедрить у себя процедуры системы менеджмента качества (СМК) и подтвердить их должное исполнение результатами соответствующих сертификационных испытаний. Сертификат СМК может входить в состав технической документации на изделие при выполнении требования обязательности подтверждения его соответствия в форме декларирования (федеральный закон от 27.12.2002 № 184-ФЗ “О техническом регулировании”). Федеральный закон от 05.04.2013 № 44-ФЗ “О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд” не ограничивает право государственных заказчиков указывать требования к наличию у исполнителя такого сертификата в качестве критерия оценки “Качественные, функциональные и экологические характеристики объекта закупок”, на что среди прочего было указано в письме Минэкономразвития России от 10.03.2016 № Д28и-653.

Стандарты СМК (ГОСТ Р ИСО 9000—2015 “Системы менеджмента качества. Основные положения и словарь” и т. п.) пришли на смену целому ряду государственных стандартов и руководящих документов, устанавливающих требования к соблюдению технологической дисциплины. Вот несколько цитат из нормативной, справочной и учебной литературы недавнего советского прошлого: “Соблюдение технологической дисциплины является законом производства и основой обеспечения качества изготовляемой продукции” (СТП 019.041—72 “Комплексная система управления качеством продукции. Контроль соблюдения технологической дисциплины”); “Соблюдение твердой технологической дисциплины обеспечивает нормальный ход производства, высокое качество продукции, высокую производительность труда и низкую стоимость продукции” (*Соболев Н. П.* Инструментально-лекальные работы. Трудрезервиздат, 1959); “Соблюдение технологической дисциплины является основным условием, обеспечивающим нормальный ход производства и получение высококачественной продукции” (*Барбашов Ф. А.* Фрезерное дело. Высшая школа, 1973); “Соблюдение технологической дисциплины должно сочетаться с предоставлением возможности для нововведений со стороны технологов, мастеров и новаторов производства. С этой целью разрешается после соответствующих испытаний вносить изменения в существующую технологию” (*Федосеев Д. Н.* Проектирование технологических процессов сборки приборов, Изд. 2-е. Машгиз [Ленингр. отд-ние], 1963).

Таким образом, деятельность по обеспечению основных свойств производственного и технологического процессов, то есть по соблюдению сроков, качества и объема производимой продукции, осуществлялась и раньше, но с увеличением требований к гибкости производственных процессов и неизбежной автоматизацией управления производственными и технологическими процессами эта задача существенно усложнилась. Необходимость соблюдения технологической дисциплины на производстве никуда не делась, выполнение этого требования по-прежнему влияет на качество и своевременность выпуска продукции, но перечень процессов, входящих в систему менеджмента качества, значительно расширился.

Следует отметить, что с расширением списка задач, которые должны решаться в рамках обеспечения качества и своевременности выпуска продукции в условиях все большего проникновения в производственные процессы средств автоматизации управления, уровень качества автоматизации деятельности технологической службы и ОТК не повысился. Безусловно, технологическая точность контрольно-измерительного оборудования, находящегося на вооружении работников этих служб, стала гораздо выше, но автоматизация диагностики и принятия решений осталась практически на прежнем уровне. Текущий уровень автоматизации деятельности служб, отвечающих за сохранение смысла функционирования всего производства в целом, ограничивается реагированием на негативное воздействие уже после того, как оно привело к нарушению контролируемых параметров продукции, и качественного перехода к применению превентивных мер, нейтрализующих это воздействие до списания некой части продукции в брак, пока не произошло. Тот факт, что новые средства контроля качества позволяют инспектору ОТК выявить даже самое ничтожное отклонение от нормы, никак не помогает увеличить прибыль от выпуска большего объема высококачественной продукции и снизить количество впустую потраченных ресурсов на изготовление забракованных изделий. Решение этой проблемы целиком и полностью возложено на плечи руководителей предприятий, так как регулирующая роль государства ограничивается требованиями к технологической точности контрольно-измерительного оборудования. Например, приказ Ростехнадзора от 29.03.2016 № 125 “Об утверждении федеральных норм и правил в области промышленной безопасности

ПРОДОЛЖЕНИЕ НА С. 15 ▸

ПОТРАТИВ ВСЕГО 5 МИНУТ НА ЗАПОЛНЕНИЕ АНКЕТЫ, ВЫ БУДЕТЕ БЕСПЛАТНО ПОЛУЧАТЬ PC Week/RE 50 НЕДЕЛЬ

PC WEEK

КОРПОРАТИВНАЯ ПОДПИСКА

Уважаемые читатели!

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

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

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

Название организации:

Почтовый адрес организации:

Индекс: Область:

Город:

Улица: Дом:

Фамилия, имя, отчество:

Подразделение / отдел:

Должность:

Телефон: Факс:

E-mail: WWW:

(Заполните анкету печатными буквами!)

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

2. Если основной профиль Вашего предприятия – информационные технологии, то уточните, пожалуйста, сегмент, в котором предприятие работает:
1. Системная интеграция ❑
2. Дистрибуция ❑
3. Телекоммуникации ❑
4. Производство средств ВТ ❑
5. Продажа компьютеров ❑
6. Ремонт компьютерного оборудования ❑
7. Разработка и продажа ПО ❑
8. Консалтинг ❑
9. Иное (что именно)

3. Форма собственности Вашей организации (отметьте только один пункт)
1. Госпредприятие ❑
2. ОАО (открытое акционерное общество) ❑
3. ЗАО (закрытое акционерное общество) ❑
4. Зарубежная фирма ❑
5. СП (совместное предприятие) ❑
6. ТОО (товарищество с ограниченной ответственностью) или ООО (Общество с ограниченной ответственностью) ❑
7. ИЧП (индивидуальное частное предприятие) ❑
8. Иное (что именно)

4. К какой категории относится подразделение, в котором Вы работаете? (отметьте только один пункт)
1. Дирекция ❑
2. Информационно-аналитический отдел ❑
3. Техническая поддержка ❑
4. Служба АСУ/ИТ ❑
5. ВЦ ❑
6. Инженерно-конструкторский отдел (САПР) ❑
7. Отдел рекламы и маркетинга ❑
8. Бухгалтерия/Финансы ❑
9. Производственное подразделение ❑
10. Научно-исследовательское подразделение ❑
11. Учебное подразделение ❑
12. Отдел продаж ❑
13. Отдел закупок/логистики ❑
14. Иное (что именно)

5. Ваш должностной статус (отметьте только один пункт)
1. Директор / президент / владелец ❑
2. Зам. директора / вице-президент ❑
3. Руководитель подразделения ❑
4. Сотрудник / менеджер ❑
5. Консультант ❑
6. Иное (что именно)

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

7. Численность сотрудников в Вашей организации
1. Менее 10 человек ❑
2. 10–100 человек ❑
3. 101–500 человек ❑
4. 501–1000 человек ❑
5. 1001–5000 человек ❑
6. Более 5000 человек ❑

8. Численность компьютерного парка Вашей организации
1. 10–20 компьютеров ❑
2. 21–50 компьютеров ❑
3. 51–100 компьютеров ❑
4. 101–500 компьютеров ❑
5. 501–1000 компьютеров ❑
6. 1001–3000 компьютеров ❑
7. 3001–5000 компьютеров ❑
8. Более 5000 компьютеров ❑

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

10. Коммуникационные возможности компьютеров Вашей организации
1. Имеют выход в Интернет по выделенной линии ❑
2. Объединены в intranet ❑
3. Объединены в extranet ❑
4. Подключены к ЛВС ❑
5. Не объединены в сеть ❑
6. Dial Up доступ в Интернет ❑

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

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

13. Сколько серверов в сети Вашей организации ?

14. Если в Вашей организации используются мэйнфреймы, то какие именно?
1. EC ЭВМ ❑
2. IBM ❑
3. Unisys ❑
4. VAX ❑
5. Иное (что именно)
6. Не используются ❑

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

	Настольные ПК	Портативные ПК	Серверы
"Аквариус"	❑	❑	❑
ВИСТ	❑	❑	❑
"Формоза"	❑	❑	❑
Acer	❑	❑	❑
Apple	❑	❑	❑
CLR	❑	❑	❑
Compaq	❑	❑	❑
Dell	❑	❑	❑
Fujitsu Siemens	❑	❑	❑
Gateway	❑	❑	❑
Hewlett-Packard	❑	❑	❑
IBM	❑	❑	❑
Kraftway	❑	❑	❑
R.&K.	❑	❑	❑
R-Style	❑	❑	❑
Rover Computers	❑	❑	❑
Sun	❑	❑	❑
Siemens Nixdorf	❑	❑	❑
Toshiba	❑	❑	❑
Иное (что именно)			

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

17. Если в Вашей организации установлено ПО масштаба предприятия, то каких фирм-разработчиков?
1. "1С" ❑
2. "АйТи" ❑
3. "Галактика" ❑
4. "Парус" ❑
5. BAAN ❑
6. Navision ❑
7. Oracle ❑
8. SAP ❑
9. Epicor Scala ❑
10. ПО собственной разработки ❑
11. Иное (что именно)
12. Не установлено никакое ❑

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

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

20. Если Вы используете СУБД в своей деятельности, то какие именно?
1. Adabas ❑
2. Cache ❑
3. DB2 ❑
4. dBase ❑
5. FoxPro ❑
6. Informix ❑
7. Ingress ❑
8. MS Access ❑
9. MS SQL Server ❑
10. Oracle ❑
11. Progress ❑
12. Sybase ❑
13. Иное (что именно)
14. Не используем ❑

21. Как Вы оцениваете свое влияние на решение о покупке средств информационных технологий для своей организации? (отметьте только один пункт)
1. Принимаю решение о покупке (подписываю документ) ❑
2. Составляю спецификацию (выбираю средства) и рекомендую приобрести ❑
3. Не участвую в этом процессе ❑
4. Иное (что именно)

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

Системы
1. Мэйнфреймы ❑
2. Миникомпьютеры ❑
3. Серверы ❑
4. Рабочие станции ❑
5. ПК ❑
6. Тонкие клиенты ❑
7. Ноутбуки ❑
8. Карманные ПК ❑

Сети
9. Концентраторы ❑
10. Коммутаторы ❑
11. Мосты ❑
12. Шлюзы ❑
13. Маршрутизаторы ❑
14. Сетевые адаптеры ❑
15. Беспроводные сети ❑
16. Глобальные сети ❑
17. Локальные сети ❑
18. Телекоммуникации ❑

Периферийное оборудование
19. Лазерные принтеры ❑
20. Струйные принтеры ❑
21. Мониторы ❑
22. Сканеры ❑
23. Модемы ❑
24. ИБП (UPS) ❑

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

Программное обеспечение
30. Электронная почта ❑
31. Групповое ПО ❑
32. СУБД ❑
33. Сетевое ПО ❑
34. Хранилища данных ❑
35. Электронная коммерция ❑
36. ПО для Web-дизайна ❑
37. ПО для Интернета ❑
38. Java ❑
39. Операционные системы ❑
40. Мультимедийные приложения ❑
41. Средства разработки программ ❑
42. CASE-системы ❑
43. САПР (CAD/CAM) ❑
44. Системы управления проектами ❑
45. ПО для архивирования ❑

Внешние сервисы
46. ❑

Ничего из вышеперечисленного
47. ❑

23. Каков наивысший уровень, для которого Вы оказываете влияние на покупку компьютерных изделий или услуг (служб)?
1. Более чем для одной компании ❑
2. Для всего предприятия ❑
3. Для подразделения, располагающегося в нескольких местах ❑
4. Для нескольких подразделений в одном здании ❑
5. Для одного подразделения ❑
6. Для рабочей группы ❑
7. Только для себя ❑
8. Не влияю ❑
9. Иное (что именно)

24. Через каких провайдеров в настоящее время Ваша фирма получает доступ в интернет и другие интернет-услуги?
1. "Демос" ❑
2. МТУ-Интел ❑
3. "Релком" ❑
4. Combellga ❑
5. Comstar ❑
6. Golden Telecom ❑
7. Equant ❑
8. ORC ❑
9. Telmos ❑
10. Zebra Telecom ❑
11. Через других (каких именно)

Дата заполнения

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

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

ПОДПИШИСЬ

СК ПРЕСС

PC WEEK

Подписаться на бумажную версию газеты PC Week можно в агентстве
ООО "Агентство "Урал-Пресс"" 8 (495) 789-86-39

НА 2016 ГОД

ДОКУМЕНТООБОРОТ & ECM

Тематический раздел портала PC Week Live

Блог
Форум
Статьи
Новости
События
White papers

pcweek.ru/ecm

Huawei...

ПРОДОЛЖЕНИЕ СО С. 1

ность. Согласно аналитическому агентству IHS, общий объем мировых инвестиций в решения для обеспечения общественной безопасности превысил в прошлом году 5,5 млрд. долл., а к 2019 г. он должен вырасти до 8 млрд. долл. Утверждается, что с помощью решений Huawei сегодня обеспечивается защита 400 млн. жителей из 100 городов в 30 странах, включая Кению, Саудовскую Аравию, Индонезию и Китай. На конференции была представлена новая интегрированная коммуникационная платформа (ИКП), дополнившая линейку решений Safe City. Она способна регистрировать оповещения, поступающие из разных каналов, включая социальные сети и Интернет вещей, а также позволяет быстро получать доступ к большим объемам видео. Утверждается, что ИКП решает проблему использования различными ведомствами разнородных технологий и сетей. Голосовые и видеосообщения, а также другие данные могут быть переданы любой группе пользователей или устройств через SDN-сети.

Еще один пример сотрудничества в экосистеме — облачное решение New Financial Cloud Solution for Mission Critical, разработанное Huawei совместно с Infosys Finacle для решения сложных задач финансовой и банковской отрасли. В нем используется облачная платформа Huawei FusionCloud и первый в мире 32-процессорный x86-сервер для обработки критически важных задач Huawei KunLun, на которых развернута банковская система Infosys Finacle, поддерживающая функции онлайнового и мобильного банкинга, управления взаимоотношениями с клиентами (CRM) и частными капиталами. В ходе конференции соглашения о сотрудничестве с Huawei в этой сфере подписали два ведущих российских разработчика банковских систем — "Диасофт" и ЦФТ. Они надеются, что наряду с реализацией программно-аппаратных инновационных пакетных решений для финансового сектора данное соглашение позволит им продвигать совместно с Huawei системы на международных рынках.

По словам президента подразделения Huawei IT Product Line Чжэн Елая, особые надежды в плане формирования экосистемы компания возлагает на своих давних и крупнейших клиентов в телекоммуникационной отрасли, таких как Deutsche Telekom, Telefonica и China Telekom. Они широко применяют облачные технологии для обеспечения своей основной деятельности, а также все чаще сами становятся провайдерами облачных услуг для своих клиентов.

Еще одним важным элементом облачной стратегии Huawei можно считать четкое позиционирование относительно направлений, в которых компания работать не собирается. Как заявил еще один CEO Huawei Эрик Сюй, компания не намерена становиться провайдером публичных облачных услуг за пределами Китая. Это означает, что она не будет конкурировать на данном поле с такими вендорами, как Microsoft, Oracle и SAP, а потому вполне может рассчитывать на взаимовыгодное сотрудничество с ними в рамках экосистемы. Эрик Сюй отметил также, что Huawei не планирует сама разрабатывать средства искусственного интеллекта и машинного обучения, но ведет работы по созданию специализированного процессора для подобных задач, который превосходит по своим характеристикам широко применяемые сегодня многоядерные графические процессоры Nvidia Tesla.

Компания не хочет также заниматься выпуском собственных датчиков и устройств Интернета вещей (IoT), но готова предоставить производителям подобных устройств готовые чипсеты и легкую операционную систему с открытым кодом LiteOS, поддерживающие узкополосный беспроводной стандарт NB-IoT. Цена такого модуля не превышает 5 долл., а построенные на его основе IoT-устройства благодаря низкому энергопотреблению смогут работать 10 лет без замены батарейки. Совместно с телеком-операторами Vodafone, Deutsche Telekom, China Unicom и Etisalat уже выполнен ряд пилотных проектов по созданию интеллектуальных систем измерения расхода воды, контроля освещения и управления парковкой автомобилей.

Как и любая конференция такого рода, Huawei Connect не могла обойтись без анонсов новых решений и версий продуктов. Помочь заказчикам в переносе их приложений в облака призван 31 новый сервис платформы FusionCloud. Сервисы эти охватывают ресурсы процессоров, СХД, сетей, БД, а также систем защиты, тестирования, управления и т. д. Выпущена очередная версия платформы СХД FusionStorage 6.0, обеспечивающая распределенное хранение с блочным, файловым и объектным доступом к данным. Новая PaaS-платформа FusionStage предназначена для разработки и развертывания облачных приложений, их эксплуатации и контроля. Решение Agile Network 2016 призвано обеспечить построение простой, открытой и безопасной программно-конфигурируемой сети, включающей беспроводные сегменты для мобильных и IoT устройств.

У стратегической ориентации Huawei на облака есть еще одно, экономическое, объяснение: такая стратегия может обеспечить дополнительные рыночные возможности для подразделения Enterprise Business Group, работающего на корпоративном ИТ-рынке. Это направление до сих пор обеспечивает львиную долю выручки Huawei: из зафиксированного в 2015 г. оборота 60,8 млрд. долл. на него приходится более половины (35,8 млрд. долл.). Немалый вклад (19,9 млрд. долл.) вносит и подразделение Consumer BG, отвечающее за выпуск мобильных устройств. Доход Enterprise BG, хоть и вырос за год на 44%, находится пока что на уровне 4,3 млрд. долл. Вполне вероятно, что выход на рынок облачных решений, в которых используется весь спектр продуктов Huawei, простимулирует более активный спрос и на корпоративные ИТ-решения компании, в частности, со стороны телекоммуникационных компаний.

В нашей стране нередко упоминают о китайском пути как примере успешного экономического развития. И наилучшей его иллюстрацией служат достижения таких компаний, как Huawei. В :этой связи хотелось бы обратить внимание на то, что Huawei всегда была и остается частной компанией, а в структуре ее доходов зарубежные продажи составляют более половины (уникальный показатель для китайских ИТ-вендоров). Из 170 тыс. сотрудников 76 тыс. работают в подразделениях исследований и разработок во множестве стран, включая и Россию. На R&D тратится 15% годовой выручки компании (9,2 млрд. долл. в 2015 г.).

Государственное...

ПРОДОЛЖЕНИЕ СО С. 12

«Правила безопасности нефтегазоперерабатывающих производств»" гласит, что "… метрологические характеристики систем, приборов, устройств автоматизации и телемеханизации не должны быть ниже значений, указанных в проектной и технической документации". Требования государственных регуляторов предполагают также, что в системе управления наряду с функциями управления производством должны быть и функции защиты самой АСУ ТП. Например, в приказе Ростехнадзора от 26.12.2014 № 615 "Об утверждении федеральных норм и правил в области промышленной безопасности «Требования к безопасному ведению технологических процессов нитрования»" сказано, что "…АСУ ТП должны обеспечивать стабильность технологического процесса с помощью автоматизированного контроля технологических параметров, визуализации процесса и выдачи управляющих воздействий на исполнительные механизмы как в автоматическом режиме, так и в результате действий оператора", а также "должна быть обеспечена надежная защита АСУ ТП от несанкционированного доступа и от разрушения или остановки работы программного обеспечения в результате некорректных действий оператора". Приказ ФСТЭК России от 14.03.2014 № 31 "Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды", устанавливает требования к защите АСУ ТП, где уровень такой защиты опять же определяется в соответствии с масштабом чрезвычайной ситуации, которая может возникнуть в случае, если нарушен штатный режим работы системы управления, и сопряжён с затратами на устранение ее последствий, но не со стоимостью ресурсов предприятия, списанных на производство брака.

***

Подводя итог, можно сказать, что государственное регулирование в области безопасности производственных и технологических процессов, включая требования к функциям и защите систем автоматизации управления ими, ограничено вопросами обеспечения безопасности граждан — как непосредственно персонала потенциально опасных производств, так и населения, проживающего в зоне чрезвычайной ситуации, которая может возникнуть в результате аварии на производстве. Вопросы качества и сроков производства продукции могут регулироваться государственными заказчиками через требования к наличию на производстве сертифицированной системы управления качеством. Определение путей и способов решения проблем экономии временных и материальных ресурсов, которые тратятся на производство продукции с нарушением тех или иных параметров (производственного брака), снижения времени перестройки технологических процессов для выпуска новых версий или типов продуктов при сохранении заданного уровня их качества, равно как и решение прочих подобных вопросов, возникающих в условиях конкурентной борьбы (или режима жесткой экономии при выполнении государственных заказов), возложено на самих руководителей предприятий. Те компании, руководство которых сегодня начнет обращать внимание на эти проблемы, завтра получат неоспоримое конкурентное преимущество.

Интеграторам в области защиты информации, которые с выходом в свет 31-го приказа ФСТЭК России с огромным энтузиазмом бросились предлагать свои услуги по защите АСУ ТП, следует понять, что в отличие от сферы защиты информации ограниченного доступа, осознание заказчиком необходимости обеспечения безопасности АСУ ТП лежит не в области соблюдения требований государственных регулирующих органов, а в области повышения эффективности и маржинальности производства. Тратить средства на защиту от иллюзорной "карающей длани государства" ни одно производственное предприятие не будет. Нужно доказать, что реализация тех или иных мер безопасности снизит затраты на производство или при сохранении текущего их уровня повысит прибыль.

AQUARIUS | НАЦИОНАЛЬНАЯ КОМПЬЮТЕРНАЯ КОРПОРАЦИЯ

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ

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.

intel XEON inside™

Реклама. Товар сертифицирован.