РБК+

Генеральный партнер выпуска

КРОК

РЕКЛАМА

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Тематическое приложение к ежедневной деловой газете РБК
Вторник, 29 мая 2018 | 093 (2817)

РИСКИ: ПОЧЕМУ АТАКИ НА ОБЛАКА РАЗРУШИТЕЛЬНЕЕ УРАГАНОВ |
РЫНОК: КАК ИТ-ПРОВАЙДЕРЫ ПОДСТРАИВАЮТ СЕРВИСЫ ПОД ЗАКАЗЧИКОВ |
ИННОВАЦИИ: ЧТО ДАСТ БЛОКЧЕЙН БИЗНЕСУ И ГОСУДАРСТВУ

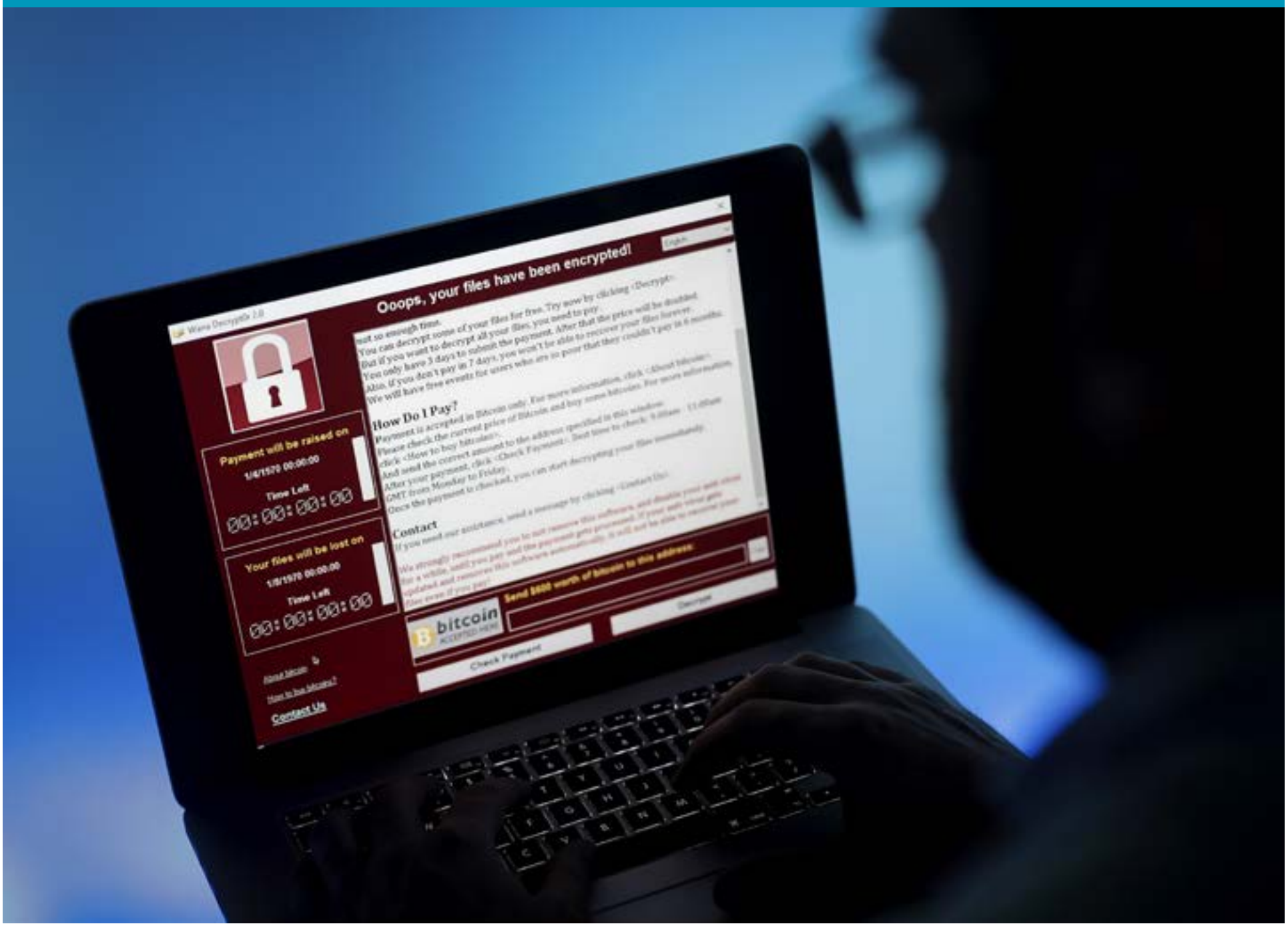

ФОТО: BLOOMBERG

ПРИЕМЫ ПРОТИВ КИБЕРВЗЛОМА

СТАБИЛЬНОСТЬ БИЗНЕСА ВСЕ БОЛЬШЕ ЗАВИСИТ ОТ УСТОЙЧИВОСТИ К КИБЕРАТАКАМ, ОДНАКО ПОЧТИ У ПОЛОВИНЫ КОМПАНИЙ МИРА ДО СИХ ПОР НЕТ ЕДИНОЙ СТРАТЕГИИ ИНФОРМБЕЗОПАСНОСТИ. **АЛЕКСАНДР КОЧЕТОВ**

Кибератаки и несовершенство программного обеспечения могут привести к сбоям, способным «каскадно распространяться по сетям, влияя на общество самым неожиданным образом», говорится в отчете Global Risks Report 2018 Всемирного экономического форума (ВЭФ).

По мнению экспертов форума, киберугрозы достигли «беспрецедентных масштабов» и по разрушительному воздействию сопоставимы с экологическими и геополитическими проблемами. Пока этой опасности отведено лишь шестое место в рейтинге технологических рисков. Но уже в ближайшую пятилетку кибератаки возглавят список потенциальных угроз, уверен совладелец Group-IB Илья Сачков.

За последние несколько лет география киберпреступности серьезно расширилась. В 2015 году в Турции атака на 400 тыс. веб-сайтов повлияла на работу СМИ, телекоммуникационных, банковских сетей и госучреждений. Взлом группой хакеров BlackEnergy электроэнергетических информационных систем Украины в том же году оставил без электричества около 200 тыс. человек, параллельно киберпреступники атаковали телефонные сети, затрудняя восстановление энергоснабжения.

В 2017 году северокорейская банда кибервзломщиков добралась до эталонной системы межбанковских переводов SWIFT и сумела вывести из тайваньского банка Far Eastern International около $60 млн. Наиболее масштабными по охвату и эффекту в СМИ стали эпидемии вирусов-шифровальщиков, прокатившиеся по миру в прошлом году: вредоносная программа WannaCry за три дня атаковала 200 тыс. компьютеров в 150 странах. Зашифрованными оказались

Окончание на с. 2

Начало на с. 1

данные в китайских университетах, на французском и японском автозаводах Renault и Nissan, а также в немецкой железнодорожной компании Deutsche Bahn. Ущерб от одного только WannaCry был оценен в $1 млрд.

ГОСУДАРСТВЕННЫЙ ФАКТОР

По оценке страхового синдиката Lloyd's of London, общий ущерб от глобальной кибератаки может достичь $121 млрд в том случае, если бизнес лишится доступа ко всем облачным хранилищам данных. Ущерб может быть выше потерь от знаменитых североамериканских ураганов, говорит Илья Сачков: последствия шторма «Сэнди» в 2012 году были оценены в $70 млрд, а ущерб от «Катрины» 2005 года — в $108 млрд.

Министерство внутренней безопасности США выявило 60 объектов, на которых даже единственный инцидент в сфере кибербезопасности способен привести к 2500 смертям, убыткам $50 млрд или значительному снижению обороноспособности страны. Главным бизнес-риском в Америке признано «воздействие вредоносных программ, несущих убытки, геополитическую напряженность или вызывающие повсеместную потерю доверия к интернету».

Однако, по оценке экспертов ВЭФ, инфраструктура США до сих пор остается уязвимой.

Около 60% опрошенных в 2017 году американским Pew Research Center экспертов в области ИТ-безопасности уверены: в ближайшие два года именно США столкнутся с кибератаками на объекты инфраструктуры, и эти атаки окажутся успешными.

В 2016 году убытки российских компаний от кибератак, по данным исследования Фонда развития интернет-инициатив (ФРИИ), Microsoft и Group-IB, превысили 200 млрд руб. и достигли 0,25% российского ВВП.

Важная в масштабах страны инфраструктура должна быть защищена государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), напоминает руководитель направления информационной безопасности компании КРОК Андрей Заикин. Закон о безопасности критической информационной инфраструктуры РФ, предусматривающий подключение «транспортной, промышленной, финансовой отрасли, телекома и компаний в области здравоохранения» к этой системе, был принят в прошлом году. Бизнесу предстоит пересмотреть свое отношение к возможным последствиям информационных угроз.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Прошлогодние инциденты показали, что далеко не все компании готовы к отражению даже довольно простых киберугроз, говорит Андрей Заикин: «Проблема чаще всего кроется в человеческом факторе — несоблюдении людьми регламентов эксплуатации и обслуживания систем».

Пока бизнес довольно безалаберно относится к новым рискам или как минимум недооценивает их.

Больше 50% топ-менеджеров компаний — участников опроса PwC, проведенного совместно с журналами CIO и CSO (участвовали 9,5 тыс. руководителей в 122 странах), признались, что у них нет внятной политики реагирования на чрезвычайные ситуации в области ИТ. Почти половина руководителей сообщили, что на предприятиях нет программ обучения сотрудников навыкам защиты информации. Лишь 19% российских респондентов сообщили PwC, что сумеют в случае атак определить их источник.

При этом 40% респондентов понимают, что киберугрозы способны нарушить операционную деятельность бизнеса, а 39% опасаются утечки конфиденциальной информации. Примерно треть понимают, что сбои или действия хакеров способны нанести ущерб качеству их продукции, а пятая часть респондентов осознают возможную угрозу жизни сотрудников.

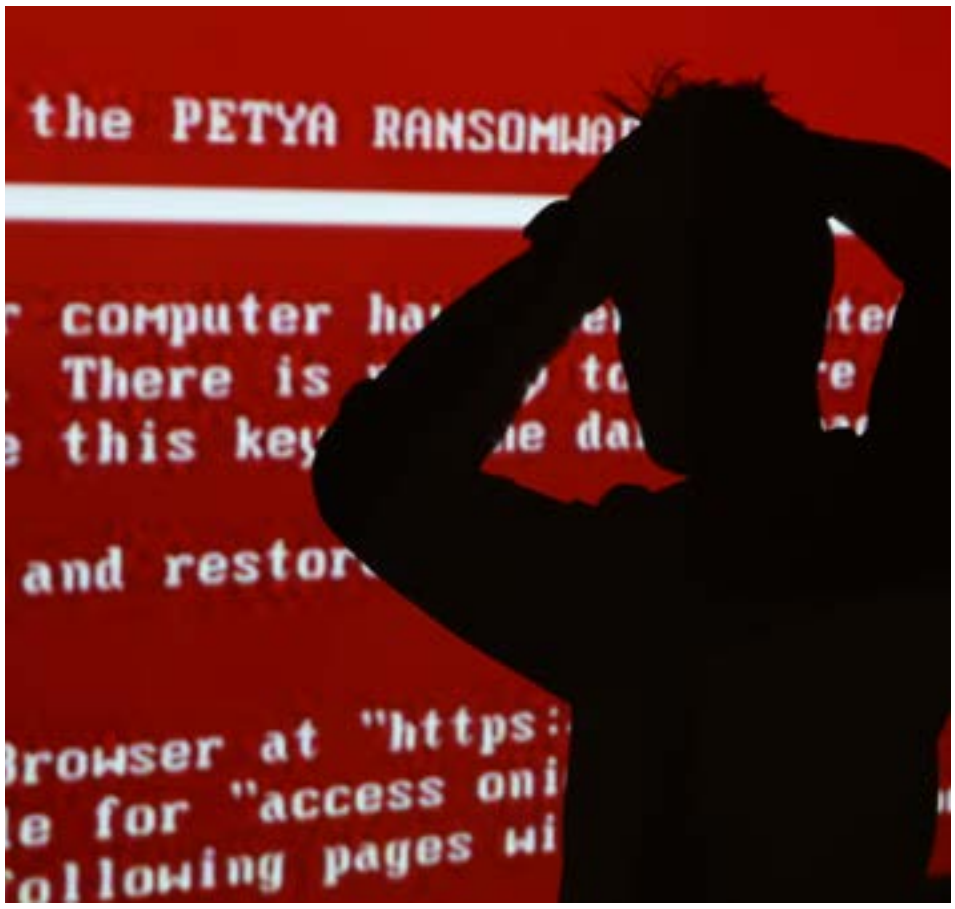

ФОТО: АЛЕКСАНДР РЮМИН/ТАСС

Российские участники исследования PwC, CIO и CSO главной опасностью кибератак считают не нарушение деятельности компании, а утечку данных — так ответили почти половина опрошенных менеджеров.

«Предприятиям необходимо провести переоценку цифровых рисков, сфокусировавшись на повышении устойчивости к угрозам», — говорит глава практики PwC в области кибербезопасности в США Шон Джойс.

ПРЯМАЯ УГРОЗА

Интернет-магазинам больше всего стоит опасаться DDoS-атак, приводящих к отказу обслуживающих покупателей сайтов, говорит Андрей Заикин. Для промпредприятий, по его мнению, наиболее опасны кибератаки, приводящие к изменениям в конфигурации автоматизированных систем управления: «Это может привести к серьезным авариям с человеческими жертвами».

С развитием интернета вещей растет и количество потенциальных целей киберпреступников. По прогнозам американской Strategy Analytics, к 2020 году к Всемирной сети будет подключено до 30 млрд различных приборов — смартфонов, холодильников и других устройств «умного» дома.

Специалисты международного форума по безопасности Threat Horizon 2019 прогнозируют, что именно эти устройства станут основной мишенью модернизированных вирусов-вымогателей, причем зачастую с риском для жизни их владельцев — если речь идет, скажем, о датчиках и термостатах в «умных» домах. Растет вероятность умышленных отключений интернета с целью уничтожить корпорации (жертвами могут стать, например, банки или операторы связи), а также атаки и шантаж сотрудников компаний, владеющих ценными данными о бизнесе, отмечают аналитики Threat Horizon 2019.

Банки сегодня наиболее подготовлены к сбоям структуры, считает руководитель направления «Защита данных и непрерывность ИТ-сервисов» компании КРОК Александр Дубский. «Создание резервных мощностей для защиты данных на случай сбоев в секторе — это уже рыночный стандарт», — говорит эксперт.

НОВАЯ ИНФОРМАЦИОННАЯ ПОЛИТИКА

В этой ситуации исследователи из PwC, CIO и CSO советуют топ-менеджерам взять на себя ответственность за обеспечение кибербезопасности и убеждать в необходимости этой работы советы директоров. Сейчас лишь в 44% компаний советы директоров участвуют в выработке стратегии безопасности.

В крупных компаниях меняется роль главы по информационной безопасности, считает основатель IronNet Cybersecurity, экс-глава киберкомандования США Кейт Александер: именно этот топ-менеджер должен докладывать совету обо всех кибератаках «с акцентом на недостатки в обучении, оборудовании и инструментарии» и помочь совету директоров определиться со стратегией защиты.

Разрозненный набор систем защиты — файрволы, антивирусы, системы защиты от DDoS-атак, которые в настоящее время используют компании,— исчерпал себя, говорит Андрей Заикин: «Такая тактика не позволяет выстроить единую сеть защиты и выявлять уязвимости». Это привело к развитию Security Operation Center (SOC), располагающих технологиями защиты, а также штатом сотрудников, отвечающих за информационную безопасность и регламенты, правила реагирования на атаки.

Устойчивость к кибератакам и сбоям должна рассматриваться владельцами бизнеса как необходимое условие получения прибыли, а не только как способ предотвращения рисков, считают в PwC. Инициатива должна исходить от первых лиц организаций.

Компаниям необходимо разработать стресс-тесты, которые учитывали бы и зависимость бизнеса от других предприятий, считает директор по информационной безопасности компании In-Q-Tel Ден Гир. Он призвал менеджеров в таких тестах получить прямой ответ на вопрос: смогу ли я выдержать сбой в работе тех, от кого я завишу?

Одной из стратегий может стать переход к управляемым услугам по непрерывности бизнеса, которые способны защитить данные от потери и застраховать ИТ-инфраструктуру от сбоев, говорит Александр Дубский. В пример эксперт приводит «разработку устойчивой к катастрофам платформы» для одного из банков, где КРОК «обеспечил высокую доступность клиентских сервисов и ключевых приложений».

«Такие платформы позволяют подготовиться к пиковым нагрузкам и другим непрогнозируемым факторам», — говорит Александр Дубский. Эксперт также призывает бизнес не стесняться «привлекать внешнюю экспертизу, а затем на ее основе формировать актуальные планы на случай аварийного восстановления ИТ-инфраструктуры».

Аналитики PwC стараются убедить руководство крупнейших компаний и даже государств противодействовать новым рискам сообща, «невзирая на организационные, секторальные и национальные границы».

$121

млрд может составить ущерб от глобальной кибератаки в случае, если бизнес лишится доступа ко всем облачным хранилищам, по оценке Lloyd's of London

«УПРАВЛЯЕМЫЕ СЕРВИСЫ — ЕДИНСТВЕННЫЙ ПУТЬ ДЛЯ БЫСТРОЙ ЦИФРОВИЗАЦИИ БИЗНЕСА»

О ВЫЗОВАХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ И ПОДДЕРЖКЕ, КОТОРУЮ ОКАЗЫВАЮТ БИЗНЕСУ ИТ-ПРОВАЙДЕРЫ, РБК+ РАССКАЗАЛ ДИРЕКТОР ДЕПАРТАМЕНТА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ КОМПАНИИ КРОК **ВАЛЕНТИН ГУБАРЕВ**

ФОТО: ТИМУР ИВАНОВ ДЛЯ РБК

«УСПЕХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЕСПЕЧИВАЮТ ПРИНЦИПИАЛЬНО НОВЫЕ ПОДХОДЫ И ДИНАМИЧНЫЕ МОЛОДЫЕ КОМАНДЫ. СЕГОДНЯ БОЛЬШИЕ КОМПАНИИ ВСЕ ЧАЩЕ СОТРУДНИЧАЮТ С АКСЕЛЕРАТОРАМИ И СТАРТАПАМИ»

— В условиях цифровой трансформации какая ИТ-поддержка необходима бизнесу?

— Цель трансформации — кардинальное изменение процессов внутри организации, как взаимодействия с клиентами, так и непосредственно производства.

80% функционала блока ИТ крупной организации — поддержка и модернизация существующих систем, и в лучшем случае 20% ресурсов выделяется на развитие. Выход — аутсорсинг базовых сервисов (управление дата-центрами, вычислительные ресурсы, хранение и защита данных). На рынке достаточно сильных провайдеров, которые оказывают такие услуги профессионально.

Сейчас востребован формат управляемых сервисов, то есть полноценный аутсорсинг. Фактически все, что требуется от клиента, — гибко менять условия договора с поставщиком, так называемый SLA, в зависимости от текущей потребности.

Еще один вызов — способность быстро запустить новые сервисы, необходимые заказчику. Есть целый набор методологий — поиск проблемных областей, клиентоориентированная разработка (CustDev), быстрое тестирование гипотез, создание прототипов и MVP (minimal value product) и гибкие подходы к разработке. Для традиционных ИТ сложно быстро перестроиться. Эту задачу решает, например, формирование совместной кросс-команды с провайдером. Эксперты заказчика лучше знают свой бизнес и потребности клиентов, а подрядчик — методологию и современные инструменты. По такому принципу рождаются очень интересные модели, новые для рынка. Мы используем такой подход с нашими заказчиками, сейчас тестируем прототипы и MVP.

— Каких эффектов позволяет добиться цифровая трансформация и что их обеспечит?

— Цифровая трансформация приводит к тому, что технологии помогают принимать решения, предсказывать события, умно ранжировать и делать индивидуальное предложение для клиента, радикально снижать издержки.

Например, разработанный нами для газораспределительной компании VR-тренажер для отработки последовательности операций персонала при обслуживании оборудования почти вдвое уменьшил расходы на обучение сотрудников. Использовать это решение можно как в «поле», так и в корпоративном учебном центре.

Успех трансформации обеспечивают принципиально новые подходы и динамичные молодые команды. Сегодня большие компании все чаще сотрудничают с акселераторами, стартапами и нередко покупают целые команды. От классических ИТ требуется максимальная гибкость и готовность к изменениям. Меняется роль дата-центров как инфраструктуры для запуска цифровых сервисов в масштабах целых отраслей экономики. Современные ЦОД — это интеллектуальные хабы, предоставляющие широкий спектр сервисов для надежного хранения и обработки данных любого объема. В дата-центрах КРОК для этих целей запущены управляемые сервисы аутсорсинга вычислительной инфраструктуры и защиты данных от потери. Производители ИТ-решений тоже перестраиваются. Например, решения Veritas Netbackup сегодня максимально гибко поддерживают любые конфигурации ИТ-инфраструктуры: физические, виртуальные, облачные. Управляемые сервисы позволяют уйти от большого CAPEX, оплачивая ресурсы только по факту использования. Например, мы создали для компании Avon устойчивую к сбоям инфраструктуру, которая обеспечивает стабильную работу онлайн-магазина, корпоративного портала, системы управления заказами, включая модули отчетности и биллинг представительства компании в России.

— Какие цифровые технологии вы считаете a must для трансформирующегося бизнеса?

— Облачные вычисления обязательны для любого бизнеса, осуществляющего цифровую трансформацию. В облаке запускают онлайн-банки и клиентские кол-центры, обрабатывают и анализируют любые объемы данных. Данные — стратегический актив. Получая самую актуальную аналитику данных из единого хранилища, бизнес сокращает time-to-market новых продуктов и может гибко реагировать на изменения рыночной конъюнктуры. Мы, например, объединили пул решений и управляемых услуг КРОК для эффективной работы с данными согласно концепции «умного» хранения данных.

Растущие объемы данных необходимо защищать от киберугроз — соответственно, технологии информационной безопасности тоже в топе.

— Насколько облачный рынок готов к запросам цифровой экономики?

— Российские облачные услуги хорошего качества при более низкой цене, чем у западных аналогов. Провайдеры способны быстро меняться, добавляя необходимые технологии по запросу. Если каких-то сервисов в России пока нет, то, вероятно, заказчики просто не обозначили на них спрос.

Потребности заказчика — драйвер для рынка. Например, молодая команда онлайн-сервисов Туту.ру, с которой мы сотрудничаем, выжимает из любой технологии максимум и не боится экспериментировать. Работа с ними — своего рода тест на прочность, мы постоянно на связи в режиме онлайн, совместно выявляем узкие места, ищем точки для развития. Таких примеров много, и это идет на пользу облачному рынку.

— Как обеспечить непрерывность бизнеса?

— Любой простой чреват не только убытками, но и репутационными рисками, оттоком пользователей, санкциями со стороны регуляторов. При блокировке IP-адресов ряда глобальных провайдеров деградировали отдельные функции сервисов, и использующие их ИТ-приложения компаний начинали работать медленнее. Быстрый накопительный эффект таких рисков требует от бизнеса оперативной адаптации и предотвращения оттока пользователей.

Путей здесь несколько, включая создание резервных площадок в собственном ЦОД, построение резервного ЦОД или резервирование ИТ-инфраструктуры в облаке.

Спрос на услуги по обеспечению непрерывности бизнеса Disaster Recovery (DR) и внедрение Business Continuity Management растут ежегодно. Причем сегодня можно использовать управляемый сервис DR, когда заказчик резервирует облачные ресурсы провайдера, но платит за них только при возникновении сбоя.

Нашим заказчикам в облаке доступны HA/DR-решения как на основе продуктов open source, так и разработки вендоров. Например, для бэкапа данных клиентов мы используем ПО Veritas (технологию резервного копированию NetBackup), которое дублирует данные и защищает их от потери в случае любых сбоев.

— Какие цифровые инициативы вы реализуете?

— Оценив потенциал промышленного применения технологий виртуальной реальности (VR), мы в 2013 году открыли центр компетенций с демоплощадкой и теперь выступаем экспертами в составе первого в России VR-консорциума.

У нас есть несколько инициатив в области блокчейна. Для крупного инвестиционного банка мы разработали систему регистрации и безопасного хранения ключевых событий инвестиционного процесса «Цифровой контракт». Для ряда государственных ведомств создали систему профилей граждан на блокчейне, позволяющую обрабатывать данные, в том числе о приезжающих в страну.

Совместную работу в командах мы отрабатываем в корпоративном акселераторе. Сначала акселерацию прошли внутренние инициативы, на новом этапе планируем привлечь технологические стартапы. Чтобы цифровые решения были наиболее адаптированы для реального корпоративного рынка, их отрабатывают в общих «песочницах». Например, уже готовы сервисы видеоаналитики для борьбы с кражами в ретейле или решение на базе интернета вещей (IoT) для мониторинга температурных условий и параметров влажности на промышленных объектах. В дата-центрах КРОК такой климат-контроль обеспечил оптимальные условия для стабильной работы вычислительного оборудования и бизнес-приложений заказчиков.

ПРОБНОЕ РАСПРЕДЕЛЕНИЕ

ОПЫТА ВОЗВРАТА ИНВЕСТИЦИЙ В БЛОКЧЕЙН-ПРОЕКТЫ МАЛО, А МНОГИЕ ПРАВОВЫЕ ВОПРОСЫ НЕ РЕШЕНЫ. ОДНАКО В ЭТОМ ГОДУ ВЛОЖЕНИЯ В БЛОКЧЕЙН ДОСТИГНУТ $2 МЛРД, А В 2021-М — $9 МЛРД, ПРОГНОЗИРУЮТ ЭКСПЕРТЫ IDC. МАРИЯ ПОПОВА

ФОТО: ЕВГЕНИЙ ПАВЛЕНКО/КОММЕРСАНТЪ

К 2023 году до 10% мирового ВВП будет сформировано с использованием технологии блокчейн, прогнозируют в международной организации экономического сотрудничества и развития (ОЭСР). Пилотные проекты на блокчейне запускают банки и финтех-компании, ретейлеры, промышленные и транспортные предприятия, а также госорганизации. По данным отчета «Укрепление доверия к правительству», подготовленного IBM Institute for Business Value (2017), девять из десяти руководителей стран планируют в 2018 году инвестировать в разработку блокчейн-решений в области финансовых операций, управления активами, управления контрактами и соблюдения нормативных требований.

От внедрения блокчейна ожидают сокращения операционных расходов (73% респондентов), уменьшения рисков (57%), а также получения дополнительных доходов (51%), приводят результаты опроса ОЭСР среди участников Всемирного экономического форума 2017 года.

В частности, распределенная платформа снижает затраты на устранение ошибок в данных или транзакциях за счет открытого контроля — любые изменения данных возможны, только если участники Сети подтверждают легитимность транзакции в соответствии с общими правилами, говорит Виктор Морозов, директор практики анализа и контроля рисков PricewaterhouseCoopers (PwC) в России. Системы, выполненные с использованием этой технологии, по его словам, повысят доверие между сторонами — участниками информационного обмена и снизят зависимость от центров обработки данных. Благодаря этому блокчейн может использоваться для ведения разнообразных реестров, в процессах контроля государственных инвестиций, социальных платежей.

В цепочках блоков могут храниться записи о продаже недвижимости, государственные реестры и прочая информация. Электронный паспорт на основе блокчейна может даже заменить все другие удостоверяющие документы.

Все данные из блокчейна хранятся на каждом узле, и отключение части узлов никак не влияет на работу сети в целом, отмечает заместитель генерального директора ГК «Программный продукт» Тимур Аитов: «Никто не сможет за вас отправить транзакцию, только вы, от своего имени, подписав ее своим приватным ключом. А все транзакции, которые уже были приняты, — «замайнены» и остаются в блокчейне навсегда».

ПИЛОТНОЕ ВНЕДРЕНИЕ

По итогам 2017 года глобальные расходы на блокчейн-решения составили $945 млн. Лидируют по инвестициям США, страны Западной Европы и Китай. В результате массового перехода от пилотных проектов к полномасштабному внедрению технологии расходы на блокчейн уже в этом году вырастут до $2 млрд, а к 2021 году — до $9 млрд, прогнозируют в международной IDC.

Согласно результатам прошлогоднего опроса IBM среди более 3 тыс. организаций по всему миру, более трети компаний и ведомств отметили актуальность применения блокчейна. 29% государственных ведомств подошли к апробации технологий. Эстония, например, за счет внедрения блокчейна уже экономит до 2% ВВП в год. В распределенную систему переведены данные электронных медицинских карт более 1 млн граждан страны. Технология используется и для системы голосования e-voting в Эстонии.

В Грузии создан реестр прав собственности на блокчейне, где хранится почти 200 тыс. записей о правах на земельные участки, доступных для просмотра всем желающим. Швеция внедряет технологию в сфере сделок с недвижимостью. А в ОАЭ запустили пилотный проект, чтобы к 2020 году перевести на блокчейн весь государственный документооборот (включая заявки на получение визы, оплату счетов, продление лицензий и пр.).

РОССИЙСКИЕ ЦЕПОЧКИ

Объем отечественного рынка блокчейн-решений в прошлом году составил около 1 млрд руб., без учета привлеченных в ходе ICO средств (данные Qiwi). Растет интерес к блокчейну со стороны компаний со сложными цепочками поставок и высоким уровнем контрафакта — на рынках продуктов питания, фармацевтики, автокомплектующих, отмечают в британской Ernst & Young (EY).

Сначала результаты от применения технологии ждут в поставках и логистике, финансах, отслеживании уникальных активов, например драгоценных камней, совместном или частичном владении активами, отслеживании авторских прав, автоматизации микротранзакций с IoT (интернет вещей), говорит руководитель центра технологий, медиа и телекоммуникаций EY Юрий Гедгафов.

В дальнейшем развитие блокчейн-инициатив в России прогнозируется в нефтегазовой, энергетической и финансовой отраслях, а также в поддержке сервисов госуслуг, уверены аналитики PwC.

В начале этого года Росреестр зарегистрировал первый договор участия в долевом строительстве с применением технологии блокчейна совместно с «Дом.РФ» (ранее — АИЖК) и Внешэкономбанком. В дальнейшем было зарегистрировано более 250 ДДУ с использованием распределенного реестра.

Центр блокчейн-компетенций Внешэкономбанка, со своей стороны, представил платформу для госзакупок на блокчейне, которая позволит увеличить эффективность государственных закупок на 30%. Банк России разрабатывает возможность создания блокчейн-системы для расчетов между членами Евразийского экономического союза (ЕАЭС). Предполагается, что за основу будет взята платформа «Мастерчейн» (на основе Ethereum), которую сейчас разрабатывает ассоциация «Финтех» совместно с ЦБ и российскими банками. На первом этапе платформа будет работать лишь внутри России, в дальнейшем с помощью системы члены ЕАЭС смогут передавать финансовые сообщения в формате SWIFT.

ЗАВЫШЕННЫЕ ОЖИДАНИЯ

Однако пока блокчейн остается экспериментальной технологией. Многие вопросы, выявленные при его использовании, еще не решены; например, по производительности решения на блокчейне пока значительно уступают традиционным. При этом на больших объемах такие проекты требуют значительных объемов вычислительных мощностей и существенных энергетических затрат.

Пока «традиционные» технологии дают тот же или более удобный интерфейс для работы пользователей и более высокую скорость обработки транзакций, говорит Виктор Морозов.

Переход на блокчейн — достаточно сложный процесс, требующий экспертизы, которую рынок пока только накапливает. И в вопросе возврата инвестиций также недостает опыта. Не сформированы и стандарты для проектов, говорит Юрий Гедгафов. «Большинство решений реализуется на платформах (Ethereum, Corda, Hyperleger) без формальной сертификации для возможности работы с персональными данными», — отмечает он.

Задачи, связанные с обработкой персональных данных или данных, составляющих коммерческую и государственную тайну, требуют сертифицированной платформы, которая в случае блокчейна включала бы шифрование по ГОСТу, считает Тимур Аитов.

До последнего момента в России использование блокчейн-технологий осуществлялось вне правового поля. Ожидается, что нормативная база по блокчейну и криптовалютам будет сформирована в России до конца 2018 года. Это должно усилить внимание к отрасли со стороны институциональных игроков и, как следствие, заметно расширить возможности компаний по привлечению финансирования.

Ожидания от блокчейна сейчас завышенные, отмечает Юрий Гедгафов, добавляя: «Но потенциал точно есть, и надо пробовать, чтобы не отстать».

«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ» (18+)

Тематическое приложение к «Ежедневной деловой газете РБК» является неотъемлемой частью «Ежедневной деловой газеты РБК» № 093 (2817) от 29 мая 2018 г.
Распространяется в составе газеты
Материалы подготовлены редакцией партнерских проектов РБК+

Партнер: ЗАО «КРОК инкорпорейтед».
Реклама

Учредитель: ООО «БизнесПресс»
Издатель: ООО «БизнесПресс»
Директор ИД РБК: Ирина Митрофанова
Главный редактор партнерских проектов РБК+: Наталья Кулакова
Шеф-редактор печатной версии РБК+: Юрий Львов
Редактор РБК+ «Информационные технологии»: Юлия Хомченко

Выпускающий редактор: Андрей Уткин
Дизайнер: Дмитрий Иванов
Фоторедактор: Алена Кондюрина
Корректоры: Татьяна Поленова, Маргарита Тарасенко

И.о. главного редактора газеты: Игорь Игоревич Тросников

Рекламная служба: (495) 363-11-11, доб. 1342
Коммерческий директор издательства РБК: Анна Брук
Директор по продажам РБК+: Евгения Карлина
Директор по производству: Надежда Фомина

Адрес редакции: 117393, Москва, ул. Профсоюзная, 78, стр. 1