



15 Сетевая виртуализация открывает двери отечественному телеком-оборудованию

16 Российские компании посчитали цену «бумажной безопасности»

17 Стартап заплатит пользователям за их персональные данные

Финты вокруг финтехе

Крупные российские банки вслед за иностранными коллегами идут по пути цифровой трансформации. Основные ее признаки — переход на онлайн-каналы взаимодействия с клиентами и интеграция их в единое пространство. В это же время инновационные лаборатории банков уже заглядывают в будущее: тестируют блокчейн и открывают свои API для финтех-стартапов.

— инновации —

Блокчейн и инновации вокруг этой технологии называют убийцами классических финансовых институтов. Ведь использование криптовалют и «умных контрактов» делает участие доверенного посредника (банка) ненужным. Но это в теории — на практике оказывается, что блокчейн укрепляет позиции финансовых компаний и усиливает их роль в экономике.

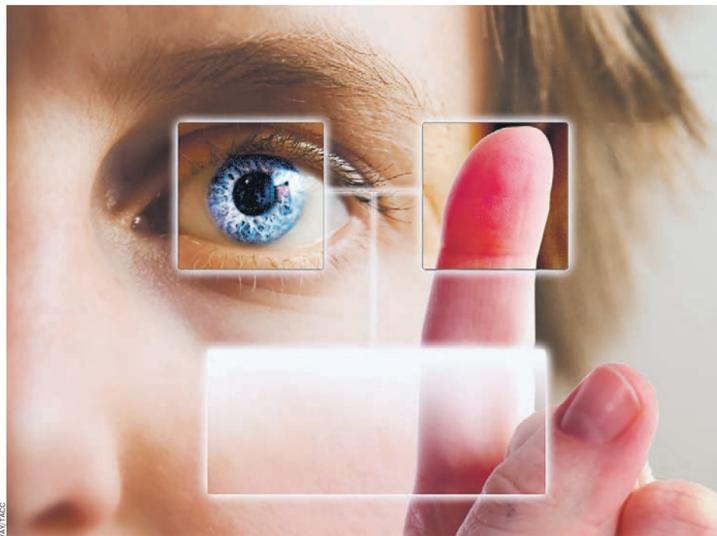
Первый громкий эксперимент в этой сфере провели несколько российских финансовых компаний, создавших в октябре совместный проект на блокчейне. Алексей Благирев, директор по инновациям банка «Открытие», объясняет: «Мы предложили создать интерфейс между банками—операторами персональных данных, чтобы можно было проверять информацию о клиентах не только в государственных источниках, но и друг у друга, без передачи самих данных. Для каждого человека создается отдельная запись закодированных признаков, которая его уникально идентифицирует. Эта запись сохраняется в блокчейне. Мы, по сути, создали прототип digital identity, то есть виртуальной личности или электронного паспорта. Это такой «слепок» человека, который позволяет банкам обмениваться информацией о мошенниках, банкротях, умерших — и очень оперативно это делать. При этом передача персональных данных не происходит: передается сложный хэш (шифр), который в теории можно математически перебрать, но в реальности это крайне трудозатратно. Это на самом деле даже не один хэш, а сложная комбинация нескольких, включающая в том числе «отпечаток» сведений о переданном документе. Перед тем как этот хэш формируется, обязательно необходимо выполнить так называемый

proof of existence — определить, действительно ли данная личность существует, используя для этого государственные источники через систему межведомственного электронного взаимодействия».

Данный проект решает одну из самых актуальных проблем в финансовом секторе — идентификации клиентов. «Всегда сложно проверить, существует ли человек на самом деле, не пришел ли кто-то с паспортом умершего. Банки — одни из крупнейших операторов персональных данных. Более того, именно банки осуществляют процедуру идентификации клиентов перед открытием счета или проведением транзакции. Актуальность данных, которыми располагает банк, выше, чем актуальность аналогичных данных, представленных в государственные учреждения. Отраслевой стандарт банковской индустрии — это контакт с клиентом как минимум каждые шесть месяцев. Также банк собирает больше информации о клиенте в процессе сопровождения сделок, чем другие организации», — говорит господин Благирев.

Распределенный реестр «Мастерчейн» Банка России, о котором рассказывает эксперт, создали в партнерстве банк «Открытие», Сбербанк, Альфа-банк, Тинькофф-банк и Qiwi. Первые транзакции в платформе прошли успешно. Их провели на прототипе компании «Синимекс», который представляет собой сервис для обмена данными о клиентах разных банков. В основу «Мастерчейна» легла технология Ethereum.

На следующем шаге в «Мастерчейн» можно будет записывать также события, которые происходят с каждым клиентом и которые сопровождаются идентификацией. Например, факт мошенничества или просрочки по кредиту. Это открывает множество перспектив. К примеру, кредитное бюро, которое хранит



информацию о просроченных платежах и выполняет скоринг, можно будет вообще заменить алгоритмами на основе распределенных реестров для банков участников блокчейна. Такая система на основе данных из распределенного реестра сама будет проводить идентификацию, рассчитывать условия кредита и заключать «умный контракт», причем мгновенно. «Технически идею о переиспользовании факта идентификации другим банком мы можем воплотить в реальность уже к концу текущего года. Но на уровне существующего законодательства (115-ФЗ) по-прежнему требуются уточнения и изменения, чтобы это стало возможно использовать», — комментирует господин Благирев. Сегодня уже существуют возможности ускорить блокчейн до 1 тыс. транзакций в секунду, так что технология может использоваться на практике. В будущем это позволит решить возможные проблемы кредитных бюро, связанные с достоверностью данных, ошибками, потерей данных и прочими сложностями.

Технологией блокчейна активно интересуется также MasterCard. Михаил Федосеев, директор по развитию бизнеса и цифровых

технологий MasterCard в России, рассказывает: «Возможности, которые мы видим, работа с блокчейном, заключаются в объединении нашего многолетнего опыта, знания локальных рынков и партнеров для того, чтобы и в дальнейшем предлагать простые решения для людей и бизнеса. В R&D-подразделении MasterCard Lab мы исследуем и развиваем потенциал блокчейна. Запатентовали собственное решение на основе этой технологии и сейчас тестируем его. Как часть подготовительной работы в этом направлении подали заявки более чем на 30 патентов, связанных с блокчейном и криптовалютами. Это дополняет наши инвестиции в Digital Currency Group».

Сыр для изобретателей

Финтех — решения на стыке информационных технологий и финансовых услуг — горячая тема для венчурных инвесторов. Глобальные инвестиции в финтех-стартапы, по данным CB Insights, только во втором квартале текущего года достигли \$9,4 млрд. Павел Никон, инвестиционный менеджер Фонда развития интернет-инициатив (ФРИИ), говорит, что по количеству компаний и их оценкам

самые большие области финтехе — это платежи и онлайн-кредитование. Это, к примеру, площадки для peer-to-peer (когда финансовые услуги предоставляют люди друг другу напрямую, минуя банки и других посредников), платежные системы. В среде таких проектов идет серьезная конкуренция. Помимо блокчейна также повышенный интерес наблюдается к чат-ботам, в том числе для финансовой сферы. Один из таких проектов — TalkBank (<http://www.talkbank.io/>), первый в РФ чат-банк, резидент десятого акселератора ФРИИ. В девятом наборе акселератора ФРИИ приняла участие компания Choicy (<http://gochoicy.com/>), разработавшая технологию на базе искусственного интеллекта, который помогает сделать выбор.

Банки относятся к финтех-стартапам не как к угрозе, а как к источнику новых идей, а также потенциальным объектам для поглощения. Среди партнеров ФРИИ в программе развития финтех-стартапов — Сбербанк, Райффайзенбанк, банки «Открытие», «Санкт-Петербург», «Ак Барс». «Представители банков не только делятся экспертизой с нашими проектами, готовы делать пилотные проекты, но и соинвестировать в них», — говорит господин Никон. Для развития финтех-предпринимательства банки даже хотят затеять «регуляторную песочницу». Алексей Благирев рассказывает, что суть идеи заключается в создании пространства для экспериментов, в котором компании-инноваторы получают льготы от регуляторов на определенный период и объем операций. «Самое сложное здесь, как оказалось, — это сформулировать, какие же, собственно, эксперименты там проводить. Главным большим вопросом для банков остается идентификация. Основной фокус пока приходится пока на этот процесс, например предоставление кредита по ограниченному количеству полей (знаний) о клиенте», — говорит господин Благирев. — В этом проекте также важно понимать, как будет устроена инфраструктура, как именно будут раскрываться API».

Пока в России идет дискуссия на этот счет, Европейский рынок уже активно готовится воплощать вторую платёжную декларацию, принятую Еврокомиссией. Она обязывает банки с января 2018 года предоставлять API для внешних финтех-проектов и стартапов.

«Новая оргструктура стала фундаментом для дальнейших изменений»

— цифровая трансформация —

Райффайзенбанк в нынешнем году начал активно поддерживать стартапы в области финтехе, которые, по сути, становятся внешними R&D-лабораториями компании, тестирующими разные гипотезы и бизнес-модели. Впрочем, и внутри организации идут инновационные преобразования, о которых корреспонденту «Ъ-Информационные технологии» СВЕТЛАНА РАГИМОВОЙ рассказал АНДРЕЙ ПОПОВ, член правления Райффайзенбанка.



— В последнее время часто слышу о том, что в Райффайзенбанке реализуются заметные ИТ-проекты. Знаю, что проведен масштабный переход на VDI (Virtual Desktop Interface), используется интеллектуальная система IVR (Interactive Voice Response), внедренная сов-

местно с КРОК. Вы даже получили премию «IT-Лидер». — Мы действительно много делаем в последние годы. Мне тяжело судить, насколько эта активность заметна рынку. Было несколько случаев, когда на конференциях подходили кол-

леги и спрашивали о наших проектах, о которых дошла информация. Партнеры говорят, что наш проект по VDI — один из самых крупных в Европе. Мы перевели 95% сотрудников на виртуальный десктоп. — Насколько я знаю, вы перестроили работу ИТ-департамента в последние годы. Возможно, с этим связано то, что на рынке стали говорить о ваших ИТ-проектах... — Мы действительно стали активнее. Меня пригласили в компанию для того, чтобы изменить схему взаимодействия ИТ-департамента с бизнесом, создать здоровые взаимоотношения, которые помогли бы банку развиваться. Научить айтишников и менеджеров работать вместе.

— В чем была основная проблема? Бизнес чего-то хотел от ИТ, айтишники этого не делали? — Была классическая ситуация: бизнес чего-то хочет, но не умеет объяснить, чего именно. Причем запросы постоянно меняются. Айтишники не укладываются в сроки, у них очередь из проектов на три года вперед. Еще и задачи постоянно меняются на ходу. Условия на рынке ведь динамичные — менеджеры пытаются под них подстроиться. В итоге никто ничего не успевает, каждый сваливает вину на другого, департаменты прекращают общаться вообще. На самом деле и те и другие правы. Но и не правы в чем-то тоже обе стороны. — Получилось в итоге их подружить? Через какие сложности пришлось пройти? — На мой взгляд, да, нам удалось наладить коммуникации между департаментами. Пару лет назад мы вышли на уровень, на котором уже можно думать не просто о превращении накопленного за 15 лет багажа в нечто ценное, а о чем-то новом.

Было сложно, конечно. Пришлось объяснять бизнесу, что нереально абсолютно все сделать сразу. Даже если

увеличить штат айтишников в два, три, десять раз, все равно не получится ускорить процесс. Иногда, наоборот, увеличение числа разработчиков приводит к замедлению работы над проектом. Я в свое время рекомендовал прочитать книгу «Мифический человекомесяц» всем руководителям среднего звена. Она очень помогает понять суть происходящего. Но, думаю, мало кто прочитал. Приходилось объяснять на пальцах, на конкретных проектах. Но и этого было мало — оставался оттенок недоверия.

В управлении бизнесом все линейно: нанимаем в два раза больше продавцов, они начинают в два раза больше продавать. Как объяснить, что в ИТ так не работает? Мы стали полностью открытыми, начали приглашать к нам в офис, все объяснять и показывать, ничего не скрывая. Рассказываем в деталях: если хотите внести изменения в проект — не вопрос, вне-

сем, но последствия будут вот такие. Мы не перестраховываемся, закладывая дополнительное время на проект, ничего не прячем. Этот процесс преодоления недоверия потребовал больших усилий и времени. Сложно изменить отношение, когда оно уже сложилось, когда менеджеры думают, что тут просто сидят ленивые люди, которые не хотят ничего делать.

Провели огромное количество встреч, от которых осталось много ярких воспоминаний. На них я старался объяснить, что, так же, как ребенка нельзя родить раньше срока, так и ИТ-проект не получится взять и реализовать за три недели. Однажды мне коллега ответила на этот аргумент: да, но девять женщин могут усыновить девять детей за месяц. Возможно, но результат будет совсем другой. Одним из шагов к полной прозрачности был переход на регулятивный выпуск релизов корпоративной системы.

Panasonic BUSINESS

Architect team

Нравится: 1364

#МФУ #экономичные #быстрые #дуплекснаяпечать #печатьА3 #надежные #универсальные

НА ТЭГЕ УНИВЕРСАЛЬНОСТИ

Возьмем поддержку дуплексной печати и печати формата А3, добавим надежность, скорость и экономичность и получим новую линейку лазерных МФУ Panasonic. Созданные ускорить и облегчить рабочий процесс, они мгновенно станут незаменимыми помощниками в трудовых буднях!

- Поддержка дуплексной печати и печати формата А3
- Экономичность в использовании и удобство в обслуживании

DP-MB545RU
факс/телефон/
принтер/сканер/
копир/РС-факс

DP-MB536RU
факс/телефон/
принтер/сканер/
копир/РС-факс

www.panasonic.com mfu.panasonic.ru

Информационный Центр Panasonic: для Москвы 8-495-725-05-65, для регионов РФ 8-800-200-21-00 (звонок бесплатный). На правах рекламы ООО «Панасоник Рус» — уполномоченного представителя компании Panasonic Corporation Ltd. на территории России.

Review

Связь-2017



Отечество на проводе

Российские производители телекоммуникационного оборудования стремятся поймать волну импортозамещения и получить хорошие контракты. Но клиенты пока с осторожностью относятся к отечественным вендорам. В следующем году поставщики имеют хороший шанс показать, чего удалось достичь за последние годы. На выставке «Связь-2017», которая пройдет 25–27 апреля в Москве в Экспоцентре на Красной Пресне, будет специальная секция, посвященная российским производителям телеком-оборудования.

— событие —

По данным Национального исследовательского университета ВШЭ, в 2014 году доля российских производителей на рынке оборудования для предоставления услуг связи не превышала 12%. Исследователи просчитали два сценария импортозамещения в этой области, по которым в ближайшие годы отечественные поставщики могут занять от 42% до 65% рынка. Какой из сценариев реализуется? Это зависит во многом от действий регуляторов, от закупок крупнейших операторов РФ, а также от самих поставщиков оборудования. Ведь если качество продуктов соответствует требованиям клиентов, то проблем с контрактами не будет.

Константин Анкилов, аналитик TMT-Consulting, говорит, что в сегменте программно-аппаратных комплексов для связи российские производители давно уже заняли отдельные сегменты рынка, в первую очередь это оборудование для передачи данных. «Выйти в крупнейшие сегменты, в первую очередь решений для мобильной связи, у российских вендоров, к сожалению, не получается. Попытки были. Но пока отечественные разработчики не в состоянии предложить альтернативу зарубежному многомиллиардному R&D», — добавляет он.

При этом заказчики в целом готовы к тому, чтобы покупать отечественное — это как минимум снижает валютные риски. Один из крупнейших клиентов на этом рынке — оператор «Ростелеком» — объявил о том, что треть закупленного оборудования в 2015 году была отечественной. Речь идет о системах спектрального уплотнения CDWDM/DWDM на реги-

ональных сетях и об оборудовании для сетей IP/MPLS уровня Aggregation Router, Demarcation Router. Начиная с 2013 года «Ростелеком» закупает оборудование и ПО отечественной компании «Натекс». Сумма контрактов по этим закупкам к началу 2016 года достигла 880 млн руб. На этом компания, которая ежегодно тратит на оборудование десятки миллиардов рублей, не останавливается и планирует увеличивать долю отечественных поставщиков в своих закупках. В текущем году контракт на поставку маршрутизаторов для GPON на сумму \$17,4 млрд получила российская компания «Элтекс». «Ростелеком» — якорный клиент этого поставщика и закупает продукцию выпускаемой им продукции.

Регуляторы также способствуют развитию бизнеса российских компаний. Помимо уже принятых правил о том, что отечественному оборудованию должен отдаваться приоритет при госзакупках, идет обсуждение и других инициатив. В частности, «Б» в сентябре рассказал о проекте «дорожной карты» по импортозамещению телеком-оборудования на 2016–2020 годы (подготовлена в рамках работы подгруппы «ИТ + Суверенитет»). Одна из целей, описанных в документе, — переход российских операторов к 2020 году на 85% отечественного телекоммуникационного оборудования. Среди прочих мер «дорожная карта» предлагает ввести с 2017 года законодательный запрет даже для частных телекомов использовать зарубежную технику и ПО в некоторых сферах деятельности. Например, «при накоплении статистических данных, проверке, анализе и фильтрации сетевых пакетов по их содержанию (DPI) или оказани-



нии услуг госструктур. Запрет на закупку импортного оборудования (при наличии отечественных аналогов) должен распространяться по замыслу создателей документа также на госорганы и компании с госучастием. Впрочем, участники рабочей группы позже сообщили, что проект пока еще сырой и требует доработки и что импортозамещение не должно быть директивным. Но если предпринять ряд действий, то к 2020 году 50% продаваемого оборудования в России будет отечественного производства. На это и нацелена «дорожная карта».

«Стимулирование импортозамещения может помочь отдельным рыночным сегментам, но в крупнейших с точки зрения поставок и закупок сегментах отечественная промышленность не сможет предложить альтернатив, которые не привели бы к ухудшению качества связи на массовом рынке. Соломоново решение — производство в СП на территории России. Рынок прошел этот путь 15 лет назад, но за пределы отдельных сегментов телеком-оборудования российские производители так и не вышли», — комментирует инициативы регуляторов Константин Анкилов.

Отечественные производители со своей стороны стараются подтянуть качество. Владимир Калинин, советник руководителя Федерального агентства связи, говорит, что к настоящему моменту уже можно говорить о готовности оборудования, произведенного в России, к замещению импортных аналогов на территории на-

вано единое комплексное предложение, закрывающее потребности операторского рынка.

Это реальное оборудование, которое доказало свои возможности и уже поставляется на рынок. Из заметных разработчиков можно назвать компании «Т-платформы», Т8, ряд наших компаний, в том числе «Масштаб» и «Булаг», — рассказывает он. — Был бы мнение, что сегодня российские производители не в состоянии закрыть ряд сегментов. Например, не производят оборудование для построения оптических высокоскоростных систем передачи данных. Однако это не так. В качестве примера можно привести отечественную DWDM-платформу «Волга». Это оборудование современного уровня, на котором установлен ряд мировых рекордов по скорости передачи данных на большие расстояния — это факт, который официально зафиксирован.

В контуре ОПК ведутся разработка и производство коммутаторов, маршрутизаторов, IP ATC, серверов и СХД. Весной было создано совместное предприятие с «Ростелекомом», которое осуществляет разработку широкого спектра оборудования для операторов связи с учетом их требований. В активе ОПК на сегодня порядка 40 образцов доверенного телеком-оборудования.

Кирилл Шишков, начальник отдела рекламы и PR компании Т8, говорит, что еще недавно о существовании российского оборудования знали только те, кто его разрабатывал, и небольшое количество заказчиков. «Качество нашего оборудования, под этим мы понимаем количество часов наработки на отказ, не уступает зарубежному», — говорит он. — По функциональности идет непрерывная работа — да, «плюшек» у нас нет, но оборудование отвечает необходимым требованиям заказчиков, в том числе таких требовательного клиента, как «Ростелеком». С поддержкой у нас ситуация лучше, чем у многих зарубежных вендоров, мы гораздо более оперативны и часто предоставляем услуги больше, чем прописано в договорах. По количеству сервисных центров не будем сравнивать, поскольку у нас сравнимо меньше объемов продаж. Будут такие же продажи — будем расширять сервисную сеть. Если по итогам тестов бывают замечания, опера-

тивно исправляем. Все наше оборудование сертифицировано, при необходимости проходим зарубежную сертификацию, например одного из законодателя мод оборудования для дата-центров Brocade».

Т8 работает в довольно узком сегменте рынка: разрабатывает системы спектрального уплотнения для волоконно-оптических сетей. Основной заказчик компании — оператор «Ростелеком», не так давно в список клиентов добавился Сбербанк, ведутся переговоры с зарубежными компаниями. Ключевой продукт Т8 платформа «Волга» активно конкурирует с аналогичными системами одного из самых агрессивных игроков на российском рынке — компании Huawei. «Объем нашего бизнеса не позволяет сильно расширять свою линейку, у нас нет ресурсов на это. Наше основное направление — российский транспортное оборудование для магистральных волоконно-оптических сетей, в данном сегменте мы можем заменить любого зарубежного вендора. Причем по лучшей цене и качеству», — объясняет Кирилл Шишков.

На предстоящей выставке «Связь-2017» Т8 покажет рабочие стенды, в составе которых будет новейшая плата 400 Гб/с мукспондера. «Это уникальное для России оборудование, и мы рассчитываем на интерес со стороны дата-центров», — рассказывает Кирилл Шишков. — Помимо высоких скоростей мы покажем новое низкоскоростное оборудование — агрегатор медных портов. В рамках собственной программы «импортозамещения» в планах стоит показ модификации 400 Гб/с блока на собственном оптическом модуле. Это импортные компоненты, но только модуль нашей собственной разработки».

Компания «Натекс», которая ежегодно участвует в выставке «Связь», в следующем году планирует обновить линейку Ethernet-коммутаторов, показать на мероприятии новые модели для различных сегментов.

Сегодня в гостресте отечественных производителей телеком-оборудования 18 компаний. Многие из них наряду с упомянутыми выше Т8, «Натекс» и «Элтекс» представят свою продукцию на «Связи-2017» и получат возможность убедиться в качестве своей продукции новых клиентов.

Мария Анастасьева

информационные технологии

Виртуализируй все

— инновация —

SDN — одна из самых актуальных тем на российском ИКТ-рынке. Виртуализация поможет операторам, а также крупным корпорациям, владеющим собственными сетями связи, снизить CAPEX и ускорить сроки вывода продуктов на рынок. Интеграторы и вендоры на волне популярности этих технологий надеются получить большой заказ от телекома.

Глобальный рынок SDN/NFV (Software-Defined Networks и Network Function Virtualization — программно-определяемые сети и виртуализация сетевых функций) растет на 80–100% в год и, по данным Infonetics Research, к 2019 году превысит \$13 млрд. Российские показатели скромнее, хотя аналитики существенно расходятся в оценках, определяя пока терминологически: что вообще включать в сегмент NFV/SDN. Виртуализация возможна на всех участках сетевой инфраструктуры: на последней миле, на опорных/магистральных сетях и в ЦОДах.

Промышленное применение данных технологий в России только набирает скорость. Формирующийся рынок находится на стадии «осторожных пилотов», причем технология реализуется пока в основном в дата-центрах, а не на сетях операторов.

«Рынок SDN/NFV-решений пока находится на ранней стадии, не закончена разработка стандартов, есть проблемы с кадрами: программистов и инженеров, специализирующихся на этой теме, категорически не хватает», — отмечает Олег Шапов, генеральный директор и основатель Brain4Net. — В течение трех-четырёх лет произойдет полная трансформация сетей и переход их на парадигму виртуализации, при этом среднегодовой рост будет трехзначным». В компании прогнозируют объем рынка решений для сетевой виртуализации только на транспортном уровне в \$375 млн. В компании «Техносерв» обращают внимание на то, что если рынок SDN в России, как неформированный, проходит сегодня стадию пилотов, то NFV уже находится на стадии коммерческих внедрений.

По экспертным оценкам, именно телеком будет оставаться основным потребителем (до 90%) решений SDN/NFV в России до 2020 года. Затем будет расти доля крупных частных компаний и госучреждений, эксплуатирующих распределенные сети передачи данных и также заинтересованных в виртуализации. Ожидаемый крупный игрок

здесь, например, Сбербанк. Ожидается, что поворотным в динамике российского сегмента SDN/NFV станет 2018 год.

Новый цифровой ответ

Глобальными лидерами в сегменте NFV (и виртуализации в целом) считаются Verizon, AT&T, Telefonica. Крупнейшая из коммерческих сетей SDN/NFV для операторов связи в мире построена China Mobile Communications Company. Как пример большинство российских игроков приводит AT&T, которая к 2020 году планирует виртуализировать 75% своей сети. Уже более 50% стратегически значимых приложений этого оператора перенесены в облако.

По оценкам Infonetics Research, внедрение SDN может снизить операционные расходы на телекоммуникационную инфраструктуру на 48% в год, капитальные — на 52%. Vodafone Research прогнозируют, что NFV сократит OPEX на 60% в течение трех лет, а CAPEX — на 59% в течение пяти лет. При этом ожидается, что нагрузка оборудования повысится на 20–30%. Правда, применительно к российским игрокам речь сегодня идет скорее о перераспределении CAPEX/OPEX, а резервы экономии будут рассчитаны позже.

В первую очередь технология SDN/NFV привлекают операторов связи возможностью повысить эффективность и эластичность сети в ответ на меняющиеся запросы рынка. Средний срок выведения нового продукта в телекоме составляет год-полтора (а может достигать и двух лет). За это время спрос может кардинально поменяться, и услуга будет уже просто не нужна.

Когда лавинообразно растет трафик, причем критичный к задержкам на сети, потребитель требует все больше конвергентных услуг, а традиционные доходы от голосовых услуг уходят, нужны серьезные шаги. В связи с этим ключевое слово 2016 года на российском рынке — цифровая трансформация. SDN/NFV в этой парадигме — возможность уйти от роли «трубы» по перегону трафика и перейти к сервисно-ориентированной модели, в которой облачные и прочие цифровые сервисы для клиентов становятся органичной частью основного бизнеса оператора.

«На практике переход на SDN означает перестройку „умов“, всей философии построения сетей, а главное — платформенное изменение того, во что инвестировали долгое время», — объясняет директор департамента ин-

фраструктурных и телекоммуникационных решений группы «Астерос» Валерий Соколов.

Цель внедрения SDN — сделать сети такими, чтобы можно было быстро менять их конфигурацию, емкость и спектр услуг, отмечает Сергей Андронов, директор Центра сетевых решений компании «Инфосистемы Джет».

Сегодня основная часть анонсируемых публичных проектов в РФ сосредоточена вокруг «Ростелекома», который сообщил о планах обновления сетевой инфраструктуры с внедрением SDN и NFV и объявленными инвестициями в виртуализацию объемом примерно 60 млрд руб. на пять лет. Параллельно проводится тестирование виртуализированных сетевых функций («Вымпелком»). А МТС вместе с Ericsson протестировали облачное решение для передачи голоса в сетях LTE на компонентах с реализованной NFV.

Куски пирога

Рынок SDN/NFV пока не имеет четких границ и привлекает значительное количество новых игроков, в том числе стартапов. Артем Гениев, архитектор бизнес-решений VMware, говорит, что есть две основные категории поставщиков решений NFV и SDN: традиционные производители сетевого оборудования (Juniper, Cisco, Brocade, Huawei, Nokia, Ericsson и др.) и вендоры, которые исторически не являются поставщиками аппаратных решений (VMware, Athonet, Velocloud, Metaswitch и др.). «Овора о достоинствах и недостатках различных поставщиков, важно помнить об истории появления SDN и NFV, о задачах, которые SDN и NFV призваны решить, а также о возможных подходах к реализации SDN и NFV», — объясняет он. — Выгоды использования виртуализации функций сетей связи (NFV) достигаются за счет перехода от фрагментированной коммуникационной инфраструктуры, построенной на монолитных, вертикально интегрированных сервисных платформах, к инфраструктуре нового поколения, в которой функции сети связи представлены в виде приложений и абстрагированы от аппаратной инфраструктуры. При этом аппаратная инфраструктура представлена в виде серверов общего назначения, систем хранения и сетей».

Положительный экономический эффект от использования NFV, таким образом, складывается из трех составляющих. Во-первых, это сокращение затрат на инфраструктуру, необходимую для работы функций сетей связи за счет стандартизации оборудования, высо-

кая эффективность его использования, экономия от масштаба и возможностей дополнительной конкуренции между поставщиками функций сетей связи. Конкуренция возникает за счет привлечения новых игроков рынка, специализирующихся на поставке функций сетей связи, оптимизированных для размещения в telco-cloud. Во-вторых, использование подхода «открытых инноваций» позволяет операторам связи разрабатывать и предлагать абонентам новые услуги связи, создающие большую ценность по сравнению с традиционными услугами. Это создает возможности для роста выручки оператора связи на фоне высокого конкурентного давления в сегменте традиционных услуг. В-третьих, это сокращение времени вывода новых услуг связи на рынок, что стимулирует рост абонентской базы, способствует уменьшению оттока абонентов, повышению выручки с абонента.

«Важно помнить, что виртуализация функций сетей связи изначально создавалась по инициативе операторов связи, а не производителей сетевых решений. Фундаментальная задача была в том, чтобы отделить функции сети связи от нижележащей аппаратной инфраструктуры, создав в том числе предпосылки для появления поставщиков функций сетей связи, не отягощенных разработкой аппаратной инфраструктуры. Они должны были предлагать отрасли инновационные решения, оптимизированные для работы поверх виртуализированной commodity-инфраструктуры», — объясняет Артем Гениев. В какой-то мере задача была решена: по итогам 2015 года венчурные инвестиции в NFV/SDN превысили \$650 млн, на рынке появляются множество стартапов, разрабатывающих решения в области NFV и SDN.

В то же время традиционные поставщики сетевого оборудования стараются снова позиционировать вертикально интегрированные решения, только теперь для NFV: предлагают сетевые функции, а вместе с ними серверы, гипервизор, оркестрацию и SDN с SDS в придачу. Получается, что в попытках уйти с помощью NFV от вертикальных специализированных решений оператор связи к ним же и возвращается, только под другим соусом.

Проникновение NFV-решений от новых поставщиков также сдерживается рядом факторов. Это не всегда зрелость и стабильность решений, недостаточный территориальный охват, специфичные для локального рынка требования сертификации, отсутствие исторических отношений с операторами связи в

регионе, консерватизм, свойственный техническим блокам операторов, недостаточные возможности поставщика в области проектного и проектного консалтинга, а также последующей поддержки и эксплуатации виртуализированной функции сети связи.

В отношении SDN ситуация немного другая. Существует несколько подходов к построению программно определяемых (конфигурируемых) сетей. Можно решить задачу предоставления и эксплуатации сетевых сервисов через управление оборудованием (к подобным решениям относятся, в частности, SDN-контроллеры на основе OpenFlow). А можно полностью разделить сетевые сервисы и аппаратные средства обеспечения сетевой связности, используя оверлей-сети (это случай VMware NSX), или же можно комбинировать эти подходы в рамках единого решения. Каждый из этих путей имеет свои достоинства и недостатки. Клиенты пока не определились с тем, какие варианты они выберут.

Тем не менее SDN/NFV не слишком изменит распределение долей по вендорам телекоммуникационных продуктов, считает Валерий Никитин, отмечая, что на рынке уже сложилась практика работы с конкретными поставщиками, а все ключевые вендоры предлагают SDN/NFV-решения. «Рынок поделен, и NFV/SDN не вызовет его „ломки“, как не вызвала нигде в мире», — согласен Павел Крылов, директор департамента предпродажной подготовки решений для опорных сетей компании Huawei. — Рынок поставщиков может меняться при совпадении моментов появления новой технологии улучшения пользовательского опыта (3G, 4G и т. п.) и нового поставщика (для 3G таким поставщиком была Huawei в 2008 году). В США с NFV такое случилось, когда себе заявили Mitel и Affirmed».

Василий Горшенин, руководитель направления сервисов для операторов связи компании КРОК, выделяет помимо исторически сильных вендоров (Ericsson, Nokia, Cisco, Huawei, ZTE и др.) также группу нишевых игроков: Quanta, Supermicro, Edge-Core (в оборудовании), Mirantis, Red Hat, Canonical, VMware (в виртуализации), Affirmed, Mavenir, Tango Telecom (в конечных функциях). Они не предлагают комплексных решений, а концентрируются на своих нишах и делают наиболее качественные продукты, не пытаясь играть на смежных рынках. Их преимуществами — инновационные продукты и более низкая стоимость решений.

Мария Попова

Wi-Fi в законе

Как выполнить нормативные акты о Wi-Fi и получить дополнительную выгоду

Спустя два года после принятия постановления правительства России о Wi-Fi в публичных местах Роскомнадзор начал активно проверять общественные места на внедрение идентификации пользователей бесплатного Wi-Fi. В новых условиях интернет-операторам стало сложнее выжить. Кто-то покинул рынок, а кто-то адаптировался в новых условиях и даже сумел найти новые возможности для бизнеса. О том, как бизнесу выполнить все обязательства, рассказала директор по маркетингу и продуктам бизнес-рынка МТС Елена Нечай.



— Как ужесточение правил отразилось на рынке операторских услуг?

— Действительно, закон взволновал многих. Кто-то адаптировался к изменениям. Малым операторам стало, наверное, сложнее. Появляются Wi-Fi-точки, которые необходимо довести до соответствия новым требованиям, но существующий провайдер к этому не готов. В таком случае оборудование можно и нужно использовать. МТС успешно работает в новом правовом поле с любимыми компаниями.

— Но бизнес в любом случае вынужден перестраивать сети и нести расходы?

— Рассмотрим вариант, при котором оборудование осталось. Кажется бы, организации придется строить новую инфраструктуру и делать дорогостоящий ремонт офиса из-за переустройства сети Wi-Fi. Мы внедрили специальную услугу «Wi-Fi для бизнеса», с которой таких проблем не будет — мы ставим точку доступа на уже имеющемся оборудовании или организуем только идентификацию пользователя, соблюдая все требования закона.

— В чем еще интерес бизнеса перестраивать сети, кроме исполнения нормативных актов?

— Парадоксально, но факт: Wi-Fi — это не только и не столько

затраты, сколько возможность для компаний заработать. Страница авторизации становится удобным носителем рекламы с абсолютным контактом с аудиторией. Не нужно тратить деньги на листовки с акциями и спецпредложениями — достаточно разместить новости в окне авторизации, в фирменном стиле вашей компании. Сделать это можно одновременно во всей сети заведений,

экономив время на обучении персонала.

— Где окажется информация о пользователях сети компании?

— Конечно, вся информация останется конфиденциальной и все данные обезличены. Но авторизация позволяет собирать и анализировать данные о количестве посетителей в зоне Wi-Fi: как часто заходят, сколько времени пользуются, какой трафик потребляют. Все это помогает определить, какие маркетинговые инструменты будут работать для посетителей Wi-Fi-зоны. Также можно управлять самой сетью: регулировать скорость и время доступа, число подключенных устройств и пр.

— Может ли получиться так, что некоторые организации останутся вообще без Wi-Fi? Ведь далеко не везде есть проводной интернет.

— Конечно, нет. Мы понимаем, что интернет нужен любому бизнесу

ОБЯЗАТЕЛЬНАЯ ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

Летом 2014 года постановление правительства России №758 от 31 июля 2014 года обязало идентифицировать пользователей публичных точек доступа к интернету через Wi-Fi по паспорту, позднее правила были смягчены: кроме паспорта, идентификатором может быть номер мобильного телефона или учетная запись на портале gosuslugi.ru.

как воздух. И готовы предоставить Wi-Fi с авторизацией даже на основе скоростных мобильных сетей, таких как сети LTE. А это значит, что где бы ни располагалось бизнес-пространство — в городе,

за городом, в здании, на крыше, в подвале или это подвижная точка Wi-Fi для мероприятий — мы легко поставим фиксированный или мобильный канал доступа в интернет.

ПРОВЕРКА РОСКОННАДЗОРА В СЕНТЯБРЕ 2016 ГОДА*

- 18 тысяч точек беспроводного доступа в интернет в публичных местах по всей России проверил Роскомнадзор.
- 5,5 тысячи точек доступа к интернету через Wi-Fi работает без идентификации личности пользователей.
- 2,5 тысячи незапароленных сетей Wi-Fi из них организованы физическими лицами.

*Данные Роскомнадзора, ссылка на офици.сайт: <https://rkn.gov.ru/news/rsoc/news40898.htm>.



РЕКЛАМА

ЭФФЕКТИВНО

Wi-Fi для бизнеса от МТС. Лидер легко поставит точку!

Ваш бизнес в центре или за городом? В здании или передвижном фургоне? На крыше или в подвале? Не имеет значения — мы установим сеть Wi-Fi!

 **МТС** corp.mts.ru

ПАО «МТС» является лидером корп. рынка по объему выручки и числу абонентов среди операторов моб. связи России, по данным исследования компании ООО «ТМТ Консалтинг», проведенного в марте 2016 г. (кроме Респ. Крым и г. Севастополь). Услуга «Wi-Fi для бизнеса» включает предоставление точек доступа по технологии Wi-Fi, подключение к сети интернет и идентификацию пользователей. Услуга действует на территории всей России, кроме Респ. Крым и г. Севастополь, при условии наличия технической возможности предоставления доступа к сети передачи данных. Подробнее на corp.mts.ru

информационные технологии

Постсноуденовская безопасность

Сегмент информационной безопасности — один из немногих оставшихся на ИТ-рынке, который продолжает показывать рост. Киберпреступность эволюционирует, вместе с ней приходится развивать и технологии защиты, менять подходы к информационной безопасности бизнеса, подстраиваться под новые угрозы и, главное, переходить от «бумажной» безопасности к реальным превентивным стратегиям защиты.

— сегмент рынка —

По оценкам Gartner, бизнес во всем мире потратил на информационную безопасность (ИБ) в 2015 году \$75 млрд, что на 4,7% больше, чем годом ранее. В то же время мировой ИТ-рынок снизился на 5,8%. В РФ ситуация выглядит похоже, если учесть разницу в объемах и курсах валют. На фоне падения всего рынка информационно-коммуникационных технологий (ИКТ) сектор информационной безопасности можно назвать одним из самых перспективных. В марте аналитики IDC пересмотрели прогноз на 2016 год по рынку ИКТ в целом, заявив, что его падение составит порядка 13%, тогда как ранее ожидалось незначительное сокращение его объемов. На прошедшей в сентябре конференции по информационной безопасности IDC IT Security Roadshow 2016 старший аналитик IDC по направлению ИБ Денис Масленников сообщил, что в первом полугодии 2016 года рынок аппаратных решений для обеспечения ИБ вырос в долларах на 26,8% по сравнению с первым полугодием 2015 года и составил \$68 млн. По его мнению, положительная тенденция сохранится. «Первая половина 2016 года показала, что спрос на решения для обеспечения информационной безопасности снова растет, ведь защита критически важных данных является крайне важной для большинства компаний любого размера», — отметил Денис Масленников.

Евгений Дружинин, ведущий эксперт направления ИБ компании КРОК, описывает международный контекст: «Российский рынок ИБ показывает довольно стабильный рост в рублях, но, к сожалению, в пересчете на доллары динамика пока отрицательная. Виной тому нынешний курс валют, который повлиял на всю отечественную отрасль ИТ. Тем не менее на локальном рынке все довольно позитивно — например, по итогам 2015 года выручка по направлению информационной безопасности КРОК выросла почти на 20% в рублях».

Андрей Янкин, руководитель отдела консалтинга Центра информационной безопасности компании «Инфосистемы Джет», говорит, что в целом тенденции на рынке ИБ в России те же, что и на мировом, хотя и существует задержка в один-два года, но она уменьшилась: раньше мы отставали на четыре-пять лет. По его словам, общие для всего мира проблемы — целенаправленные атаки, защита веб-ресурсов, в том числе от DDoS-атак. «В России можно выделить также тен-

денции замены систем ИБ в рамках импортозамещения, но их уже нельзя считать уникальными, так как в постсноуденовскую эпоху многие государства задумались об этом», — добавляет господин Янкин. Кирилл Керценбаум также видит рост интереса к отечественным решениям в сфере ИБ на волне импортозамещения. Регулятор продолжает воздействовать на рынок ИТ и через него на сегмент ИБ также путем обновления российского законодательства. Так, «закон Яровой» может повлиять на рынок строительства новых дата-центров, объем поставок систем хранения данных и другого оборудования, а также повлечь рост спроса на решения в области сетевой безопасности, включая межсетевые экраны, анти-DDoS системы и пр.

Как говорит Дмитрий Огородников, директор Центра компетенций по информационной безопасности компании «Техносерв», именно в сильном регулировании заключается принципиальное отличие российского рынка от общемирового. «Технологически это выражается в использовании некоторых уникальных решений, как то средств АПМДЗ (аппаратный модуль доверенной загрузки), «Б» или отечественных криптоалгоритмов ГОСТ 28147-89 и последующего ГОСТ Р 34.12-2015. Законодательно это выражается в большом объеме различных руководящих документов в области защиты информации, которые по последним планам Федеральной службы по техническому и экспортному контролю (ФСТЭК) должны обновляться каждые три-четыре года», — объясняет он. «С другой стороны, наш рынок ИБ менее зрелый и многие процессы или технологии, которые на западном рынке уже широко используются, на нашем только делают первые шаги. Например, в этом году мы стали активно говорить о подходе Agile, о процессах ИБ и о решениях класса User and Entities Behavior Analysis (технологии анализа поведения пользователей и процессов в корпоративных системах на основе искусственного интеллекта), «Б»».

«Бумажная» безопасность подорожала

Еще одна из отличительных особенностей российского рынка ИБ, по словам господина Дружинина, — существенный рост средней стоимости ущерба от инцидентов. Так, в 2015 году по данным IDC она выросла почти в полтора раза, в то время как на мировой арене этот показатель уменьшился на 5%. Это заставляет бизнес более тщательно рабо-

довать над стратегиями защиты, привлекать внешних специалистов. Соответственно, серьезный рост показывает сектор услуг в области ИБ. Господин Янкин комментирует: «Если с «железом» у нас все более или менее неплохо, то в области выстраивания процессов ИБ и встраивания их в бизнес наблюдается явное отставание. Консалтинг в области ИБ в коммерческом секторе показывает хороший рост, но во многом это эффект низкой базы. Интересная тенденция на рынке ИБ, к которой скептически относились многие эксперты еще три-четыре года назад, — это существенный рост рынка аутсорсинга, как качественный, так и количественный. В целом рынок ИБ в России бурно развивается даже в условиях экономического спада».

Евгений Дружинин также видит тенденцию по смещению акцентов в сторону услуг, включая аутсорсинг ИБ и облачные сервисы типа Security as a Service (SEaaS). «Заказчики все активнее ищут помощи внешних подрядчиков в вопросах выстраивания контура безопасности. Например, спрос на облачные сервисы растет, а вместе с этим формализуются и требования к их безопасности. Например, услугу Security as a Service крайне желательно выстраивать на базе сертифицированных ФСТЭК и ФСБ средств. Как раз таким сервисом мы сейчас защищаем ряд IaaS-сервисов, арендуемых в нашем публичном облаке автомобильной компанией. Защита реализуется в соответствии с индивидуальной моделью выстраивания и с учетом требований 152-ФЗ», — говорит он.

Из-за того, что последствия киберугроз становятся все более разрушительными, бизнес стал более внимательно относиться к защите. Господин Янкин говорит, что от формального выполнения требований регуляторов и отношения к ИБ как к некоторой экзотике бизнес перешел к восприятию рисков ИБ как к будничной и неотъемлемой части использования ИТ-технологий. «Конечно, в этой области все еще сохраняется правило о том, что пока гром не грянет, мужик не перекрестится, но гром стал греметь так часто и так у многих над головами, что большинство зрелых компаний перешли к плановому обеспечению ИБ, а не латанию дыр после инцидентов. Это приводит к росту роли ИБ в компаниях, выведение подразделений ИБ из-под ИТ или СБ в отдельные независимые структуры с мощными контрольными функциями, собственными бюджетами, дифференциацией персонала», — говорит он.

Кирилл Керценбаум, менеджер по развитию бизнеса «Лаборатории Касперского», добавляет, что в связи с сокращением или оптимизацией бюджетов на ИБ российские компании стали уделять внимание более интенсивному использованию уже внедренных средств защиты, а не массовой закупке новых. В связи с этим и наблюдается рост спроса на сервисы Security & Threat Intelligence (интеллектуальные услуги по предотвращению угроз), которые позволяют повысить эффективность процессов ИБ за счет более качественной организации процессов мониторинга защищенности инфраструктуры. А также растет спрос на аудит безопасности, тесты на проникновение, данные по актуальным угрозам и услуги SEaaS, которые позволяют оптимизировать расходы на ИБ за счет аутсорсинга крупных инфраструктурных решений на сторону сервис-провайдера. Из этой категории услуги по защите от DDoS-атак — антивирусные решения по подписке, защита от влома и т. д.

Михал Салат, ведущий вирусный аналитик Avast Software, добавляет: «Простого антивируса уже недостаточно для обеспечения корпоративной информационной безопасности, нужно использовать несколько уровней защиты, включая антивирус, межсетевой экран, системы обнаружения влозов, регулярное обновление аппаратного и программного обеспечения и надлежащее использование прав доступа сотрудниками. Важно помнить про человеческий фактор. Люди совершают ошибки, и хакеры знают, как их использовать. Поэтому важно, что организации осуществляют новую политику, например устанавливая ограничения на использование документов внутри компании для предотвращения фишинговых атак. Тестовые влозы — это отличный способ узнать слабые места, которые хакеры потенциально могут использовать. Тестирования на проникновение в идеале нужно делать несколько раз в год, так как хакеры постоянно ищут и находят новые способы влома».

Бизнес реагирует на нарастающие угрозы — с существенным отставанием от развитых стран в России появился интерес к системам автоматического предотвращения мошенничества в ИТ-системах. Как говорят эксперты, сейчас в этой области настоящих бум.

Антон Карданов, руководитель сектора ИБ компании AT Consulting, говорит, что целью злоумышленников сегодня часто являются веб-приложения, которые обладают достаточным количеством уязвимостей, позволяющих реализовать такие атаки, как межсайтовый скриптинг (XSS), SQL-инъекции, уязвимости конкретных плагинов. Господин Карданов рекомендует: «Чтобы минимизировать ущерб бизнеса при построении превентивной системы информационной безопасности, развивающейся параллельно с инфраструктурой и технологиями, необходимо за-

ранее быть готовым к предотвращению наиболее вероятных атак и уходить от убежденности, что какой-то конкретный ресурс полностью защищен. Создайте центр мониторинга и реагирования на инциденты информационной безопасности: подразделения, имеющие возможность в режиме реального времени отслеживать защищенность ресурсов и принимать адекватные и соответствующие текущей ситуации меры. Проведите инструментальный аудит практической защищенности ресурсов, он выявит наиболее уязвимые места и сформирует предположение о вероятных атаках. Таким образом, у вас будет заранее спланированный план действий, следуя которому вы сможете быстро восстановить работоспособность системы в случае влома».

Андрей Бершадский, директор центра компетенции компании Positive Technologies, также подтверждает, что безопасность приложений — одна из главных проблем заказчиков в РФ в текущем году. За год продажи продукта Web Application Firewall компании в России дали вырвочку, которая вдвое превышает продажи экранов прикладного уровня за все предыдущие годы.

Также он отмечает, что за последний год стало активнее происходить строительство центров мониторинга и управления информационной безопасностью (SOC). «Именно центры мониторинга начали мирить два противоборствующих лагеря: так называемых бумажных безопасников и ИБ-практиков. Ведь SOC — это люди, регламенты и технические средства. И без правильно выстроенных процессов реализовать практическую составляющую мониторинга и реагирования вряд ли представится возможным. Интерес к SOC подтолкнул интерес к SIEM-решениям (Security information and event management — управление информационной безопасностью и событиями ИБ, «Б»). Многие сильно удивились, что, оказывается, однажды купленный и даже внедренный SIEM на практике не всегда способен решать те задачи, которые стоят перед специалистами SOC. В первую очередь ввиду неспособности оперативно подстраиваться под динамичную инфраструктуру и отсутствия серьезной встроеной экспертизы. Рынок SIEM в России фактически переживает вторую молодость, и вряд ли стоит ожидать его спада, ведь потребности заказчиков давно уже выходят за рамки классического решения SIEM», — рассказывает он.

В сфере защиты государственных учреждений господин Бершадский видит прогресс: «Сразу несколько ведомств начали создание первых центров ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, «Б»), что должно крайне положительно сказаться на безопасности государственных учреждений и подтолкнет других участников рынка присоединиться к программе».

Мария Анастасьева

«Работаем над тем, чтобы изменить восприятие ИБ в сознании людей»

— отраслевой опыт —

Сеть магазинов бытовой техники, электроники и товаров для дома «Эльдорадо» активно развивает бизнес в интернете. Это сопряжено с рисками для информационной безопасности (ИБ). ФЕДОР КУРНОСОВ, менеджер по ИБ «Эльдорадо», рассказывает, как формируется стратегия компании в этой сфере.

— Часто компании начинают думать о том, что нужно использовать какие-то средства защиты, только в тот момент, когда проблема уже возникла. Как у вас это происходит?

— Стараемся рассматривать возможные проблемы ИБ превентивно: когда интернет-магазин был в самом начале развития и в это развитие вкладывались серьезные средства, необходимо было позаботиться о защите инвестиций. Мы хотели быть уверены, что интернет-магазин будет доступен 24 часа в сутки 7 дней в неделю. В этом нам помогает то, что мы приверженцы рискованной модели: просчитываем риски в деньгах и именно эти цифры доносим до менеджмента компании, когда закладываем бюджет на ИБ. Руководство понимает язык денег. Если дать им возможность взвесить на одной чаше весов потенциальные потери от реализованной угрозы, а на второй — стоимость защиты, то возникает отчетливое понимание оправданности этих вложений.

— Насколько важен интернет-магазин для бизнеса компании?

— Трафик на сайте постоянно растет. Мы делаем ставку на онлайн, потому что все меньше людей готово идти в магазин и что-то там покупать. Особенно это касается крупных городов, жители которых хотят получать все, не вставая с дивана. Интернет-магазин, по сути, — это «лицо» компании, которое должно быть аккуратным и дружелюбным.

Офлайн-магазины также перестраиваются. Мы не считаем, что они полностью умрут. Меняется формат, люди приходят туда уже больше для развлечения, чтобы изучить какие-то новинки. Им интересна уже не только техника, но и другие категории товаров.



— Какой комплекс мер вы используете для обеспечения доступности?

— Обеспечивая доступность, решаем две задачи: отказоустойчивость и катастрофоустойчивость. Для решения первой используются средства распределения нагрузки внутри ЦОД (центр обработки данных). Для решения второй в зависимости от стратегии обеспечения катастрофоустойчивости дублируем бизнес-процессы и поддерживающую их ИТ-инфраструктуру в двух географически распределенных ЦОДах.

— Какие угрозы вы учитываете?

— Учитываем как внешние, так и внутренние угрозы. Для защиты от DDoS-атак используем внешний облачный сервис. Проводим регулярный анализ имеющихся уязвимостей, которые могут эксплуатироваться злоумышленниками как извне, так и изнутри. В частности, осуществляем аудит на нарушение бизнес-логики — это когда атаку можно устроить, используя стандартный функционал, в котором не все риски учтены.

— Многие компании, как правило, испытывают сложности с тем, чтобы пересчитать риски в возможные денежные потери. С доступностью понятно: можно вычислить оборот интернет-магазина за определенный период. А как обращаться с другими рисками? — Думаю, сложности возникают у специалистов, которые еще не поняли, как построить разговор с биз-

несом, как объяснить менеджменту, что такое доступность, конфиденциальность, целостность и почему это важно. Потери от проблем с доступностью ресурса действительно весьма просто оценить в деньгах: либо бизнес работает, либо нет.

Но как оценить потери от нарушения конфиденциальности? Со временем пришло понимание и по этому вопросу. Наш отдел маркетинга заранее просчитывает ожидаемый эффект от акции: насколько она будет выгодна, сколько денег принесет. Если конфиденциальность нарушена, о планах узнал широкий круг лиц (включая конкурентов), акция уже не принесет ожидаемых доходов. Разница между запланированным объемом выручки по акции и тем, что получилось по факту из-за нарушения конфиденциальности, — это и есть риск, выраженный в деньгах.

Этот же принцип мы пытаемся перенести и на другие отделы: просчитываем, как может повлиять разглашение определенной информации на взаимодействие с вендорами, партнерами, поставщиками. По многим подразделениям у нас уже есть ясная картина.

С целостностью тоже научились работать. Есть понимание, что определенные данные не должны измениться, пока они проходят через бизнес-процессы. Можем посчитать, сколько компания потеряет, если это случится. К примеру, потери из-за ошибки в цене мы можем вычислить практически моментально: видим, сколько людей успели сделать предзаказ по меньшей стоимости или купить этот товар. Собираем информацию о таких инцидентах и можем оценить в итоге средние потери.

— То есть вы изучаете исторические данные по конкретным инцидентам? — Да, мы берем реальную историю инцидентов и рассчитываем вероятность наступления тех или иных потерь на основе этих статистических данных. Плюс к этому считаем потерю от каждого подобного случая и, как следствие, получаем риск, рассчитанный в деньгах. С помощью этих данных мы ведем диалог с бизнесом. Менеджеру понятны те категории потерь и рисков, с которыми он сталкивается каждый день: во

сколько обойдется час простоя, какими будут потери от срыва маркетинговой акции и т. д.

— Как вы относитесь к облакам?

— «Эльдорадо» — продвинутая компания: мы используем все продукты SAP для ритейла, при этом размещаем их на облачных ресурсах. Конечно, это выделенные именно под нас облачные ресурсы — так называемое частное облако, размещенное на оборудовании подрядчика. За чем? Нам важно, чтобы высоконагруженные системы были обеспечены поддержкой 24/7. Не всегда это можно сделать собственными силами. В этом смысле контракт с поставщиком облачных ресурсов — удобный вариант.

— Учитываете ли риски, связанные с использованием облаков при формировании стратегии ИБ?

— У нас разработана большая карта всевозможных рисков, включая те, что связаны с законодательством. В нее включены в том числе риски, связанные с облачными ресурсами. Каждый год мы проводим актуализацию этой карты, которая ориентирована на бизнес-цели компании. Мы следуем стандарту ISO 27001 от 2013 года, в котором есть целый раздел о том, что нужно рассматривать риски в соответствии с видением общего развития компании. Так что мы смотрим на то, в каком направлении развивается бизнес, включаем в карту новые риски, которые являются актуальными для этого направления развития.

— Чтобы все эти риски просчитать, вам необходима собственная статистика по инцидентам?

— Если появляется новая угроза, мы сразу ее учитываем, присваиваем определенную вероятность ее реализации и применяем превентивные меры защиты. Если инцидентов в течение года не происходит, выводим эту угрозу из актуальных. При этом мы стараемся использовать имеющиеся средства защиты, если же они не позволяют предотвратить реализацию новой угрозы, то, как я говорил ранее, взвешиваем на одной чаше весов потенциальные потери от реализации угрозы, а на второй — стоимость защиты. Так можем быть постоянно в тренде.

— Какие угрозы становятся более актуальными?

— Основной тип угроз, который сейчас активно обсуждается, — это таргетированные, направленные атаки (APT — advanced persistent threats). Общей тренд такой, что защита должна становиться более эшелонированной. То есть должны быть стандартный антивирус, инструменты противодействия DDoS-атакам, Web Application Firewall от влома, средства против внутренних атак. И, конечно же, многое очень зависит от обучения людей.

В последнее время вижу очень много всяких средств защиты, которые помогают от того или иного вида угроз. Но их эффективность будет низкой, если не ликвидировать пробелы в обучении людей.

Моя личная рекомендация коллегам — в первую очередь заниматься этим вопросом. «Железо» и ПО, которые много чего умеют, на рынке полно. Но людей, которые находятся внутри периметра либо с ноутбуком перемещаются за пределы компании, нужно обязательно учить информационной безопасности, тому, как противостоять определенным угрозам. Технологии усложнились, компании используют целые арсеналы средств защиты, но вопросам социальной инженерии уделяют крайне мало внимания.

Допустим, компания использует систему защиты от таргетированных атак. И трафик просматривает, и компьютеры, а также каждый запущенный сервис мониторит. Вроде бы все хорошо. Но вот пользователь решил поработать дома, берет с собой документы на флешке, приносит обратно в офис. Воткнул ее в рабочий компьютер, всего лишь считал информацию и заразил машину. Да, проблема будет обнаружена, но до того может произойти заражение сети, да все что угодно.

— Вы проводите обучение в компании?

— У нас постоянно идут образовательные программы. При приеме на работу новый сотрудник проходит первичное обучение, затем всех приглашаем на дистанционные курсы. Мы создали пять-шесть видов образовательных дистанционных программ по информационной безопасности, по ним нужно сдавать зачет.

Это дает большой положительный эффект. Да, все еще бывают проблемы, когда люди не действуют в соответствии с тем, что они прочитали. Но некоторые инциденты были предотвращены именно потому, что человек вспомнил, что было написано в обучающих материалах, сделал все, как нужно, чтобы проблему предотвратить. В итоге не произошло массового заражения компьютеров.

Помимо обучения важно показывать людям, что требования информационной безопасности — это не палка в колеса, что бизнес и ИБ могут сосуществовать. Да, какие-то процессы могут стать чуть медленнее, потому что все-таки средства защиты нужно использовать. Да, это может как-то ограничивать бизнес. Но эти ограничения приносят дополнительную выгоду из-за того, что снижают риски. Иначе говоря, мы поручиваемся лицом к бизнесу, бизнесом лицом — к нам и происходит взаимодействие. Мы работаем над тем, чтобы изменить восприятие ИБ в сознании людей.

Много слов сказано о том, что ИБ должна быть частью корпоративной культуры. Но я все-таки исхожу из того, чтобы инструмент, который предлагается для обеспечения информационной безопасности, был удобным. Если это удобно, то не возникает мысли, как-то это ограничение обойти. Всегда есть альтернатива публичным слабозащищенным сервисам типа Dropbox и пр. Можно развернуть удобные сервисы внутри защищенного периметра, если их функциональность нужна бизнесу.

Конечно, чтобы получилось людей склонить к альтернативе, нужны сильная воля и возможности руководителя по ИБ, а также поддержка от генерального директора, чтобы не произошло первичного отторжения. Если первичное отторжение у людей удается преодолеть, то обычно они начинают сотрудничать. Ну и, конечно, специалистам по ИБ нужно не бояться влезать в процессы, пытаться почувствовать, чем живет компания. Разумеется, не сразу, но обязательно получится добиться эффективного взаимодействия на всех уровнях.

Интервью взяла Светлана Рагимова

информационные технологии

Плата за дату

Благодаря развитию технологий у интернет-пользователей появляется возможность контролировать передачу своих персональных данных заинтересованным компаниям. Этому способствуют и изменения в законодательстве разных стран. На этой волне зарождается новый рынок сервисов, которые предлагают пользователям монетизировать свои данные.

— **стартап** —

Алексей Ермаков, создатель сервиса Sberdatabank, уверен, что пришла пора ни много ни мало менять мир: пользователи должны сами решать, хотят ли они делиться своими персональными данными с рекламодателями и прочими компаниями. И если соглашаются на это, имеют право требовать денежную компенсацию. «Интернет-компании говорят, что забота о пользователях является для них приоритетом — она проявляется в показе им наиболее подходящей рекламы, но при этом компании не дают пользователям возможности выбрать, хотят ли они вообще видеть ту или иную рекламу. Людей просто используют», — объясняет Алексей Ермаков. По его мнению, блокировщики рекламы — предвестники смены технологического уклада. «Они растут быстрее социальных сетей, это целая индустрия. Интернет-гиганты в своих финансовых отчетах прямо заявляют, что подобные технологии являются критически опасными для их бизнеса в плане получения доходов. К тому же крупнейший блокировщик рекламы Adblock Plus недавно сам объявил о старте продаж рекламы в своей сети. То есть блокировщики довольно быстро прошли путь от гуманитарных сервисов в сторону коммерческих проектов», — говорит основатель Sberdatabank. Он ссылается на статистику исследовательской компании PageFair: потери мировой выручки из-за блокировки рекламы в 2015 году составили \$21,8 млрд, а в 2016 году рекламодатели могут недосчитаться уже \$41,4 млрд.

В мире появляются все больше сервисов, подобных Sberdatabank, которые предлагают пользователям монетизировать собственные данные, используя различные бизнес-модели. Этот стартап, основанный выходцем из МТС, работает как блокировщик рекламы, но не убирает ее, а заменяет баннерами, которые разместили рекламодатели через Sberdatabank. Для рекламодателя ценность в том, что он получает доступ к точно таргетированной аудитории. С пользователями компания делится прибылью: делает ежемесячные отчисления, причем сумма их зависит от того, как много личной информации о себе готов раскрыть пользователь.

Господин Ермаков считает, что борется за справедливость: «Современный пользователь обрабатывается со всех сторон: сайтами, государством, банками, операторами связи и так далее. Информация о нем — ценный товар, поскольку позволяет продавать рекламу,

которая является де-факто валютой интернета. Но человек, являясь исключительным владельцем своих данных, лишен возможности управлять тем, как и какая информация о нем обрабатывается другими компаниями для получения выгоды в их интересах. Сервисы типа Sberdatabank позволяют исправить ситуацию». По мнению Билла Франка, директора по аналитике компании «Терадата», увеличение контроля пользователей над собственными данными — отличная мысль. «Компании используют данные людей по своему усмотрению. Меня несколько беспокоит, что моя информация доступна кому-то извне. Стал бы я сам разрешать отслеживать геопозицию, если бы мне, скажем, платили за это \$10 тыс. в год? Не думаю. Но это вопрос ценности данных. Уверен, что есть много людей, которые бы согласились на это», — говорит Билл Франк. Аналитик уверен, что такие сервисы, как Sberdatabank, заставят компании более вдумчиво относиться к тому, что они делают с данными пользователей, как их анализируют и для чего. Ведь сейчас данные практически ничего не стоят, а если бы пришлось за них платить их владельцам, это сделало бы подобную практику более осознанной, а компании стали бы использовать более продвинутую аналитику. Он напоминает, что практика оплаты за наблюдение за предпочтениями аудитории давно применяется на телевидении. Людям, которые согласны участвовать в исследованиях, устанавливая специальное оборудование, отслеживающее все, что человек смотрит на ТВ. Так, например, работает TNS, анализирующая аудиторию ТВ-каналов. В интернете есть также системы сбора данных через анкетирование, которые платят участникам за каждый опрос. Логично было бы интернет-корпорациям платить своим пользователям за использование их данных.

«Шаг навстречу пользователю — верное решение, но образованных и грамотных людей крайне мало, — считает Геннадий Нагорнов, сооснователь и управляющий директор компании Auditotius. — В большинстве своем пользователи не разбираются в специфике современной коммуникации и не понимают, что есть данные и как они могут быть использованы. В частности, в России до сих пор не ввели обязательное информирование аудитории, что сайты и сервисы собирают данные (cookie-файлы). На Западе это контролируется на законодательном уровне».

Но господин Нагорнов сомневается, что бизнес-модель, выбранная Sberdatabank, мо-

жет быть успешной: «Мы занимаемся этим бизнесом уже четыре года, и культура оплаты использования данных в России на крайне низком уровне. Рекламодатели и агентства не хотят платить за данные вменяемые суммы. В большинстве своем хотят получать их бесплатно. Почему? Потому что привыкли к единой цене за размещение, без разделения на статьи — за показ и за данные. К тому же общий тренд идет на снижение стоимости размещения в интернете. Только селлеры с государственным участием могут успешно поднимать цены». Бизнес-модель Sberdatabank построена на том, что пользователь получает процент от бюджета рекламодателя. Но в ценообразование, по мнению господина Нагорнова, должны быть заложены и стоимость показа, и стоимость данных, и стоимость технологии, и маржа проекта. «Еще одним важным аспектом является объем доступной аудитории. Рекламодателям не интересно таргетироваться на маленькие сегменты — это не дает эффекта. Нужна большая аудитория. Это замкнутый круг. Если пользователи не будут получать достаточное количество денег, они не будут использовать приложение. Если они не будут его использовать, сегменты будут маленькие, и это не будет интересно рекламодателям. Также не понятно, что с эффективностью. Тут две составляющие: первый аспект — перформанс, оплата за результат. По нашему опыту данные чаще не влияют на перформанс. Второй аспект — это точность контакта. Это важно для крупных рекламодателей, но они доверяют площадкам только в том случае, если есть внешний верификатор и измеритель (например, TNS). В общем идея отличная, но должны сойтись все звезды, чтобы она взлетела».

Любая информация, которая может рассказать о пользователе больше (история его покупок, платежеспособность, его перемещения), по мнению Михаила Берлизева, генерального директора Data-Centric Alliance, давно уже превратилась в товар. «У нас в России торговля пользовательскими данными пока распространена не столь широко, однако все больше отечественных компаний выражают желание выходить на этот рынок. Некоторые социальные сети и сервисы уже сейчас поощряют активность пользователей внутри своей валюты. На Западе это нормальная практика. При этом любой гражданин имеет право знать, для каких целей собираются, обрабатываются и используются

его данные. Чем менее очевидна пользователю выгода передачи данных, тем дороже или менее охотно он захочет их отдать или продать», — комментирует он.

Роман Нестер, основатель рекламной платформы Segmento, контрольный пакет которой принадлежит Сбербанку, считает, что, если пережить с регулировкой доступа компаний к информации о своих пользователях, множество бесплатных сейс сервисов закроются либо перейдут на платную модель, а их услуги станут в разы хуже. «Пользователи, не желающие делиться данными, начинают использовать Тог-сети. Вы можете сами посмотреть, на что похожа реклама на сервисах „ушедших“ в эту зону сети. Почти все они теперь отказываются от рекламной модели: без таргетинга (кроме площадки, где она размещена) реклама становится в разы менее эффективной и ненужной рекламодателям», — рассуждает господин Нестер.

Александр Кабаков, сооснователь компании N-Tech.Lab, разработавшей технологию распознавания лиц, уверен, что в отрыве от продукта сами по себе персональные данные не представляют никакой ценности. «Пользователь не способен генерировать полезную „дату“, она становится таковой только благодаря технологиям и глубокой аналитике. Пользовательские данные собираются в том числе в интересах самих пользователей, потому что они позволяют компаниям подстраивать свои сервисы под конкретных людей. Поэтому в этом заинтересованы обе стороны. И даже когда речь идет о таких квазиперсональных данных, как лицо человека, то и здесь в ближайшем будущем общество придет к пониманию, что глобальное распознавание лиц идет на пользу. В частности, потому, что использование таких технологий значительно повышает безопасность самих людей. Когда появилась Facebook, были те же разговоры о нарушении приватности. Сейчас про эти разговоры все забыли. Прогресс не остановить, и прогресс же будет менять сознание людей, в том числе в понимании, что такое приватность, личное пространство», — уверен господин Кабаков.

История развивается по спирали, и сегодняшний всплеск общественного внимания к контролю над собственными данными и блокировке рекламы — это всего лишь очередной виток развития истории, старой, как сам интернет. В этом уверен Михаил Балакин, и. о. генерального директора международной рекламной сети CityAds. «Предыдущие всплески привели к появлению контроля над своей историей поиска, режима инкогнито в браузерах, возможности отключать непонравившиеся баннеры, самоуничтожающихся сообщений в мессенджерах и раздражающих окошек с уведомлениями „дан-

ный сайт использует куки“. Но рекламный рынок только вырос и продолжает расти, а реклама как была, так и осталась доминирующей моделью монетизации. На мой взгляд, очередной виток, как и предыдущие, не приведет ни к какому радикальному изменению бизнес-моделей. Пользователи отвоюют чуть больше контроля над своим следом в интернете, законодатели примут очередной запрещающий закон, а инструменты рекламного таргетинга станут еще изощреннее и точнее», — прогнозирует господин Балакин.

«Пока на российском рынке данных законодательное регулирование где-то более жесткое, где-то более формальное, — замечает Михаил Берлизев. — После подписания „пакета Яровой“ пользователи стали еще более чутко относиться к сохранности своих данных. По большей части общественность еще не до конца понимает, как на самом деле работает рынок данных, и относится к этой теме с опаской. Рынок данных остается до конца неурегулированным, в том числе на законодательном уровне, но, несмотря на это, продолжает набирать обороты».

По мнению господина Балакина, ажиотаж вокруг контроля над собственными данными базируется на наивном заблуждении рядового пользователя, что коварные глобальные интернет-корпорации собирают информацию и анализируют его переписку, чтобы потом контролировать и вторгаться в его личную жизнь. «На деле же бездушным интернет-гигантам нет никакого дела до ваших личных тайн: поете ли вы дома „Марсельезу“ нагишом или имеете интрижку на стороне. За такие секреты рекламодатели не платят. Все что их интересует — это поймать вас в тот момент, когда вы задумались о покупке новых ботинок или присматриваете новый автомобиль. И показать вам рекламу максимально полезную и релевантную моменту. В этом случае выигрывает в том числе и пользователь», — уверен он.

«Проект, позволяющий пользователю зарабатывать на своих данных, забывает, зачем этот пользователь идет в сеть, — добавляет Роман Нестер. — Пользователь идет на сайты и ресурсы, которые создали другие компании — Google, Facebook, крупные издательские дома. За прекрасную почту, отличные социальные сети, качественные новости люди не платят напрямую: они платят косвенно, позволяя этим компаниям зарабатывать на рекламе. Попытка „трубы с трафиком“ встраиваться в эту цепочку очень наивна и противоречит логике бизнеса. В истории уже были, например, провайдеры, которые пытались вставлять рекламу „на пути“ к странице, но в итоге после судебного процесса эти провайдеры были закрыты».

Алексей Упатов

«Новая оргструктура стала фундаментом для дальнейших изменений»

— **цифровая трансформация** —

С13 Мы обозначили конкретный день, и каждый месяц именно в этот день сотрудники уже знают, что будет обновление, заранее готовятся, выделяют на это время. Им не приходится в панике перестраивать расписание, когда внезапно из IT-отдела выкатывается новый релиз. Это создает доверие к тому, что делает IT-департамент, а также позволяет вписать необходимые изменения в план этих регулярных релизов. Все происходит плавно и понятно. Так и складывается нормальное взаимодействие бизнеса и ИТ. — **Обычно такие преобразования требуют перестройки оргструктуры. Производили какие-то кадровые изменения?** — Было довольно много разных изменений — кадровых и организационных. С коллегой, который курирует операционный блок и проектные офисы, мы начали с перестройки процесса управления спросом. Стремился к тому, чтобы на все запросы в один конкретный проектный офис, на каждое бизнес-направление был выделен отдельный менеджер. Чтобы этот человек был в курсе всего, что там происходит.

Также системная архитектура претерпела множество изменений, пока мы не нашли подходящих enterprise-архитекторов, способных не только «хрустальные замки» рисовать, но и хорошо понимать бизнес, его потребности в новых технологиях на перспективу.

Произошла серьезная трансформация внутри IT-службы: мы построили продуктово-функциональную матрицу. Идея очень простая: стали группировать специалистов по функциональным доменам. То есть разработчики — в одном, сетевые архитекторы — в другом и т. д. Так они могут обмениваться опытом, помогать друг другу развиваться, вырабатывать внутрикорпоративные стандарты. При этом каждый понимает, что является также частью команды по какому-то конкретному продукту. Получается похоже на матричную структуру, но это не жесткая матрица. Это было очень непростое для IT-департамента изменение, потому что все привыкли к тому, что есть один внутренний заказчик и вот на него сотрудник работает. А здесь нуж-

но было понять, как меняется роль конкретного сотрудника и почему теперь у него два босса. На то, чтобы перейти на новый режим работы, прояснить все моменты, привыкнуть, ушло полгода. Примерно летом прошлого года этот процесс был по большей части завершен, и эти изменения стали давать свои плоды. Стало возможным планировать следующие шаги, будь то маленькие подзадачи внутри релизов или более длинные проекты.

Новая оргструктура стала фундаментом для дальнейших изменений. На ее основе уже можно осваивать принципы agile, стремиться больше работать головой, меньше — руками, сокращать time-to-market и т. д.

— **Какие позитивные результаты эта перестройка дала бизнесу?**

— Команда стала выпускать регулярные релизы, работа наладилась, появилось доверие к тому, что можем попробовать что-то более масштабное. В конце прошлого года начали обсуждать с коллегами из департамента корпоративного бизнеса, как изменить акценты восприятия банка на рынке. Хотим вернуть динамику, может быть даже стартаперский дух, искру, которые были свойственны организации на первом этапе развития бизнеса в РФ. В этом контексте решили пойти на довольно смелые шаги. Долгое время упорно работали над системой ДБО (дистанционного банковского обслуживания), последний год активно перерабатывали всю внутреннюю часть: процессы, платформы, форму системы. Сделали ее такой, чтобы дальше можно было активно развивать. В частности, открыли стандартизированные интерфейсы для партнеров. Это важный шаг, демонстрирующий миру, насколько сильно мы меняемся.

Мы переделали схему взаимодействия розничного интернет-банка с другими системами, разделили бизнес-логику и создали слой, через который можем взаимодействовать с внешними компаниями без ущерба для информационной безопасности. — **Какого рода партнерство возможно?**

— В теории это может быть любой стартап, который строит бизнес в области финтех. Например, у компании есть идея, как более эффективно организовать платежи или кредитный андеррайтинг. Может быть,

она нашла способ, как более активно привлекать клиентов, более эффективно открывать счета и т. д.

Речь идет о любых сервисах, которые можно делать на основе нашего интернет-банка. Мы предоставляем доступ к своей системе в виде некой «песочницы», чтобы в ней можно было поэкспериментировать.

— **Где вы ищете стартапы?**

— Мы обнаружили, что в России очень активное стартаперское движение. Конечно, это еще молодая сфера: ей всего около десяти лет. Но это уже не «первобытный бульон», уже есть если не «киты», то вполне зрелые «рыбы». Буквально пару месяцев назад мы в сотрудничестве со «Сколково», РВК и ФРИИ начали программу поддержки стартапов. Посмотрели, наверное, около сотни проектов, с парой десятков активно поработали. Предложили нескольким командам доступ к данным о наших клиентах (конечно же — обезличенным), чтобы на их основе создать за два-три месяца MVP (Minimum Viable Product), проверить гипотезу. Если она рабочая, идея может приносить прибыль, можно идти на следующий шаг.

— **С какими проектами к вам приходят? Наверняка с теми, что связаны с анализом больших данных.**

— У нас есть три проекта по этой теме, они связаны с платежами и аналитикой. Такие технологии используются также, например, в казначействе для анализа данных о торгах на валютной бирже. Но не для высокочастотной торговли, а для построения стратегии. Этот проект был реализован с нашей помощью. Занимались им около одного-двух лет, строили модели на архивных данных, весной начали применять на реальных. В розничном бизнесе в основном применяется эта технология для поиска корреляций и сегментации клиентов и антифрода.

— **Как финансово организована схема взаимодействия со стартапами?**

— Мы не являемся инвесторами, мы предоставляем данные и доступ к банковским сервисам, выделяем небольшой грант. Я не исключаю возможности того, что банк может стать инвестором проекта, если мы увидим, что идея хорошо работает, что в ней есть долгосрочный потенциал.

РЕКЛАМА



AT Consulting

КРУПНЕЙШИЙ ПОСТАВЩИК УСЛУГ
в сфере информационных технологий

15 лет на рынке



15 МЕНЯЮЩИЕ РЕАЛЬНОСТЬ

Доверие. Энергия. Экспертиза.

www.at-consulting.ru

информационные технологии

Зерно течет по проводам

В интернет вещей играют сегодня все: поставщики оборудования, вендоры программного обеспечения для бизнеса, производители гаджетов. Каждая компания стремится занять свое место под солнцем в новом подключенном мире.

— сегмент рынка —

В 2015 году тема IoT (Internet of Things — интернет вещей) была на пике ожиданий: она занимала верхнюю точку на кривой Gartner Hype Cycle for Emerging Technologies (график, показывающий, какие новые технологии наиболее активно изучают клиенты). В августе текущего года Gartner обновила график, и оказалось, что термин IoT выбыл из списка обсуждаемых инноваций вообще. Это означает, что концепция IoT, во-первых, утратила интерес инвесторов и их клиентов, а во-вторых, разделилась на несколько подтем. В частности, среди наиболее обсуждаемых технологий в текущем году оказались «Подключенный дом» (Connected Home) и дроны для коммерческого использования (Commercial UAVs).

Опрошенные в прошлом году компаниями IDC организации связывали свои ожидания от IoT с тем, что эти технологии могут принести следующие преимущества бизнесу: повышение производительности (14,4% опрошенных), ускорение вывода на рынок новых продуктов (11,3%), автоматизация процессов (11,1%), снижение издержек (9,9%), ускорение процесса принятия решений (9,9%), повышение энергоэффективности (7,8%), улучшение пользовательского опыта (6,5%), дифференциация на фоне конкурентов (6,4%), создание новых потоков выручки (5,2%), доступ к новым клиентским сегментам (3,6%). То есть для бизнеса во всем мире IoT — это одно из стратегически важных направлений развития.

Потому аналитики обещают рынку решений для интернета вещей огромный рост. По прогнозу IDC 30 млрд подключенных устройств в 2020 году помогут компаниям из этой индустрии сгенерировать выручку объемом \$1,7 трлн. Ежегодно рынок будет прирастать на 16,9%, а к се-

ти будет подключаться от 4,8 тыс. IoT-устройств в минуту в 2015 году до 7,9 тыс. — в 2020 году.

Андрей Биветски, генеральный директор SAP Labs в СНГ, говорит: «Мы согласны с рядом экспертов, которые оценивают рынок IoT до 2025 года в объеме 10–11% мирового ВВП. Из этой цифры примерно 70% придется на сегмент B2B, то есть как раз на индустриальный интернет вещей», — говорит глава SAP Labs в СНГ.

По данным J'son & Partners Consulting, в России количество IoT-устройств к концу 2015 года составило 16 млн, их число удвоится к началу 2018 года. Джонатан Батти, директор по связям с общественностью IBM Watson Internet of Things, считает, что в РФ есть своя специфика: «В России мы видим огромный потенциал индустриального применения интернета вещей, в частности в промышленном производстве, сельском хозяйстве, горнодобывающей промышленности и ТЭКе. Ведь интернет вещей идеально подходит для управления удаленными объектами». Географические особенности страны подсказывают, что удаленные системы интернета вещей должны обрабатывать информацию близко к точкам ее сбора для работы в условиях невысокой пропускной способности каналов.

Взгляд сквозь телеком

По всем направлениям IoT идет борьба за лидерство между «ветеранами» рынка ИКТ (информационные и коммуникационные технологии) и новыми игроками. «Старички» уже выбрали свои ниши и следуют разработанным стратегиям. Один из игроков телеком-рынка, претендующий на лидерство на зарождающемся рынке IIoT (Industrial Internet of Things — индустриальный интернет вещей), — федеральный оператор «Ростелеком» — включает данную тему в число направлений стратегическо-



В Интернете вещей комбайн станет умнее комбайнера

го развития. «Решение о включении его в стратегию компании продиктовано, с одной стороны, нынешней логикой развития телеком-операторов, смещения денежных потоков на рынок. С другой стороны, индустриальный интернет вещей — это комплексная задача. Мы верим, что в текущих экономических условиях внедрение технологий IoT в приборно- и машиностроении, в энергетике и ряде других отраслей должно помочь российской экономике не выпасть из обоймы стран, успешно участвующих в реализации идей очередной промышленной революции, и перейти к так называемой индустрии 4.0», — комментирует Владимир Шукин, директор по индустриальному интернету ПАО «Ростелеком».

Оператор смотрит на экосистему IIoT как на «слоеный пирог», состоящий из нескольких сегментов: передача данных, облачные технологии, защита информации, разработка ПО и оборудования и др. На передаче данных приходится всего 5% доходов, 10% приходится на услуги защиты данных. Исходя из исторических предпосылок, можно было бы пред-

положить, что оператор претендует на эти 15% рынка. Но компания смотрит шире. «Данные и так будут передаваться через наши защищенные сети, — объясняет Владимир Шукин. — Мы ищем нишу, достаточно весомую, чтобы мотивировать крупных клиентов осваивать ее вместе с «Ростелекомом». Мы считаем, что этой перспективной нишей является бизнес-интеракция. По некоторым оценкам, на нее придется около половины доходов в экосистеме IIoT. Если прибавить к этому упомянутые 15% доходов из традиционных для нас ниш, становится понятным, ради чего «Ростелеком» выбирает индустриальный интернет в качестве стратегического направления развития».

Компания больше года активно разрабатывает это направление. По словам Владимира Шукина, работа ведется как на институциональном уровне — путем формирования «дорожных карт» и участия в профильных международных организациях, так и на практическом уровне — путем реализации пилотных проектов. Оператор также стал инициатором создания Национальной ассоциации участников рынка промышленного интернета, которая выступает в качестве организационно-правовой основы Консорциума индустриального интернета (его создание поддержано президентом Российской Федерации в поручении от 18 декабря 2015 года №Пр-2642). «Ростелеком» видит себя участником конкретных проектов в этой сфере, оператором инфраструктуры сбора и обработки технологических данных, а также поставщиком платформ, на которой будут развернуты приложения для крупнейших отраслевых предприятий.

Приложение силы

На роль поставщиков приложений для IIoT претендуют разработчики ПО для бизнеса, многие из которых активизировали работу по данному направлению в текущем году. IBM объявила в октябре об открытии глобальной штаб-квартиры для бизнес-подразделения Watson Internet of Things в Мюнхене, которое будет заниматься разработкой новых решений в области интернета вещей для технологических компаний и систем безопасности. IBM инвестирует в работу штаб-квартиры \$200 млн.

Компания SAP в июне открыла на базе Лаборатории совместных инноваций Центр интернета вещей.

Андрей Биветски рассказывает, что в текущем году в России компания фокусируется в данном направлении на нескольких отраслях. В первую очередь, это медицина. SAP разработала прототип решения по интеграции бизнес-систем с терминалами, производимыми компанией «Квазар». Они заменяют врача, проводящего медосмотр работников перед сменой. Такие терминалы установлены у ряда заказчиков SAP из металлургической и нефтегазовой отраслей. Вторая отрасль, находящаяся в фокусе внимания SAP, — сельское хозяйство. SAP Labs в Москве разработала сценарий для животноводства, в котором дроны собирают информацию с датчиков, данные передаются в облако, где обрабатываются и помогают принимать важные решения. По словам Андрея Биветски, сценарии интернета вещей можно использовать для мониторинга выращивания определенных культур, контроля за удобренностью почвы. Еще один сценарий, который уже прошел тестирование в крупнейших международных агрохолдин-

гах, — умный комбайн. Он не только вспахивает землю, но и одновременно собирает информацию с датчиков и отправляет ее в базу данных. Для одного из крупнейших российских металлургических предприятий компания разработала решение Predictive Quality, позволяющее предсказывать качество выпускаемой продукции (лития) на базе показаний, собранных с производственных датчиков.

Продукт под названием Internet of Things Cloud Service есть и у Oracle. Компания собирается включить в него готовые приложения и поставлять их по модели SaaS. В свежем релизе, выпущенном в августе, разработчик предложил Asset Monitoring Application — приложение для наблюдения за состоянием активов. Это могут быть движущиеся объекты (например, автомобили или грузы) либо статические (здания, инфраструктура).

В этом году компания SAS также представила продукт Analytics for IoT — специализированный пакет приложений для анализа больших объемов данных, поступающих с датчиков и устройств, подключенных к IoT. Антон Заяц, директор по развитию бизнеса «SAS Россия/СНГ», говорит, что эти приложения уже проверены и не раз доказали свою эффективность при прогнозировании сбоев оборудования, при оптимизации нагрузки на электростанции. Теперь же они объединены в интегрированный пакет. SAS выбрала для себя роль поставщика аналитических приложений для IIoT, что логично: компания более 40 лет специализируется на этой теме.

Григорий Сидоров, директор практики по оказанию услуг компаниям в области связи, информационных технологий и СМИ, PwC в России, объясняет: «По нашей экспертной оценке, различные отраслевые сегменты рынка IoT в России будут расти темпами от 10% до 20% в год. В массовом сегменте рынка IoT значительную долю сможет занять топ-игрок, который предложит простое и понятное end-to-end решение для конечного потребителя. Это могут быть глобальные бренды, обладающие огромной пользовательской аудиторией, а могут быть и локальные игроки (телеком-операторы, интернет-компании), которые понимают российский специфику и могут быстро «собрать» новую бизнес-модель, учитывая потребности рынка. Возможно также смешанное решение, когда крупный игрок предоставляет IIoT-платформу, на которой работают нишевые решения, разработанные отдельными специализированными компаниями».

Светлана Рагимова

Panasonic BUSINESS

ДАЙТЕ МНЕ UC-ПЛАТФОРМУ, И Я ПЕРЕВЕРНУ МИР

Унифицированные коммуникации. Передовые технологии. Оптимизация расходов.

UC-платформа KX-NSX — это переворот в представлении о традиционных офисных коммуникациях от Panasonic. Современные IP-технологии и все необходимые сервисы позволяют сотруднику работать из любой точки мира.

- Высокая надежность системы за счет «горячего» резервирования
- Возможность подключения до 2000 IP-адресов
- Поддержка всех существующих коммуникационных сервисов

Мы создаем платформу для вашего бизнеса, чтобы вы перевернули этот мир!

www.panasonic.com b2b.panasonic.ru

Информационный Центр Panasonic для Москвы 8-495-725-05-65, для регионов РФ 8-800-200-21-00 (звонок бесплатный). На правах рекламы ООО «Панасоник Рус» — уполномоченного представителя компании Panasonic Corporation Ltd. на территории России

UC-платформа KX-NSX2000/1000 SIP-видеотелефон KX-HDV430

5

ПЯТЬ ЛЕТ ГАРАНТИИ

Финты вокруг финтех

— инновации —

По мнению Алексея Благирева, это может сильно изменить банковскую систему. К примеру, станут реальными такие проекты, как Bank as a Service, где банк может быть представлен как платформа, интегрирующая в себя те или иные финтех-проекты. В РФ, как считает господин Благирев, подобные изменения тоже рано или поздно произойдут, но степень их влияния на банковский сектор сильно зависит как от действующего регулятора, так и от активной работы самих участников, в частности по созданию упомянутой выше «специализации».

Сам банк «Открытие» в конце октября планирует провести мероприятие «Открытые бои», на котором предоставит доступ к API по интернет-эквайрингу и peer-2-peer эквайрингу всем внешним командам разработчиков, которые успели подать заявки и пройти отбор.

MasterCard также активно сотрудничает со стартапами в рамках целого ряда инициатив. К примеру, программу Start Path Global, которую компания запустила в 2014 году, прошли 60 стартапов, в том числе из РФ. Некоторые из них строят бизнес-модели на основе блокчейна. Во время Start Path участники взаимодействуют с командой экспертов MasterCard, получают доступ к ее клиентам и партнерам, а также возможность создавать инновационные продукты на основе уже существующих решений MasterCard. Другая инициатива компании по поддержке финтех-предпринимательства — платформа MasterCard Developers, с которой разработчикам проще создавать коммерческие решения нового поколения. Она позволяет партнерам получить доступ к API компании. С помощью «Новых и экспериментальных интерфейсов» API-платформы MasterCard разработчики могут создавать сервисы электронных платежей, к примеру для оплаты VR-контента, покупок в дополненной реальности и в интернете вещей.

Михаил Берлизев, генеральный директор DCA (Data-Centric Alliance) говорит, что финтех способствует повышению эффективности финансовой системы: «Тинькофф», «Альфа», «Открытие» и другие банки ориентируются на новое поколение российских потребителей, которые требуют мобильности, удобства, скорости, более низкой стоимости услуг и визуализации информации. Финтех-компании нивелируют посредников и снижают затраты на финансовые услуги, создают удобные и интуитивно понятные мобильные приложения, которые позволяют экономить время в очередях, визуализируют все стадии финансовых отношений, индивидуализируя процесс финансовых отношений, и позволяют клиентам чувствовать себя в личном кабинете как дома, с массой индивидуальных настроек». В качестве примера господин Берлизев приводит проект, реализованный DCA совместно со «Скористой», в котором с помощью методов машинного обучения и технологий Big Data строятся модели, выявляющие потенциальных мошенников среди заемщиков. Технология позволяет снизить количество выданных по подложным документам займов на 80%.

Банки без границ

Исследовательские лаборатории передовых банков демонстрируют то, какими станут финансовые услуги в будущем. При этом большинство банков в РФ не прошли еще первые этапы цифровой трансформации. Давид Мартиросян, директор практики страховых и банковских решений компании AT Consulting, говорит, что финансовые организации в РФ осваивают мобильные платформы и omnichannel — интегрируют различные каналы взаимодействия с пользователями в единую среду. На мобильных устройствах банки начинают помимо классических функций предлагать платформенные фишки, такие как возможность сфотографировать и распознать номер карты для

перевода или применить биометрическую идентификацию при входе в приложение.

«Банки делают упор на внедрение omnichannel-решений, так как это позволяет создать для клиентов комфортную, «знакомую» среду в независимости от того, зашел он оплатить счета за коммунальные услуги или же заинтересован в получении сервисов для своего предприятия. Хорошее знание клиента и его предпочтений дает возможность банкам предоставлять таргетированные сервисы и увеличивать за счет этого выручку», — объясняет Давид Мартиросян. Еще один тренд последних лет — цифровизация: ряд банков отказывается от работы через физические отделения и переводит клиентов на онлайн-обслуживание. Самые известные в России бренды, которые работают по таким принципам, — Тинькофф-банк и Рокетбанк. В СНГ — цифровой банк Altun-i, запущенный в нынешнем году в Казахстане.

Давид Мартиросян считает, что финтех-стартапы помогают финансовой индустрии быстрее осваивать передовые технологии: «Банковская отрасль консервативна с точки зрения ИТ, но финтех-стартапы стимулируют рынок оказывать услуги быстрее и делать доступ к ним более удобным. Даже очень крупные кредитные организации вводят в ИТ-процессы элементы гибкой методологии разработки ПО (Agile, — «Б»). Кроме этого часто на рынке происходит ситуация, когда финтех-стартап начинает сотрудничать с банком, а при успешном сотрудничестве уже происходит их слияние. Это дает дополнительный импульс к трансформации ИТ-инфраструктуры в банковской среде. Заслуживает внимания также исчезновение границ между услугами для клиентов — когда базовые банковские сервисы дополняются партнерскими опциями. Например, возмещение части стоимости поездки на такси Uber с карты банка-партнера. Таких решений становится все больше».

Светлана Рагимова