К чему приводят взломы домашних устройств и утечки конфиденциальной информации | 14

ИТ

Тематическое приложение к газете **Коммерсантъ**

Информационные технологии

Четверг 30 мая 2019 №92 (6572 с момента возобновления издания)

kommersant.ru

16 | Как зарабатывают интернет-пираты и можно ли победить пиратское видеосмотрение

17 | Почему мировые корпорации инвестируют в развитие квантовых технологий

Киберспорт на вырост

После ряда крупных сделок последних лет российский рынок киберспорта вышел на перепутье. Его объем продолжает расти ежегодно на 20–30%, а российские команды претендуют на участие в крупнейших мировых соревнованиях. Однако сегмент уже перестал быть приоритетным для некоторых возможных стратегических инвесторов, что может подтолкнуть клубы обратиться за поддержкой к государству.

REUTERS

— обзор рынка —

Выйти на мировой уровень

20–25 августа в Шанхае пройдет киберспортивный турнир по игре Dota 2 The International 2019. Соревнования, организованные американской компанией Valve, разработчиком этой игры, проводятся уже девятый год подряд. В турнире будут участвовать 18 команд, среди них будет 2 команды из СНГ — такой размер квоты на регион. Пока с уверенностью можно сказать, что одна команда из России точно примет участие в турнире — это Virtus.pro, сообщил „Ъ“ Роман Дворянкин, генеральный менеджер киберспортивного клуба Virtus.pro: «Мы снова, как и год назад, стали первым клубом, получившим прямое приглашение на The International».

РЫНОК КИБЕРСПОРТА РФ В 2018–2019 ГОДАХ

ИСТОЧНИКИ: SOSTAV, PAYPAL, SUPERDATA, ESFORCE, WINSTRIKE, NIELSEN, ФКС РОССИИ.

По словам Романа Дворянкина, с 22 по 30 июня в Москве на турнире Epicenter Major разыграют последние очки этого сезона, которые позволят набравшим их командам войти в число 12 приглашенных участников The International; еще 6 мест займут команды, прошедшие специальные отборочные, организованные по всему миру, в том числе в СНГ. «Будут ли среди них российские команды — покажут предстоящие игры. У нас в стране есть достойные коллективы»,— считает он.

Среди других команд из СНГ фаворитами считаются российская Gambit Esports и украинская Natus Vincere (победитель The International 2011 года.— **„Ъ“**). По мнению гендиректора команды Vega Squadron Алексея Кондакова, они выглядят сейчас сильнее остальных, «но это не означает, что поедет кто-то из этих двух команд — поехать может третий, кто наберет внезапно хорошую форму перед квалификацией»,— уточняет он. CEO Natus Vincere Евгений Золотарев считает, что в нынешнем году попадание на The International 2019 «уже будет неплохим результатом, а выход в топ-8 — успехом», писал Sports.ru 16 мая.

У Dota 2 в СНГ наибольшее число геймеров, в том числе поэтому она считается главной киберспортивной дисциплиной в СНГ, поясняет Алексей Кондаков. Крупнейшие клубы также имеют составы по игре в Counter-Strike: Global Offensive, Fortnite, FIFA, PlayerUnknown's Battlegrounds и др. В других странах Европы и США Dota 2 не так популярна, а «дисциплиной номер один остается League of Legends», считает Алексей Кондаков. Таким образом, The International 2019 — это самый важный турнир для российских киберспортсменов, заключает он: «Сам турнир — это хайп во всем мире, большое количество просмотров, и, скорее всего, его посмотрит даже тот, кто не увлекается Dota 2, просто потому что это очень большой турнир с большим призовым фондом».

К слову, на данный момент он составляет более $13 млн: стартовую сумму $1,6 млн выделила Valve, остальное фактически заплатили геймеры за счет внутриигровых покупок. Сбор продолжается, и окончательная сумма еще не известна, но по темпам прироста за первые сутки сбора она на 24% превысила динамику 2018 года, когда итоговый призовой фонд составил $25,5 млн. У турнира есть все шансы поставить новый рекорд по призовым в текущем году, считает Роман Дворянкин. Призовой фонд в 2019 году будет либо таким же, либо выше, рассуждает Алексей Кондаков.

Болельщики у мониторов

Главный турнир по Dota 2 в 2018 году привлек заметную аудиторию. Пиковое число зрителей на трансляциях стадии play-off The International в 2018 году составило 14,9 млн человек, что на 37% больше показателя 2017 года, указывает Роман Дворянкин. В нынешнем году турнир впервые пройдет в Китае, так что нет никаких сомнений, что аудитория покажет сопоставимый рост, считает он.

Если российская компания хочет получить доступ к аудитории The International, она может пойти как минимум двумя путями: стать спонсором команды—участницы турнира или партнером трансляции, поясняет Роман Дворянкин. «Возможны оба варианта сразу — так поступил в прошлом году телеком-оператор «МегаФон», в цвета которого мы даже перекрасили на тот период форму команды. Возможны по отдельности — например, бренд контактных линз Acuvue спонсировал трансляцию квалификаций на турнир и проводил специальный конкурс для зрителей. Все зависит от текущих задач и планируемого масштаба маркетинговой кампании»,— уточняет Роман Дворянкин.

The International транслируют по всему миру, в том числе есть русскоязычная трансляция, пиковое число зрителей на ней в прошлом году составило почти 500 тыс. человек, рассказывает он. Например, трансляция турнира в «Одноклассниках» собрала 12 млн уникальных зрителей, сообщала ранее социальная сеть. В ходе этого проекта Mail.ru Group (владеет «Одноклассниками») еще раз убедилась, что социальные сети — один из немногих каналов коммуникаций, где есть потенциал для роста киберспортивной аудитории и где людям действительно удобно наблюдать за турнирами, рассказывает руководитель киберспортивного направления Mail.ru Group Иван Возняк.

Показывать киберспортивные трансляции начал и «Яндекс». В феврале компания объявила о долгосрочном соглашении с Riot Games, разработчиком League of Legends, в рамках которого получила эксклюзивные права на показ киберспортивного контента на русском языке через сервис «Яндекс.Эфир» и возможность монетизировать трансляции и видео. «Мы видим огромный интерес к киберспорту, которого на телевидении просто нет. Мы рассчитывали, что контракт с Riot Games позволит нам привлечь мужчин в возрасте от 20 до 34 лет, и не прогадали»,— сообщил порталу Adindex коммерческий директор «Яндекса» Леонид Савков.

с16

«Цифра» поворачивается в профиль

— госпрограмма —

Цифровизация экономики России немыслима при сохранении текущего порядка сбора и обработки персональных данных и юридически значимой информации россиян. Сейчас мы вынуждены искать информацию о себе в реестрах десятка разных ведомств, которые зачастую не интегрированы между собой. Несмотря на действующую систему электронных госуслуг, для получения некоторых документов все еще нужно лично приходить в «присутственные места», все прелести посещения которых описаны еще в произведениях русских классиков и знакомы россиянам со школы. Изменить ситуацию и дать серьезный толчок для роста экономики может единый цифровой профиль гражданина, созданием которого сейчас заняты власти. Такая платформа позволит собрать разрозненные данные о россиянах и будет предугадывать их потребности в получении государственных и коммерческих услуг.

Миграция данных в виртуальную среду

В конце марта президиум правительственной комиссии по цифровому развитию под руководством вице-премьера Максима Акимова утвердил концепцию цифрового профиля гражданина — его создание предусмотрено национальным проектом «Цифровая экономика». Проект концепции в декабре 2018 года подготовили ЦБ и «Ростелеком», ее основная цель — упрощение получения россиянами коммерческих и государственных услуг. Так, по словам директора по направлению «Информационная инфраструктура» АНО «Цифровая экономика» Дмитрия Маркова, цифровой профиль позволяет получить доступ к данным государственных информационных систем (ГИС): «Эти данные гражданин сможет согласиться предоставить какой-либо организации — государственной или коммерческой — с помощью смартфона или компьютера». Создаваемая система, как ожидается, позволит обеспечить удобный и безопасный обмен данными между гражданами, государством и бизнесом.

В последнее десятилетие жизнь значительной части людей стала активно мигрировать из физического мира в виртуальный, при этом удобство многих сервисов, доступных онлайн, во многом превосходило удобство сервисов «физических». Благодаря этому стал экспоненциально расти «цифровой след» человека в сети, включающий в себя как личную информацию человека, так и метаданные, формирующиеся в результате его «сетевого поведения», напоминает директор департамента консалтинга «Делойт» СНГ Максим Налютин. В то же время большинство людей не имели полного представления о том, где эта информация содержится и каким образом она используется компаниями, отмечает он.

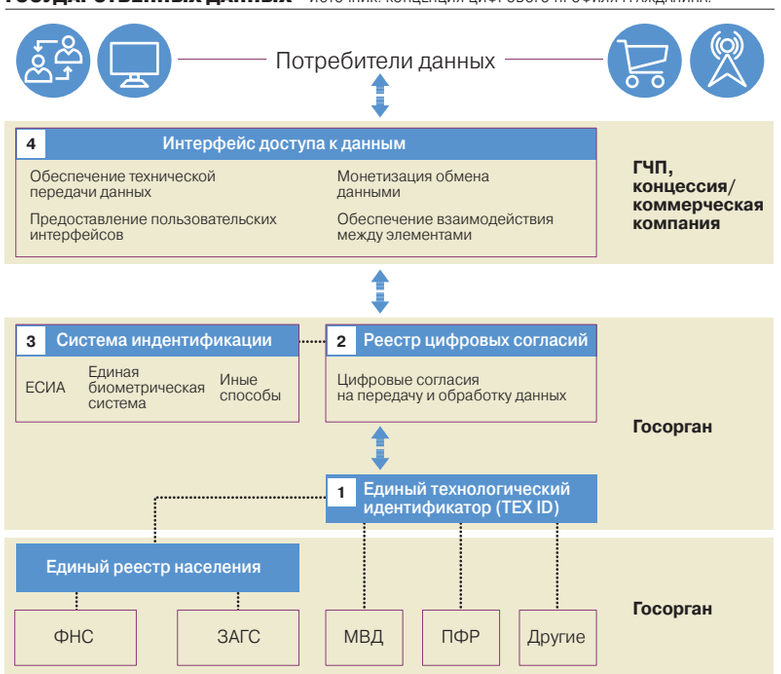
Решением этой задачи во многих странах мира занялись государственные органы, которые разработали свод законов, позволяющих усилить контроль за сбором и обработкой персональных данных. «Примером таких законов является GDPR в Европе или CCPA в Калифорнии,— считает эксперт.— Российская инициатива является аналогом этих инициатив и также призвана упорядочить регулирование сбора и обработки персональных данных пользователей интернет-сервисов».

Вся информация вместе

Создание цифрового профиля потребует 3,091 млрд руб. внебюджетных средств до 2021 года — эти средства включены в раздел «Информационная инфраструктура» нацпроекта «Цифровая экономика». Цифровой профиль гражданина будет включать основные сведения о нем: паспортные данные, СНИЛС и ИНН, а также ссылки на информацию из ГИС и реестр цифровых согласий на обработку персональных данных. Всего цифровой профиль будет хранить 57 видов личных данных, тогда как сейчас в единых системах россияне могут хранить лишь 21 вид данных. При необходимости можно будет потребовать удалить неактуальную или недостоверную информацию о себе.

Чтобы получить доступ к своему цифровому профилю, гражданин должен будет пройти идентификацию с помощью инфраструктуры Единой системы идентификации и аутентификации (ЕСИА, основной способ) и с использованием Единой биометрической системы. После этой процедуры он сможет направить запрос в соответствующую ГИС о предоставлении определенного набора сведений. Внедрение цифрового профиля в России будет происходить поэтапно через оптимизацию и трансформацию традиционных госуслуг. Предполагается, что юридически значимые электронные госреестры начнут предлагать так называемые суперсервисы, для получения которых посещать госорганы не придется. Система в автоматическом режиме будет предлагать конкретному человеку подходящие именно ему госуслуги в электронном виде, и посещать ведомство, чтобы получить бумажное свидетельство, больше не потребуется.

СХЕМА РАБОТЫ ЦИФРОВОГО ПРОФИЛЯ С ИСПОЛЬЗОВАНИЕМ ГОСУДАРСТВЕННЫХ ДАННЫХ ИСТОЧНИК: КОНЦЕПЦИЯ ЦИФРОВОГО ПРОФИЛЯ ГРАЖДАНИНА.



В феврале президиум правкомиссии по цифровому развитию утвердил перечень из 25 таких сервисов. Среди них, в частности, онлайн-сервисы по медсправкам и документам (куратор — Минздрав), регистрации нарушений ПДД и правил благоустройства, регистрационные и паспортные сервисы, сервисы по уведомлению и обжалованию штрафов (МВД), получению цифровых документов об образовании (Минпросвещения), господдержке бизнеса (Минэкономики), поступлению в вуз (Минобрнауки), безбумажным перевозкам пассажиров и грузов (Минтранс) и т. д.

Ожидается, что «дорожные карты» развития «суперсервисов» ответственные ведомства представят до конца июня. По итогам цифровой оптимизации госуслуг к 2021 году доля цифрового взаимодействия граждан и бизнеса с властями должна составлять не менее 80%. Законопроект о цифровом профиле гражданина Минкомсвязь вынесла на общественное обсуждение в конце марта, в соответствии с концепцией он должен быть внесен в Госдуму весной, а принят — до конца июня. За реализацию концепции отвечают ЦБ, Минкомсвязь и «Ростелеком». «Государство в основном выполняет роль заказчика, а бизнес вносит свою экспертизу»,— отмечает Дмитрий Марков. При этом АНО «Цифровая экономика» проводит рабочие группы и экспертные совещания.

Монетизация информации

Предполагается, что массив информации смогут использовать не только госструктуры, но и частные компании. И если сами граждане получат контроль над доступом к данным о себе, то, согласно законопроекту Минкомсвязи, бизнес должен будет оплачивать некоторые запросы к цифровым профилям граждан. Платным будет получение информации или бесплатным — это будет зависеть от категории запроса, его целей и того, кто запрашивает информацию. Размер оплаты и перечень платной информации будет определять правительство.

Пилотный проект цифрового профиля стартует нынешней весной: им станет сервис по выдаче кредитов. При согласии пользователей 16 банкам—участникам ассоциации «Финтех» предоставят проверенные и актуальные данные, хранящиеся в государственных информационных системах, для заполнения заявки на получение кредита и проведения процедуры скоринга в режиме онлайн. В тестировании также примут участие три страховые организации, МВД, Пенсионный фонд России, ФНС, Росреестр, которые поделятся сведениями о россиянах, и Аналитический центр при правительстве. До конца года будет запущено мобильное приложение для управления своими данными в государственных информационных системах. Можно будет, например, подтвердить информацию о водительских правах, не имея при себе документов, обещают авторы инициативы.

В концепции цифрового профиля между собой взаимодействуют четыре стороны: первая — это гражданин, вторая — организации, которым нужна информация, третья — организации—источники информации для профиля, которые ранее взаимодействовали с гражданином, и четвертая — это оператор профиля, поясняет руководитель практики по работе с компаниями сектора технологий, медиа и телекоммуникаций КПМГ в России и СНГ Еркожа Акылбек. И в этом случае самым вероятным сценарием монетизации части услуг, основанных на цифровом профиле, станет оплата организациями, которым нужен доступ к профилю, оператору системы, заключает он. «Это логично, потому что оператор предоставляет некий сервис и на него ложатся все затраты на создание и поддержание инфраструктуры, по архитектурному и программному решению. С меньшей степенью вероятности смогут заработать организации, которые предоставляют данные оператору»,— считает он.

При этом гражданин, который является окончательным владельцем данных, вряд ли сможет стать выгодоприобретателем от этой инициативы. «Человек в этом случае пассивен по отношению к своему цифровому профилю и не принимает активного участия в процессе его функционирования, так как одна и та же структура может использовать его данные и для того, чтобы его как-то ограничить (например, отказать в выдаче кредита), и для того, чтобы как-то ему помочь (например, предложить скидку)»,— рассуждает Еркожа Акылбек. Поэтому, по его мнению, важно, чтобы государство обеспечило должный уровень защиты персональных данных граждан и гарантировало отсутствие злоупотреблений на этой почве, отмечает эксперт.

Тем не менее, чтобы система обмена данными с компаниями заработала, необходимо проделать большую работу, ведь ни бизнес сегодня не интегрирован с ГИС, ни ГИС до сих пор технически не интегрированы между собой, напоминают эксперты. «Было бы правильно учесть ошибки прошлого и создать систему, в которую будут заложены возможности интеграции и расширения функционала, чтобы поддерживать сегодняшний темп развития технологий, оставаясь актуальной»,— считает господин Акылбек. В целом набор юридически значимых электронных документов и актуальных данных из ГИС, собранных в одном месте,— это не что иное, как «большие данные», которые, в свою очередь, будут являться базой или «топливом» для цифровой экономики как в государственном, так и в частном секторе, заключает он.

Юлия Тишина

Review

«Для многих сервисная модель — практически единственный способ обеспечить безопасность»

Хакеры перешли на сервисную модель в организации атак: одни группировки пишут вредоносы, другие обналичивают деньги, поскольку именно сервисная модель позволяет обеспечить оптимальное соотношение цена-качество. Для потенциальных мишеней атак сервисная модель является также оптимальной, так как она представляет собой идеальное соотношение цена-качество. О том, как компании могут противостоять злоумышленникам, „Ъ“ рассказал вице-президент ПАО «Ростелеком» по информационной безопасности **Игорь Ляпунов**.

ПЕТР КАССИН

— интервью —

— ЦБ, комментируя хищения средств у банков, часто отмечает крайне низкий уровень информационной безопасности в атакованной организации. Создается впечатление, что с информбезопасностью в банках совсем плохо.

— Это не так. Крупных выводов средств из банков становится все меньше благодаря усилиям ЦБ и всего финансового сегмента. При этом есть серьезная проблема — стоимость безопасности и ее доступность для небольших игроков. Например, у банков ниже топ-150 нет бюджета на покупку средств защиты и возможности нанимать хороших специалистов, их цель — выжить.

— Как обстоят дела в других отраслях?

— Мы видим рост атак на сегмент электронной коммерции, ритейлеров. Кроме того, появляются политически мотивированные группировки, цель которых не монетизация, а получение контроля над атакованной инфраструктурой. Сейчас в России есть термин «критическая информационная инфраструктура», и атаки на нее — это атаки совершенно другого профиля.

— Чем они отличаются от традиционных атак на банки или тот же ритейл?

— При атаке на банк сначала идет долгий процесс изучения потенциальной жертвы, далее достаточно быстро преодолевается периметр, после, уже почти не прячась, злоумышленник движется туда, откуда можно вывести деньги. При атаках с целью получения контроля мы сталкиваемся с другим подходом. Это медленные атаки, развивающиеся в течение многих месяцев, при этом на каждом шаге атакующий очень аккуратно подчищает следы.

— Для чего злоумышленнику такая осторожность?

— Потому что его главная задача — не быть скомпрометированным, обнаруженным в этой структуре. Тут идут в ход хорошо написанные бесфайловые вирусы, используются зловреды, способные определять, является ли окружение реальной инфраструктурой или «песочницей», созданной для наблюдения за их возможностями. Разработка подобного вредоносного ПО требует высокой квалификации. Когда мы в лаборатории исследуем подобный зловред, то по тому, как он написан, насколько технически, функционально оснащен, можем понять, сколько денег было потрачено на его разработку. Иногда над созданием такого ПО может работать команда и до 100 человек. И отсюда можно делать выводы, кто готов инвестировать в атаку такие деньги.

— И много сейчас атак с целью получения контроля?

— Если в процентном отношении — очень небольшая часть. Однако угроза атак на критическую инфраструктуру очень ощутима с точки зрения национальной безопасности. Обычно при таких атаках используется вредоносное ПО, специально написанное под конкретную организацию, и стандартные средства защиты от него не спасут. К счастью, во многих организациях это понимают. Сейчас около трети клиентов Solar JSOC — это объекты критической информационной инфраструктуры: энергетика, жизнеобеспечение, системы государственного управления.

— Однако подключение к Solar JSOC — недешевое удовольствие, которое небольшие компании себе позволить не могут.

— Да, это так, и для них мы создали единую платформу сервисов кибербезопасности. Концепция, с которой «Ростелеком-Solar» идет на рынок, как раз в том, чтобы сделать технологии безопасности существенно более доступными — как по цене, так и по модели потребления.

— А в чем преимущество сервисной модели перед выстраиванием защиты собственными силами?

— В первую очередь преимущество в скорости получения технологии. Сейчас, чтобы самостоятельно построить защиту, необходимо потратить четыре-шесть месяцев. Мы же можем сократить эти сроки до нескольких дней.

— Сразу предлагая готовый сервис?

— Да, за счет возможностей «Ростелекома». Вместе с каналом «Ростелекома» мы можем представлять технологии защиты на основании нашей единой платформы кибербезопасности — защиту от сетевых атак, обеспечение безопасности электронной почты и веб-приложений.

— Каков примерный порядок стоимости подключения к платформе?

— Для небольшой компании или банка мы можем собрать в сервисной модели пакет необходимых средств защиты за сумму порядка 100–200 тыс. руб. в месяц, который обеспечит адекватный уровень защиты. И на дистанции три-четыре года, если суммировать все сервисные платежи, клиенту будет дешевле оплачивать услугу, чем самостоятельно покупать средства защиты и постоянно оплачивать техподдержку. Кроме того, понятное преимущество заказчика состоит в том, что он может собрать необходимую именно ему защиту как из конструктора и платить только за тот объем сервисов, который реально потребляет.

— Создание подобной платформы потребовало серьезных инвестиций. Сколько было потрачено и за какой срок планируете выйти на окупаемость?

— Более 1 млрд руб.— это прямые и косвенные инвестиции в создание платформы в течение полутора лет. Обычный срок окупаемости проектов у нас три года.

— Сколько клиентов необходимо привлечь, чтобы выйти на прибыльность проекта?

— Текущая емкость платформы — 1 тыс. точек подключения, и думаю, что на эту цифру мы выйдем уже в 2019 году.

— Есть ли у вас конкуренты, которые предлагают аналогичные сервисы?

— У нас нет конкурентов, и это проблема.

— Проблема в отсутствии конкуренции? Так не бывает.

— Бывает. Когда мы запускали в 2013 году Solar JSOC, у нас не было конкурентов. Дело в том, что заказчик любит выбирать, а когда мы одни на рынке, он лишен этой возможности и начинает сомневаться. Когда в 2016 году появились конкурирующие SOC, нам стало гораздо проще. Вместе с другими сервис-провайдерами мы воспитываем рынок и даем заказчику возможность выбора. В случае с ЕПСК мы сейчас бьемся не за то, чтобы кого-то обогнать, а за то, чтобы люди поняли, что защищаться от киберугроз необходимо и что для многих сервисная модель — это практически единственный способ обеспечить безопасность.

— Вы говорите об этом так уверенно…

— Мы прошли этот путь в 2013 году с Solar JSOC, когда кибербезопасность воспринималась как очень закрытый, внутренний процесс, который нельзя отдавать на аутсорсинг. Однако прошло два года, хакеры начали массово взламывать банки, потребовался мониторинг 24/7, который никто не мог обеспечить собственными силами, и стала очевидна необходимость в SOC.

— Часто слышу от банков: можно построить высокий забор из информбезопасности, но достаточно одному невнимательному сотруднику открыть фишинговое письмо от хакеров…

— Да, около 70% всех сложных атак осуществляется через социальный вектор, через фишинг.

— Что же делать? В теории правила безопасности знают все, а на практике…

— Единственный вариант — программы повышения осведомленности, которые обязательно должны включать тестирование, проверку того, насколько хорошо сотрудники умеют выявлять фишинг. Тестирование показывает: как бы сотрудников ни обучали, на практике 80% открывают письмо, похожее на внутреннюю рассылку компании, даже если ссылки в нем явно ведут на внешние ресурсы. Повторное тестирование обычно показывает, что фишинг выявила уже бОльшая часть сотрудников.

— Работа в сервисной модели требует высококвалифицированных специалистов, которые на рынке в большом дефиците.

— Да, и сейчас это главное поле конкуренции: мы конкурируем с игроками рынка не за заказчиков, а за людей.

— И как вы решаете кадровую проблему? Переманиваете специалистов у конкурентов?

— Нет, сейчас мы вкладываемся в программы взаимодействия с вузами. У Solar JSOC есть подразделения не только в Москве, но и в Нижнем Новгороде, Самаре, Хабаровске, в этом году планируется открытие офиса в Ростове-на-Дону. Мы ориентируемся на города, где есть вузы с сильными IT-кафедрами. Начиная с четвертого-пятого курса берем студентов на стажировку — примерно 50–60 человек в городе раз в полгода. Из них десять человек получают предложение о работе.

— Но бывшие выпускники же еще совсем зеленые.

— Бывших выпускников мы сажаем на первую линию, через 9–12 месяцев переводим на вторую и так далее. В итоге за несколько лет мы получаем действительно хорошего специалиста.

— А то, что вы читаете лекции в лагере «Сириус», в школах,— это тоже своего рода инвестиция в будущие кадры?

— Скорее отражение нашей социальной функции, так как из 12-летних школьников лишь через семь-десять лет вырастут кадры для рынка. Прежде всего это возможность выявить талантливых детей и помочь им в развитии способностей. Мы стремимся создавать кадровый ресурс не только для себя, но и для отрасли в целом. Кибербезопасность уже стала необходимым условием для уверенного развития страны, и талантливые ребята — это наше будущее.

Интервью взяла Вероника Горячева

информационные технологии

Опасные сети

— информбезопасность —

В конце апреля основатель Facebook Марк Цукерберг объявил о первом в истории соцсети масштабном преобразовании: он пообещал, что изменится не только дизайн станицы, но и уровень конфиденциальности. К этому моменту руководство соцсети уже несколько раз признавало утечку персональных данных своих пользователей. Но если в Европе и США Facebook и другим IT-гигантам грозят серьезные штрафы за «утерю» паролей и адресов электронной почты, то в России за такое нарушение нет строгой ответственности. Параллельно с этим мир потрясают скандалы, вызванные небезопасностью интернета вещей: взламывая «умные» устройства, злоумышленники превращают их в шпионов и даже получают контроль над финансами пользователей.

РОССИЙСКИЙ РЫНОК ВЫСОКОТЕХНОЛОГИЧНЫХ ХИЩЕНИЙ

ИСТОЧНИКИ: GROUP-IB, ДАННЫЕ ЗА 2-Ю ПОЛОВИНУ 2017 — 1-Ю ПОЛОВИНУ 2018 ГОДА.

Сегмент рынка	Количество групп	Успешные атаки в день	Средняя сумма одного хищения (руб.)	Средняя сумма хищений в день (руб.)	H2 2017 — H1 2018 (руб.)
Хищения у юрлиц с троянами для ПК	3	2	1,1 млн	2,2 млн	547,8 млн
Хищения у физлиц с Android-троянами	8	100	7 тыс.	770 тыс.	191,73 тыс.
Целевые атаки на банки	3		118 млн		1303,9 млн
Фишинг	26	108	1 тыс.	1,008 млн	251 млн
Обналичивание похищенных средств				1,336 млн	919,5 млн
ИТОГО				**3,114** млн	**3214** млн

Скандал на £500 тыс.

540 млн записей пользователей Facebook стали доступны для скачивания на открытой облачной платформе Amazon, сообщила в начале апреля австралийская компания по кибербезопасности UpGuard. Названия учетных записей, действия пользователей, их лайки и другую личную информацию собирала мексиканская цифровая платформа Cultura Colectiva: эта информация хранилась в облаке Amazon. База другой, уже не работающей площадки — приложения At the Pool — содержала имена, пароли, информацию о любимых фильмах и книгах, фотографии, а также адреса электронной почты 22 тыс. пользователей соцсети. Доступ к базам был закрыт уже после того, как журналисты Bloomberg предупредили Facebook об утечке.

Штраф Facebook выписало в конце 2018 года и Антимонопольное ведомство Италии, обязав соцсеть заплатить €10 млн за использование в коммерческих целях данных своих пользователей. Затем к числу стран, которые недовольны действиями соцсети, присоединилась Турция: управление по защите персональных данных оштрафовало Facebook на $270 тыс. за нарушения конфиденциальности фотографий пользователей. При этом большую часть суммы компания должна заплатить за то, что не приняла мер после того, как получила предупреждение о нарушении закона.

В будущем соцсети могут грозить новые выплаты: в апреле расследование против Facebook начала прокуратура Нью-Йорка из-за несанкционированного хранения электронных почт и контактных данных 1,5 млн пользователей. Перед этим Facebook призналась, что может непреднамеренно загружать контакты в электронных почтах пользователей, которые регистрировались в соцсети с мая 2016 года.

Помимо ущерба компании такие утечки непосредственно влияют на безопасность пользователя. Данные — особенно те, что связаны с платежной информацией,— могут монетизировать злоумышленники, поэтому интерес со стороны киберпреступного мира к ним по-прежнему высокий, рассказывает руководитель российского исследовательского центра «Лаборатории Касперского» Юрий Наместников. Личные данные пользователей могут использовать фишеры (технически подкованные злоумышленники): имея подробную информацию о человеке, намного легче провести успешную целенаправленную кибератаку как на него самого, так и в дальнейшем попасть в сеть компании, в которой он работает, добавляет эксперт.

Радионяня-шпион

Facebook не единственный IT-гигант, который сталкивается с проблемами, связанными с защитой и хранением конфиденциальной информации. Google и ее «дочки» также вынуждены защищаться от критики, вызванной утечкой персональных данных. Камеры видеонаблюдения, радионяни, дроны, «умные» колонки, бытовые приборы с выходом в интернет — эти устройства все чаще используют семьи по всему миру. Такие гаджеты становятся новыми мишенями для хакерских атак, особенно в США, где каждый третий потребитель владеет двумя и более устройствами для «умного» дома.

На рубеже 2018 и 2019 годов Америку потрясли скандалы, вызванные взломами камер фирмы Nest (принадлежит Google), установленных в радионянях. Например, в январе в Калифорнии американка Лаура Лайонс находилась дома, когда ее «умная» камера предупредила, что на Лос-Анджелес, Чикаго и Огайо были направлены три северокорейские ракеты. В сообщении говорилось, что США принимают ответные меры, а люди в зоне поражения должны быть эвакуированы в течение трех часов. Когда Лайонс включила телевизор, чтобы узнать подробности, то не нашла никакой информации о предстоящей атаке. Ничего о ней не знали и в службе спасения. После звонка в службу поддержки Nest женщина поняла, что стала жертвой хакерского взлома.

Если злоумышленники взломают устройство «умного» дома, то они могут долгое время записывать информацию о пользователях — таким образом, помощники под управлением мошенников становятся шпионскими устройствами, предупреждает аналитик ГК InfoWatch Андрей Арсентьев. Домашний интернет вещей может быть использован для дестабилизации комфортного существования: взломав «умные» датчики температуры, злоумышленники получают контроль над изменением климата в комнате, а взломанный «умный» замок кардинально меняет свою функцию и становится отмычкой к дверям дома, отмечает он. «Страшно представить, к каким последствиям приведет внешнее управление „умным“ автомобилем или подключенным к сети кардиостимулятором»,— говорит эксперт.

После серии взломов устройств Nest в начале текущего года компания разослала своим пользователям предупреждение и попросила придумать «сильный» пароль к домашней камере видеонаблюдения и защитить ее двухфакторной аутентификацией.

Деньги пользователя могут оказаться под угрозой в том случае, если взломанные устройства интегрированы с платежными системами, при этом не требуют подтверждения трансакции, отмечают в InfoWatch. Если холодильник запрограммирован на автоматический заказ молока, то, когда в нем не останется ни одного пакета, теоретически возможно изменить параметры оплаты и совершить мошеннический платеж. Выход для пользователя здесь в использовании технологии токенизации: она позволяет совершать безопасные мобильные платежи путем шифрования данных, заключает господин Арсентьев.

Инциденты с нарушением прав пользователей в области персональных данных подтолкнули европейских законодателей начать заботиться о своих граждан: после четырех лет обсуждений в 2018 году в ЕС вступил в силу закон об усилении ответственности за нарушение в области персональных данных (General Data Protection Regulation). Санкции за его неисполнение грозят компании максимальным штрафом до €20 млн или 4% от глобального оборота компании. Из-за этого суммы, которые начали выплачивать компании, значительно выросли.

Заткнуть утечку

Говорить о том, какая индустрия больше всего страдает от утечек данных, сложно, так как личную информацию клиентов сегодня хранит и обрабатывает большое количество организаций, работающих совершенно в разных областях, говорит Юрий Наместников. При этом в России компании действительно стали аккуратнее относиться к обработке и хранению данных — это произошло после принятия законов «О персональных данных» и «О безопасности критической информационной инфраструктуры».

В 2018 году в мире наиболее громкие случаи утечек, связанные, в частности, с платежными данными пользователей, происходили в финансовых организациях и онлайн-магазинах, а также в ресторанных и отельных сетях, через которые ежедневно обрабатывают большое количество платежных данных пользователей, добавляет господин Наместников. Но защита собственных данных особенно актуальна для российских пользователей: если в Европе и США за утечку информации пользователей компаниям грозят большие штрафы, то в России такая практика еще не сложилась. И сами граждане не относятся к персональным данным с должным вниманием, и строгой ответственности за нарушение их хранения не предусмотрено, говорит адвокат Forward Legal Данил Бухарин.

Административный штраф в России значительно меньше, чем в Европе: для организации он ограничен суммой 75 тыс. руб., отмечает юрист. За весь 2018 год Роскомнадзор составил всего 30 административных протоколов в случаях, когда оператор персональных данных не обеспечил безопасные условия их хранения и это привело к неправомерному доступу к личной информации. Отдельный вид ответственности за нарушение требований к сбору и хранению персональных данных россиян — это блокировка иностранного интернет-ресурса по требованию Роскомнадзора и решению суда. Например, в августе 2016 года в России был заблокирован LinkedIn.

Более серьезные санкции предусмотрены в Уголовном кодексе, но к уголовной ответственности возможно привлечь только физических лиц. За неправомерное копирование персональных данных могут лишить свободы на срок до семи лет, однако доказать наличие состава такого преступления крайне сложно, подчеркивает господин Бухарин. Если же компания незаконно передаст третьим лицам персональные данные клиента, с нее могут потребовать возмещения убытков или компенсации морального вреда. Суды удовлетворяют подобные иски, но суммы взысканий небольшие: моральный вред оценивается не дороже 30 тыс. руб.

Ирина Юзбекова

Review

«Сила SAP — в комплексности»

В апреле представительство SAP в России и странах СНГ возглавил **Андрей Филатов,** вернувшийся в компанию после девяти лет работы в IBM. По словам топ-менеджера, в ближайшие годы SAP сможет создать в СНГ инновационные проекты, заметные и в мировом масштабе. О том, за счет чего SAP удается наращивать выручку, почему бизнес переходит на облачные сервисы и какие задачи стоят перед компанией под его руководством, он рассказал в интервью „Ъ“.

ФОТО ПРЕДОСТАВЛЕНО ПРЕСС-СЛУЖБОЙ «SAP»

— экспертное мнение —

— SAP для вас не чужая компания: вы начали работу в SAP CIS в 2007 году, возглавив подразделение по работе с клиентами, в феврале 2009-го стали руководителем «SAP Украина» и офиса в Казахстане. Но через год ушли в IBM. Теперь вы снова в SAP. Почему?

— Девять с лишним лет, которые я был вне SAP, достаточно долгий и важный этап как для предприятия, так и для страны. Я бы не сказал, что вернулся в ту же самую компанию. Сейчас другая ситуация, у меня абсолютно другая роль.

Я всегда относился к SAP с большим уважением и, уходя, сохранил связи и контакты. Возвращение было логичным, легким, так как я вернулся в хорошо знакомую мне среду.

— В должность главы SAP CIS вы вступили 15 апреля. По сути, прошел только месяц с того момента, как вы заняли позицию гендиректора. Вошли в курс? Какие задачи перед вами стоят?

— Месяц прошел очень насыщенно, мне нужно было в очень сжатые сроки войти в курс всех дел. Я прекрасно понимал, что у меня будет непростой стартовый период, компания занимает ведущие позиции на рынке, а чтобы быть в курсе и сразу вовлечься в работу, требуются большие усилия. Задачи — не только сохранить темп и результаты прошлого года, но и мыслить более амбициозно.

— По данным финансового отчета за 2018 год, подразделение SAP в СНГ и РФ, несмотря на санкции и ухудшение экономической ситуации в стране, сумело увеличить выручку и даже расширить штат сотрудников. Выручка составила €472,5 млн против €468,4 млн в 2017 году, прибыль за год выросла втрое — €23,1 млн против €8,7 млн в 2017 году. Что стало главными драйверами роста в минувшем году?

— Здесь нельзя говорить о какой-то одной причине, скорее о комплексе. Мы здесь давно, у нас значительно расширился портфель решений, это не только ERP, но и управление кадрами, поведением клиентов, существенно выросло количество аналитических решений. Спрос на них огромен.

К тому же цифровая экономика требует своих инструментов. Рынок существует в непростых экономических условиях, которые заставляют компании бороться за эффективность.

Глобально идет активное перемещение бизнеса в облака — нам, безусловно, очень помогает наличие в Москве собственного ЦОДа. Этот бизнес идет по нарастающей: все больше клиентов выбирают облако — это и определенная зрелость рынка, и клиентов.

— Какой рынок из числа ближнего к России зарубежья наиболее интересен с точки зрения ведения бизнеса? Чем отличаются партнеры и клиенты SAP в СНГ от российских?

— На протяжении своей карьеры я очень много времени занимался именно странами СНГ. Многие проекты, которые мы запускаем в России, через некоторое время повторяем в других странах. Российский рынок же, наоборот, очень часто бывает первопроходцем: мы периодически внедряем решения первыми в мире. Надеюсь, что на ПМЭФ расскажем еще об одном таком проекте.

Сейчас в СНГ власти меняют свое отношение к цифровизации и IT, а так как у них нет большого количества устаревших решений, здесь они могут себе позволить внедрять самые передовые технологии с нуля. Наш приоритет — Казахстан, Беларусь, Азербайджан и Узбекистан. Узбекистан, кстати, переживает большие изменения. Мы уже говорили о нескольких проектах по цифровизации крупнейших банков, в том числе «Ипак Юли».

— Какова структура российской выручки SAP по итогам 2018 года? Насколько она неизменна от года к году? Из чего состоит бизнес SAP в РФ?

— Доходы ERP-бизнеса уже не являются основными. Из отраслей можно выделить металлургию, добычу. А также сектор быстрорастущих компаний, который раньше не ассоциировался с нами. Мы видим здесь хорошую динамику и фантастические проекты. Например, завод-робот «Черкизово». Представьте себе производство, где вместо 700 человек работают 200. Все процессы производства — от склада сырья и до упаковки — работают автономно. При этом завод может закрыть 30% российского спроса на сырокопченую колбасу.

— Результаты SAP в СНГ и РФ идут вразрез с объявленным властями курсом на импортозамещение в сфере IT. Казалось бы, при такой политике финансовые результаты иностранных компаний должны падать. В чем парадокс?

— Сила SAP в комплексности. Наши решения отвечают условиям по масштабированию, обработке больших объемов данных, отказоустойчивости и хранения данных, ведь от их качества зависит не просто бизнес, а ключевые для экономики направления. Мы можем дать сквозное решение компании любого размера и любой индустрии: от нескольких магазинов до миллионов сотрудников.

— SAP является автором концепции «интеллектуального» предприятия, идея которой заключается в передаче компанией всех действий, обычно выполняемых человеком, технологиям. Есть примеры с клиентами в России?

— Ключевая идея «интеллектуального» предприятия — объединение всех систем и данных — и на ERP и на MES-уровнях — на базе единой платформы, где все работает в режиме реального времени, поддерживается такими технологиями, как машинное обучение, блокчейн, предиктивная аналитика и т. д.

На наш взгляд, потенциально строить интеллектуальное предприятие могут все компании, перешедшие на новую платформу SAP S4/HANA — цифровое ядро, основа будущего интеллектуального предприятия. В России их уже более 30. К примеру, «Металлоинвест», «Крастцветмет», АСГ, «Валента Фарм», «Аэроэкспресс» и другие.

— На вопрос „Ъ“ о прогнозах по развитию IT-отрасли в 2019 году и точках роста ваш коллега из «Ланита» Филипп Генс ответил, что будут развиваться и интеграция, и консалтинг — то, что связано с реализацией программы «Цифровая экономика» и цифровизацией бизнеса. Согласны с ним? Какими вам видятся тренды и точки роста рынка в 2019 году?

— Согласен. На мой взгляд, это очень мощное сочетание, при успешной реализации может трансформировать целые отрасли: телеком, ритейл, банки. Говоря о трендах, я бы еще выделил облака. Уже несколько лет мы фиксируем трехзначный рост направления. Еще одной из заметных тенденций на рынке стало формирование нового типа экосистем: на базе новых технологий создаются маркетплейсы, более жизнестойкие бизнес-взаимодействия. У нас как раз есть все инструменты для реализации таких экосистем.

— Среди ваших партнеров в России — крупнейшие участники рынка, такие как «Ростелеком», «Яндекс», «Лаборатория Касперского». Как продвигаются технологические партнерства SAP с российскими компаниями? Какие совместные проекты вы делаете с ними и другими игроками, что из этого можете особо выделить?

— Со всеми этими клиентами мы продолжаем проекты, динамика разная.

Сейчас мы поменяли формат, открываем с клиентами совместные лаборатории. С НЛМК мы создали первую в мире систему 3D-позиционирования сотрудников в условиях производственного объекта — агрегата непрерывного горячего цинкования. Сейчас еще с несколькими клиентами обсуждаем открытие лабораторий, в том числе для работы над сценариями «цифровых двойников».

— SAP выводит российские разработки на глобальный рынок через свой глобальный прайс-лист. Какие из этих разработок наиболее значимы и важны для SAP, какие успехи у них на мировом рынке?

— По данным IMD World Digital Competitiveness, Россия сейчас занимает 42-е место в мировом рейтинге цифровизации, доля цифровой экономики в ВВП России — 3%. Но у страны есть потенциал, сохранилась прекрасная матшкола. Наши сильные стороны — аналитика, решения для кибербезопасности. Эти направления как раз критически важны для развития Индустрии 4.0. У российских компаний есть решения в основных отраслях, например нефтянке. Мы внесли в свой глобальный прайс-лист первое российское решение — UFAM — после их перехода на нашу платформу.

Оно востребовано в России и СНГ, ведутся переговоры в Европе, на Ближнем Востоке, в Северной Африке. У нас есть еще предложения и идеи о том, как можно продвигать российское ПО за рубеж. Сейчас мы ведем переговоры с еще несколькими компаниями, которые также хотели бы попасть в наш прайс-лист.

— Если не ошибаюсь, в России работает центр интернета вещей SAP, который занимается сценариями для внедрения IoT для нашей страны. Какие сценарии вы уже внедрили? Какие — в планах?

— Да, в 2016 году был открыт Центр интернета вещей в московском офисе SAP Labs. Главная задача — разработка сценариев для различных отраслей: промышленной и сырьевой индустрии, сельского хозяйства и животноводства, транспорта и многих других. Мы активно работаем с клиентами. Одна из крупнейших сельскохозяйственных компаний в России уже использует наш мониторинг данных на всех этапах: от посева и выращивания культур до их сбора, а также для контроля за расходом горючего и химикатов.

— О каком объеме инвестиций SAP в российский рынок может идти речь за год?

— SAP — один из немногих мировых вендоров, которые вне зависимости от политических изменений продолжают инвестировать в российскую экосистему, и инвестиции эти измеряются миллионами евро. В прошлом году мы открыли Центр цифрового лидерства, инвестиции в его строительство составили €20 млн. На обучение партнеров в прошлом году потрачено около €3 млн.

— Власти провозгласили курс на построение цифровой экономики, принята соответствующая национальная программа. Насколько масштабным является сотрудничество SAP с российским государством в этой истории?

— Сейчас мы «цифровой акселератор» для российского бизнеса, мостик в единую мировую цифровую экономику.

Одной из важных инициатив мы считаем GRID — совместную инициативу по цифровизации российской экономики. В рамках проекта мы участвуем в экспертных группах и ассоциациях, разрабатываем новые решения и адаптируем концепцию Индустрии 4.0 под специфику бизнеса в России.

Интервью взял
Роман Рожков

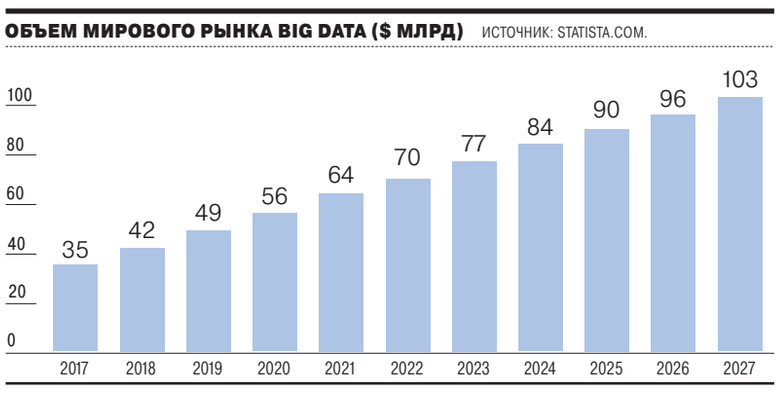
информационные технологии

Сага о Big Data

— большие данные —

Использование технологий Big Data (больших данных) в бизнес-процессах стало сегодня неотъемлемой частью цифровизации не только отдельных корпораций или отраслей, но и экономики в целом. По данным IDC, к 2020 году мировой объем рынка больших данных превысит $200 млрд, и нет ничего удивительного в том, что власти обратили внимание на такую динамично развивающуюся индустрию. У России есть неплохие шансы стать одним из мировых центров Big Data — понимая это, президент Владимир Путин поручил до конца года утвердить генеральную схему развития сетей связи и инфраструктуры хранения и обработки данных. Впрочем, насколько отрасль нуждается в регулировании и каковы шансы нашей страны стать глобальным лидером на этом рынке — вопрос все еще открытый.

ОБЪЕМ МИРОВОГО РЫНКА BIG DATA ($ МЛРД) ИСТОЧНИК: STATISTA.COM.



Big Data идет на выручку

Задача Big Data — анализировать доступные данные, вычислять тренды и корреляции между, казалось бы, не связанными между собой событиями. По консолидированному прогнозу аналитиков, рынок больших данных в России к 2024 году достигнет как минимум 300 млрд руб., сейчас, по разным оценкам, он составляет от 10 млрд до 30 млрд руб. Общий экономический эффект и рост выручки всех индустрий в России за счет использования результатов обработки Big Data в среднесрочной перспективе составит от 1,5% до 3% ВВП, подсчитали в Ассоциации участников рынка больших данных (АУРБД).

Пока в России наиболее активными участниками рынка больших данных являются компании телекомсектора, интернет-компании, банки и ритейл. Наибольший вклад в бизнес пока вносит применение аналитики с использованием больших данных, а не продажа услуг на основе Big Data в чистом виде. Так, удаленная цифровая идентификация, проверки, предсказательные модели на основе больших данных — все это снижает издержки, связанные с мошенничеством, на 15–20% в зависимости от используемых технологий, отмечает гендиректор IDX Светлана Белова.

Аналитика больших данных способствует развитию конкуренции, а это один из наиболее мощных драйверов экономики, отмечает глава дирекции аналитических и индустриальных решений «SAS Россия/СНГ» Александр Ефимов. По его словам, цифровизация позволит по-новому взглянуть на те стороны экономики страны, которые до этого оставались в тени: например, на рынок аренды: «Механизмы нелегальной сдачи квартир планируется отслеживать с помощью больших данных и анализа крупных интернет-ресурсов, после чего обязывать арендодателей уплачивать законный налог». Сегодня государство — уже крупнейший владелец данных о своих гражданах и организациях, напоминает президент АУРБД и член совета директоров «МегаФона» Анна Серебряникова: «Однако потенциал коммерческого использования обезличенных данных, которые можно получить из государственных информационных систем и других источников, пока не раскрыт».

Данные в беззаконье

Вместе со стремительным развитием технологий сбора и обработки Big Data возникает вопрос о защите прав и свобод субъектов персональных данных, то есть простых интернет-пользователей, клиентов банков и абонентов сотовых операторов. Один из наиболее ярких примеров связан со скорингом. На основании вольного толкования информации из соцсетей человеку могут отказать в открытии счета или не дать кредит, отмечает Светлана Белова.

Сейчас в России существуют понятия разных типов данных: это и персональные данные, и так называемые открытые данные, и данные, доступ к которым ограничен, в том числе данные, содержащие различные виды тайн. Но четкого понимания, что из этого может считаться Big Data, что — свободно собираться и обрабатываться, а что требует особой защиты, нет, отмечает директор по правовым инициативам Фонда развития интернет-инициатив (ФРИИ) Александра Орехович. В России назрела необходимость регулирования этой сферы, в том числе Big Data, убеждена она.

С точки зрения регулирования большее беспокойство вызывает использование больших данных в тех аспектах, где они пересекаются с данными персональными, говорит руководитель технологической практики в риск-консалтинге КПМГ в России и СНГ Николай Легкодимов. У Google был проект, связанный с ранним обнаружением эпидемий, приводит пример он: «По нему предлагалось анализировать утреннюю переписку людей с родственниками или коллегами и выявлять жалобы на самочувствие. Такие информационные сигналы появляются гораздо раньше, чем люди приходят в поликлиники, и это критически важно для раннего реагирования и предотвращения распространения заболевания». Это пример того, как технология может реально сохранить человеческие жизни, но из-за нарушения прав человека в области персональных данных она не используется, говорит господин Легкодимов.

Регулировать нельзя оставить

Считая саморегулирование больших данных недостаточным, власти настаивают на регулировании этой сферы. Законопроект, закрепляющий определения больших пользовательских данных, их оператора и вводящий правила их обработки, был внесен в Госдуму еще в октябре 2018 года депутатом от «Единой России» Михаилом Романовым. Однако отрасль раскритиковала документ: по мнению экспертов, это увеличит нагрузку на бизнес и может усугубить технологическое отставание России. В результате комитет Госдумы по информполитике решил вернуть законопроект его автору.

Помимо этого, в госпрограмме «Цифровая экономика» предусмотрена разработка законопроекта, устанавливающего правила и порядок доступа к общедоступным данным. Минэкономики планировало внести документ в правительство до конца 2018 года, но он так и не был подготовлен. Власти рассматривали три концепции регулирования. Первая закрепляла за площадкой, собирающей данные, права на управление размещенными на ней данными. Модель поддерживали крупные игроки. Вторая концепция предусматривала свободную обработку общедоступных данных, размещенные на платформах без согласия их субъектов. Это было бы выгодно стартапам, которые зарабатывают на сборе данных и оказании услуг по их анализу.

Третий вариант не предусматривал введения дополнительного регулирования, а ограничивался введением дополнительных соглашений между крупными интернет-площадками и третьими лицами. Но власти до сих пор однозначно не определились в выборе модели. Сейчас концепцию управления данными готовит центр компетенций «Сколково», а предложения к ней были подготовлены АНО «Цифровая экономика».

Бизнес борется за Data

Параллельно с инициативами в части регулирования выступают и другие бизнес-объединения. Так, в январе ФРИИ подготовил законопроект, вводящий в законодательство термин «персонализированные данные» и предлагающий обеспечить их свободное обращение на рынке. Иными словами, граждане смогут предлагать бизнесу свои данные с определенной целью и сроками за вознаграждение в различных формах и тем самым зарабатывать до 60 тыс. руб. в год. Пользователь сам должен распоряжаться своими данными, решать, кому их передавать, согласна Светлана Белова. «Для этого надо предоставить гражданину удобный интерфейс для доступа к своим данным, хранящимся в ГИСах и у бизнеса, как это уже реализовано у „ВКонтакте“, Facebook, Telegram и других платформ», — считает она. «Все, что может привести к возможности нарушения прав и свобод владельцев персональных данных, должно быть четко урегулировано, в том числе их оборот, а все, что касается собственно данных, которые не могут содержать информацию ограниченного доступа, в том числе персональных данных, очевидно, может быть отдано на откуп отрасли,— полагает Александра Орехович.

Созданная в октябре прошлого года АУРБД (объединяет «Ростелеком», «Яндекс», Mail.ru Group, Сбербанк, Газпромбанк, Тинькофф-банк, «МегаФон», oneFactor и Qiwi), напротив, выступает за саморегулирование в сфере оборота Big Data. «Мы совместно с Институтом развития интернета готовим кодекс использования данных, который станет обязательным для всех участников организации»,— напомнила Анна Серебряникова. По ее словам, он должен стать актом отраслевого саморегулирования, закрепляющим не предусмотренные законодательством правила работы с массивами данных.

По оценке Николая Легкодимова, основная опасность в регулировании этой сферы заключается как в расширительном толковании того, что такое большие данные по отношению к человеку, так и в возможности выводить приватную информацию о человеке исходя из данных, которые сами по себе персональными не являются. Объемы обработки Big Data и современные механизмы позволяют, например, на основе знаний о районе проживания и истории пары покупок идентифицировать человека с точностью до ФИО, отмечает он: «В США были случаи, когда использование таких технологий приводило к поимке преступников». В то же время, если говорить о России, в силу модели взаимодействия гражданина и государства наши власти всегда будут стремиться к тому, чтобы быть владельцем и контролером таких данных, считает он: «Это неудивительно, ведь, например, аналитикой, которую дают телекомкомпании, можно пользоваться для управления электоратом». Именно в таком скрытом влиянии на предвыборный процесс обвиняют Cambridge Analytica и сторонников «Брексита», напоминает эксперт.

Юлия Тишина

контур.фокус API

Пираты не испугались «черной метки»

Летом россияне часто сталкиваются с проблемой выбора сериала или фильма: телеканалы показывают в основном старый контент. На ТВ межсезонье — зрители разъезжаются, рекламы становится меньше, и выпускать новые передачи становится бессмысленным. В итоге зрители скачивают фильмы и сериалы с торрент-трекеров или смотрят видео в онлайне — и часто на пиратских сайтах. И рынок, и законодатели такой ситуацией недовольны и разрабатывают все больше инициатив, которые должны остановить пиратство. Впрочем, эффективной борьбу с нелегальным контентом пока все же назвать не получается.

— онлайн-видео —

ФИЛЬМЫ, НЕЛЕГАЛЬНЫЕ КОПИИ КОТОРЫХ НАИБОЛЕЕ ЧАСТО БЛОКИРОВАЛИСЬ В 2018 ГОДУ

ИСТОЧНИКИ: WEBKONTROL, «БЮЛЛЕТЕНЬ КИНОПРОКАТЧИКА».

Фильм	Количество заблокированных сайтов	Дата выхода	Дистрибутор	Сборы в РФ (млн руб.)
«Красный воробей»	20	31 мая 2018	Fox	**144,1**
«Щелкунчик и четыре королевства»	20	8 декабря 2018	WDSSPR	**390,4**
«Тихое место»	20	12 апреля 2018	«Централ Партнершип»	**321,5**
«50 оттенков свободы»	20	8 февраля 2018	UPI	**684,7**
«Великий уравнитель-2»	20	6 сентября 2018	WDSSPR	**201**
«Мстители: Война бесконечности»	19	3 мая 2018	WDSSPR	**1882,5**
«Аквамен»	12	13 декабря 2018	«Каро Премьер»	**832,5**
«Лига справедливости»	12	16 ноября 2017	«Каро Премьер»	**626,4**
«Первому игроку приготовиться»	12	29 марта 2018	«Каро Премьер»	**734,2**
«Звездные войны: Последние джедаи»	10	14 декабря 2017	WDSSPR	**872,2**
«Дэдпул-2»	5	17 мая 2018	Fox	**1240,2**

По данным GlobalWebIndex на начало 2019 года, на видеопросмотр приходится огромная доля интернет-трафика, хотя бы раз в месяц видео смотрят 92% пользователей. Годом ранее агентство BrandScience (входит в Media Direction Group) подсчитало, что россияне в среднем тратят на просмотр видео 4 часа 20 минут в день. И хотя на ТВ пока приходится большая часть времени, драйвером выступает все же онлайн-просмотр. При этом платить за контент готовы немногие. В BrandScience говорят, что покупают видео не более 10% россиян. Для сравнения: торрент-трекерами пользуются 60% опрошенных.

Есть и хорошие новости: несмотря на пиратство, российский рынок легального видео активно растет. В 2018 году видеосервисы заработали 25 млрд руб., что на 56% больше, чем в 2017-м (данные J'son & Partners Consulting). По сравнению с мировым рынком это крохи (доля России оценивается только в 0,6%), но динамика роста положительная. Настоящий триумф отрасли случился в 2017 году: тогда доходы онлайн-кинотеатров от платной модели впервые превысили объем рекламных поступлений. По итогам прошлого года доходы онлайн-кинотеатров от показа рекламы составили 3,6 млрд руб., а от пользовательских платежей — уже 7,9 млрд руб.

Онлайн-кинотеатры хотят большего

Во многом благодаря активной позиции рынка российские власти все чаще обращают внимание на борьбу с пиратством. Так, в марте Роскомнадзор сообщил о разработке нового закона о защите авторских прав в интернете. Он будет основан на антипиратском меморандуме, подписанном в конце 2018 года правообладателями, поисковиками и видеохостингами.

Суть меморандума — в появлении специального реестра, куда правообладатели могут вносить ссылки на пиратские ресурсы. Затем поисковики должны удалять эти страницы из выдачи во внесудебном порядке. Меморандум возник, поскольку правообладатели были недовольны действующим антипиратским законом. Возможность через суд блокировать сайты с нелегальным контентом появилась в 2013 году, а с 2017 года вступил в силу закон «о зеркалах», который разрешал внесудебную блокировку копий пиратских сайтов. Однако система оказалась неэффективной, потому что зеркала появлялись быстрее, чем выдавались судебные приказы.

Однако с момента подписания меморандума ситуация радикально не изменилась, указывают гендиректор «Megogo Россия» Виктор Чеканов и директор по контенту tvzavr Елена Хлебникова. На верхних позициях поисковой выдачи попрежнему находятся ссылки на пиратские ресурсы. Хотя меморандум работает, пока что его действие не так эффективно, как того ожидали правообладатели, признает замгендиректора онлайн-кинотеатра ivi по правовым вопросам Михаил Платов. В качестве сдерживающей силы выступает сам «Яндекс»: поисковик удаляет пиратов из выдачи, но предоставляет им инструменты «склейки» аудитории удаленной из выдачи страницы сайта с только что созданной. И хотя в день может удаляться несколько десятков страниц, на их месте появляются новые, с тем же содержанием и, соответственно, аудиторией.

Искоренить проблему пиратства соглашение не способно, поскольку необходимы и другие инструменты, считает заместитель руководителя департамента инновационной защиты бренда и интеллектуальной собственности Group-IB Дмитрий Тюнькин. Среди них — уголовное преследование пиратов за противоправную деятельность, блокировка трансакций, связанных с пиратским бизнесом, минимизация партнерских программ, предполагающих сотрудничество с пиратами, фильтрация сайтов-партнеров со стороны рекламных сетей, вытеснение прямых рекламодателей с рынка (например, онлайн-казино).

Пиратские интересы

Хотя от пиратства страдают не только правообладатели видеоконтента, о проблемах видеопиратства в России просто исторически говорят больше, отмечает Дмитрий Тюнькин. К тому же потребление онлайн-видео стремительно растет, а за ним и количество пиратских копий. Наконец, именно видеопиратам удалось привлечь на свои площадки серых и черных рекламодателей и зарабатывать большие деньги.

Наибольшим спросом у пиратов пользуются, безусловно, новинки. Так, по данным Group-IB, почти каждая кинокартина, вышедшая в 2018 году в прокат, была скопирована пиратами и выложена в сеть. Руководитель юридического отдела WebKontrol Алена Кузьмина указывает, что в 2018 году пираты размещали в сети от 2 тыс. до 8 тыс. нелегальных ссылок по каждой крупной кинотеатральной премьере.

Новые фильмы появляются на пиратских сайтах простым способом: посетители снимают на видео экран кинозала. Делать запись получается незаметно благодаря развитию смартфонов, раньше приходилось снимать на видеокамеры. Конечно, кинотеатры тоже борются с пиратами и устанавливают специальное оборудование, позволяющее обнаружить съемку. Но пираты часто платят за запись пенсионерам или несовершеннолетним, наказывать которых за съемку никто не станет. В результате экранная копия может появиться на пиратских сайтах уже в день премьеры, что позволяет злоумышленникам зарабатывать огромные суммы. Новинки привлекают пользователей, аудитория пиратских сайтов после размещения релиза растет, а значит, увеличиваются и рекламные доходы.

Добросовестные рекламодатели не относят свои бюджеты пиратам, но этого и не требуется: основным источником дохода для пиратов стали онлайн-казино и незаконные букмекерские конторы. Сами они не могут размещаться на легальных сайтах, поэтому продвигают свои сервисы с помощью пиратов. Рекламные бюджеты у таких компаний огромные, свидетельствуют данные Mediascope. Так, в 2018 году крупнейшим рекламодателем в сегменте онлайн-видео стало казино Azino777.

Как ранее подсчитывали в Group-IB, в среднем за каждую тысячу просмотров пираты зарабатывают $3, и среднемесячный доход крупных площадок может составлять $10 тыс. Окупается бизнес быстро: на создание сайта уходит около $240, и выйти в ноль можно после 80 тыс. просмотров. В WebKontrol указывают, что благодаря антипиратским мерам в России остались единицы нелегальных ресурсов с более чем 10 млн посещений в месяц, так что пираты теряют прибыль от рекламы. С другой стороны, в этой статистике не отражены доходы «зеркал» пиратских сайтов.

Сериальный контент тоже привлекает пиратов, обращает внимание гендиректор Amediateka Дмитрий Сычугов. Для своего сервиса явным лидером среди сериалов по запросам он называет «Игру престолов». В апреле вышел новый — и последний — сезон ставшего культовым сериала HBO, и он «пиратится» очень активно, причем во всем мире, говорит господин Сычугов. Поэтому сейчас сервис делает максимальный акцент на защите «Игры престолов» от пиратов с помощью Group-IB. В последней напоминают, что пиратство не ограничивается показом отдельных фильмов или сериалов — существует, например, нелегальный стриминг целых телеканалов. Такие пираты предлагают большие библиотеки каналов за небольшие цены — 30–50 руб. в месяц.

Искоренить нельзя минимизировать

Искоренить пиратство окончательно вряд ли удастся, признают эксперты. Но свести к минимуму вред от нарушения авторских прав можно, например, если сделать «немодным» использование торрентов, считает Дмитрий Сычугов. Поскольку наказывать конечного пользователя нелегального контента в России нельзя, Amediateka использует судебные ресурсы: сервис является одним из лидеров по числу исков к пиратским сайтам. Штрафы же вряд ли можно назвать эффективной мерой по борьбе с пиратством, сомневается господин Сычугов.

В WebKontrol, как и в Group-IB, считают, что необходим комплекс мер и воздействие как на пиратов, так и на потребителей контента. Например, в России сейчас действует штраф 500–700 тыс. руб. за неудаление ссылок на вечно заблокированные сайты, но этого недостаточно, говорит Алена Кузьмина. Дмитрий Тюнькин предполагает, что бороться с пиратством стоит с помощью создания легальных предложений для зрителей и, с другой стороны, вводя жесткие меры по отношению к пиратам, вплоть до уголовного наказания. Штрафы же для пользователя — перспектива неясная со всех сторон, поскольку они снижают покупательскую способность и отбивают желание приходить на легальный портал, рассуждает он. Кроме того, выявление каждого пользователя, посмотревшего определенный контент на определенном сайте, не самая простая задача с технической точки зрения, заключает эксперт.

Защищать авторские права поможет развитие легальных сервисов, согласна Елена Хлебникова. Так, драйвером роста онлайн-кинотеатров стал Smart TV, ведь через него нелегальный контент смотреть крайне неудобно. Большую роль играет и информационный фон: еще четыре-пять лет назад никто не знал, что такое онлайн-кинотеатры и чем они отличаются от пиратских ресурсов. Сегодня же большая часть населения осознает разницу.

Есть и менее тривиальные подходы к решению проблемы. Часто пираты с помощью специальных программ упрощают и автоматизируют копирование постеров, описаний и рейтингов фильмов из разных источников, указывает директор по развитию компании Variti (специализируется на информбезопасности) Эдуард Макаров. И если эту возможность блокировать, то работа пиратов значительно усложнится.

Интересно, что все участники рынка единогласно заявляют: для дальнейшей борьбы с пиратством необходимо законодательно закрепить антипиратский меморандум. Получается, что формальная поддержка государства должна привести к более эффективной работе документа, чем его существование в статусе договора правообладателей и поисковиков. Впрочем, такую позицию можно понять. Развитие сервисов — дело хорошее, но оно не всегда способно превзойти одно из основных преимуществ пиратских сайтов — оперативность. Все же в онлайн-кинотеатрах фильмы появляются значительно позже дня премьеры.

Елизавета Макарова

Проверка на прочность

— интеллектуальный сервис —

Ведение бизнеса в России сродни прогулке по минному полю: зачастую не подозреваешь, какие угрозы скрыты от глаз партнеров. Роль взрывного устройства может исполнить целая россыпь факторов — как коммерческих, так и налоговых. Бывает, что от действий (или бездействия) контрагентов зависит существование компании, которая, как сапер из поговорки, может ошибиться только один раз. Свести риски к минимуму позволит комплексная проверка партнера, а помочь в этом могут такие сервисы, как «Контур.Фокус» — проверить контрагента, оценить его благонадежность и в случае проблем незамедлительно информировать компанию для принятия решения, адекватного ситуации.

Предприниматели могут поспорить с тем, что риск — благородное дело. Для них риск сопровождает бизнес постоянно в формате «24 на 7». Неплатежеспособность покупателей, ведущая к дефициту оборотных средств и кассовым разрывам. Возможные ошибочные выводы о собственном положении на рынке из-за отсутствия сведений о показателях конкурентов. Неисполнения обязательств «плохим» поставщиком.

Коммерческие риски сопровождаются налоговыми, особенно опасными в свете ужесточения налогового контроля в последние годы: практически 100% налоговых проверок приносят результат в виде доначислений и штрафов в бюджетную копилку. Реальные угрозы компаниям несут проблемные контрагенты: если деловой партнер окажется фирмой-однодневкой или не платит налоги, то по сделкам с таким «партнером» налоговики могут отказать в вычетах НДС. Или «снимут» расходы по налогу на прибыль, если сочтут, что занижена налоговая база. По сути, компания окажется в ответе за чужие грехи и проблемы «партнера» станут ее проблемами. Такой подход закреплен Высшим Арбитражным судом еще в октябре 2006 года, когда судьи ввели понятия необоснованной налоговой выгоды и должной осмотрительности.

Чтобы минимизировать риски, компания обязана проверять благонадежность партнеров. При этом бизнес вынужден опираться на множество разъяснений Минфина и ФНС, выводы судов и рекомендации консультантов. Вот далеко не полный список необходимых действий по проверке надежности контрагента: запросить выписку из ЕГРЮЛ (ЕГРИП), запросить копию свидетельства о постановке на налоговый учет, устав, справку из налоговой инспекции об уплате налогов, доверенности и другие документы, подтверждающие полномочия его представителей, проверить наличие судебных исков, поинтересоваться финансовой отчетностью (если получится). Убедиться, что потенциальный деловой партнер располагает необходимым персоналом и производственными мощностями для исполнения контракта. Обрести уверенность в том, что контрагент не управляется, как описывали классики, «зицпредседателем Фунтом».

Процесс проверки весьма трудоемкий, затратный, требующий специальных знаний и персонала. Очевидно, что в дальнейшем добытые сведения могут устареть, ситуация — измениться, а значит, однократной проверкой дело не ограничится. Если же у клиента, к примеру, появились финансовые трудности или он признан банкротом, отреагировать на это в нужный момент для бизнеса просто необходимо, поэтому за контрагентом придется «присматривать» постоянно.

Значительно снизить трудозатраты, попутно исключив человеческий фактор и возможные ошибки, которые могут дорого обойтись компании, позволяют специальные программы для проверки контрагентов, такие как «Контур.Фокус» от екатеринбургского «СКБ Контур», одного из первых в России разработчиков облачного софта. Все вышеперечисленные действия займут одну минуту вместо как минимум 40 минут на одного контрагента при ручном контроле.

С помощью API сервис встраивается в 1С или другую учетную систему (ERP, CRM, ABS, СЭД). Агрегируя информацию (бухгалтерская отчетность, картотека судебных процессов, товарные знаки, госконтракты, лицензии, санкционные списки и т. д.) из 32 официальных источников (ФНС, Росстат, ФССП, ФСРАР, Роспатент, арбитражные суды и др.), «Контур.Фокус» закрывает потребности специалистов в сфере безопасности, финансистов, юристов, сотрудников коммерческого блока компании. Это тот случай, когда технологии действительно развязывают руки персоналу для более сложных и творческих задач, избавляют от рутинных действий.

По итогам анализа отчетности сервис формирует экспресс-отчет с заключением о финансовом состоянии будущего контрагента, это существенно упрощает принятие решения о сотрудничестве с ним. В сервисе реализована система маркеров, позволяющая пользователю увидеть существенные изменения — например, началась процедура банкротства или ликвидации, предъявлен иск на крупную сумму, сменился собственник или руководитель. Маркеры работают по принципу светофора: «зеленый» — контрагент благонадежен, «желтый» — нужна дополнительная проверка в конкретной области, «красный» — контрагент уходит в стоп-лист. Для отслеживания рисков система предлагает более 80 готовых критериев, но компания может задать и собственные параметры.

Задача таких программ, как «Контур.Фокус»,— поддерживать честный и прозрачный бизнес, вести к оздоровлению рынка, помогая формировать благоприятную среду для развития экономики и укрепления хозяйственных связей между разными странами. Сейчас его функционал позволяет проверять компании не только в России, но и в Белоруссии, Казахстане и на Украине. В планах — дальнейшее расширение географии, что позволит ликвидировать информационные барьеры при международном сотрудничестве.

Киберспорт на вырост

— обзор рынка —

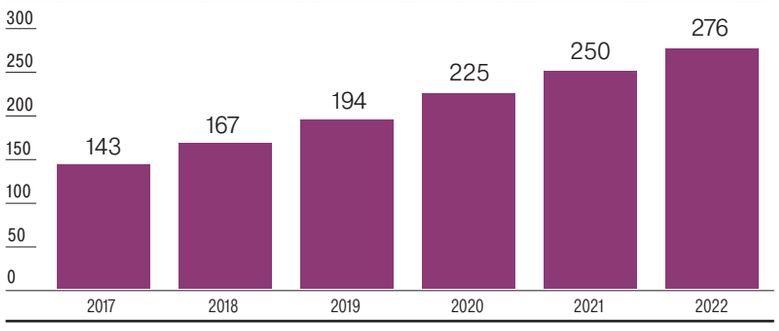
с13 Представитель «Яндекса» отметил лишь, что компания заинтересована в увеличении количества киберспортивного контента, доступного для зрителей в «Яндекс.Эфире». На данный момент в России нет компаний, которые готовы покупать права на трансляцию на чемпионат мира по Dota 2, несмотря на ее «огромную аудиторию», полагает Иван Возняк. По его мнению, продажа прав на трансляции турниров может стать точкой роста и для компании, и для всей игровой отрасли. «Необходимо научиться объяснять бизнесу, как использовать тот или иной киберспортивный актив для своего развития»,— указывает он.

Поиск спонсора

По словам представителя киберспортивного холдинга ESforce (владеет Virtus Pro) Ярослава Мешалкина, 70–80% выручки группа получает от спонсорства турниров, команд и рекламы. Оставшаяся доля формируется из доходов от организации турниров и медиапроектов «под ключ», продажи билетов, медиаправ и других источников прибыли, поясняет он. По его словам, это типичная для киберспортивного рынка модель монетизации. В 2019 году ESforce не планирует каких-то кардинальных изменений, говорит господин Мешалкин.

ДИНАМИКА РОСТА АУДИТОРИИ КИБЕРСПОРТА В МИРЕ (МЛН ЧЕЛ.)

ИСТОЧНИКИ: NEWZOO, GOLDMAN SACHS GLOBAL INVETSMENT RESEARCH.



Еще один из вариантов монетизации — привлечение инвестора, рассказывают участники рынка. «Мы могли продать 100% компании и заработать, но это не укладывается в нашу стратегию»,— сообщил „Ъ“ представитель казахстанской организации Avangar (включает составы по PlayerUnknown's Battlegrouds и Counter-Strike: Global Offensive). То, к чему идут многие участники рынка,— это продажа части бизнеса и получение средств на дальнейшее развитие, поясняет Алексей Кондаков.

Киберспорт — это быстрорастущий бизнес, но, к примеру, мультигейминговые клубы зачастую убыточны, сетует менеджер. По его словам, государство должно оказать поддержку этому виду спорта. «Как это конкретно будет выглядеть (кредиты, гранты и т. д.) — вопрос технический, главное, чтобы поддержка была финансовой, потому что зарплаты в профессиональных клубах высокие, рынок зарплат раздут в СНГ. Если ты хочешь играть на этом рынке, то должен играть по его правилам»,— заключает он.

Игры со стратегами

Крупный бизнес подключился к развитию киберспорта несколько лет назад. В октябре 2015 года фонд Алишера Усманова USM Holdings вложил $100 млн в клуб Virtus.pro, позднее он стал основой киберспортивного холдинга ESforce, в 2016 году к числу активов присоединилась немецкая киберспортивная организация SK Gaming. В 2018 году ESforce купила Mail.ru Group, а контроль над SK Gaming в начале этого года получили автомобильный концерн Daimler и футбольный клуб «Кельн».

В 2017 году сегмент привлек и сотовых операторов. Так, МТС купила клуб Gambit Esports за 220 млн руб. Осенью 2018 года Moody's в своем отчете упоминало киберспорт в качестве одного из рынков, на который выходят операторы для поддержания роста, и допускала вероятность продолжения этого тренда. Так и случилось: в марте МТС и Tele2 запустили собственные онлайн-платформы для трансляции киберспортивных турниров. Интерес к российскому рынку киберспорта объясним: в ближайшие годы он будет расти в среднем на 20% ежегодно, в текущем году его объем достигнет $55 млн, в 2023 году превысит $100 млн — такие оценки приводила в МТС в марте.

В 2017 году РБК писал, что «Ростелеком» готов инвестировать в проекты в сфере киберспорта и обсуждает сделку с командой Vega Squadron. По словам Алексея Кондакова, у него с «Ростелекомом» была только одна встреча, на которой он презентовал спонсорские пакеты. «Мы хотели, чтобы „Ростелеком“ нас поддержал как-то в качестве спонсора, ни о какой покупке и речи не шло, и дальше этой встречи никуда у нас дело не пошло»,— пояснил он. Впрочем, для «Ростелекома» тема инвестиций в киберспортивные команды сейчас не в приоритете, рассказал источник „Ъ“, знакомый с ситуацией.

Киберспорт также заинтересовал и венчурных инвесторов. Проекты в этом сегменте ищет Global Sports Opportunities Fund (по данным Crunchbase, его объем $50 млн), основанный компанией iTech Capital и бывшими игрокам сборной России по футболу Василием и Алексеем Березуцкими, рассказал партнер iTech Capital Алексей Соловьев в ходе конференции ИД «Коммерсантъ» о киберспорте. Киберспортсмены и команды пока остаются для инвестора самым сложным и непредсказуемым активом, а реально инвестиционно привлекательными объектами уже сейчас являются инфраструктура, сервисы, технологии для игр, писал он в колонке для Forbes.

Владислав Новый

Review

SberCloud

«Облако помогло пиццерии обогнать Apple»

Компания SberCloud была создана внутри экосистемы Сбербанка, когда стало понятно: разработанные в Сбербанке инфраструктурные и платформенные решения готовы не только обеспечивать деятельность многочисленных сервисов крупнейшего в стране финансового института, но и решать задачи внешних клиентов. Сегодня компания заявляет о своем намерении стать лидером российского рынка облачных технологий. О том, почему бизнес все чаще делает выбор в пользу облаков, с кем планирует работать SberCloud и что дает клиентам IT-экспертиза Сбербанка, „Ъ“ рассказал генеральный директор SberCloud **Александр Сорокоумов**.

ЖАННА ПАВЛОВА

— экспертное мнение —

— Ранее в СМИ «СБклауд» и SberCloud были представлены фактически как одна компания. Есть ли между ними разница и в чем она заключается?

— Это две разные компании. В начале этого года Сбербанк перезапустил свой облачный бизнес. 18 января мы закрыли сделку по продаже 39% акций в компании «СБклауд», сократив свою долю до 21%. Мы больше не участвуем в операционном управлении этой компании, теперь она живет и развивается по своей стратегии. Мы сделали стопроцентную «дочку» Сбербанка ООО «Облачные технологии». Она ведет операционную деятельность под брендом SberCloud и развивает облачные сервисы, продукты и платформы Сбербанка для коммерческого использования.

— Но она, получается, фактически ваш конкурент? В каких-то сферах.

— Не совсем. У нас разный приоритет, разный фокус развития. Наша стратегия — это вывод на рынок тех платформ, технологий, решений, которые мы делаем для Сбербанка.

— То есть не только для Сбербанка, для других?

— Мы сделали несколько серьезных платформенных решений, на которых работает сам Сбербанк. И теперь мы поняли, что эти решения уже настолько зрелые, что мы можем предложить их рынку. Цель SberCloud — это коммерциализация технологических разработок банка как в части инфраструктуры, так и в части платформенных решений.

— А вся инфраструктура, все «железо» принадлежат Сбербанку?

— Все оборудование, инфраструктура принадлежат SberCloud, то есть ООО «Облачные технологии».

— Давайте обсудим рынок, на который SberCloud выходит. По оценке IKS Consulting, в 2018 году рынок облачных сервисов России вырос на 25%, до 68,4 млрд руб. Основной объем, 70%, приходился на сегмент SaaS. Согласны ли вы с такими оценками и каковы ваши прогнозы по развитию этого рынка?

— Цифры по объему рынка плюс-минус близки к нашим оценкам. По распределению — нет. Доля SaaS — около 50%, может, чуть-чуть больше, но точно меньше 70%. Большая доля по-прежнему это инфраструктурные платформенные сервисы. Они обычно разделяются на IaaS и PaaS, но сейчас уже грань между ними начала стираться. Но для клиента важна конечная ценность, которую он получает, выбирая облачные решения, а не формальные определения класса этих сервисов.

— Есть ли сейчас у SberCloud партнеры из числа зарубежных компаний? Ранее СМИ писали, что одним из таких может стать Amazon.

— Мы планируем ряд крупных подписаний на ПМЭФ с российскими и иностранными компаниями, но пока я не могу их озвучить.

— В феврале 2019 года SberCloud выпустил решение «Виртуальный ЦОД». Какие конкретные задачи крупные компании будут решать за счет этого сервиса?

— Виртуальный ЦОД дает бизнесу динамичность. Ведь как обычно происходит? Бизнес ставит IT задачу сделать определенную платформу с таким-то набором приложений и сервисов завтра. Но «завтра» не получится. А мы можем сделать уже сегодня, потому что у нас есть все необходимое оборудование и клиент может за несколько минут развернуть, сконфигурировать нужный ему набор инфраструктуры и начать им пользоваться.

Мы сейчас идем по пути, который до нас прошли Amazon и Alibaba. Несколько лет назад они начали делать облачную платформу для себя, а потом поняли, что могут предложить облачные сервисы клиентам. А потом уже, например, Domino's Pizza, используя платформу Amazon Web Services, по скорости роста капитализации обогнала Apple.

— На российском рынке кто-то еще проходил этот путь?

— Облачный рынок в России только начал развиваться. Его доля в IT в целом — 3–4%. И даже эти 3-4% — это еще не полноценное облако, а скорее интеграционный проект.

Чем в принципе отличается облачный провайдер от бизнес-интегратора? Интегратор каждый раз делает кастомизированный проект под клиента. А полноценное облако — это проверенное, надежное типовое решение, в основе которого всегда лежит большой и сложный процесс R&D.

Но этот сложный процесс позволяет создать ключевые ценности облака — это скорость развертывания, возможность масштабирования, надежность типового решения, которое протестировали миллиарды раз в различных конфигурациях.

Крупные российские технологические компании только выходят на этот рынок. На облачном решении, которое мы предлагаем рынку, работает процессинг Сбербанк и справляется со сверхвысокими нагрузками. Никто в России не может похвастаться, что делает то же самое.

— Расскажите подробнее про вашу платформу IoT, реализовывались ли уже какие-то кейсы?

— Мы предоставляем IoT-платформу, на которой уже работают прикладные, конечные решения наших клиентов. Совместно с компанией «Меркатор» мы предлагаем нашим клиентам продукт «Монитор мэра» — платформу для мониторинга в режиме реального времени работы коммунальных служб и спецтехники.

Например, прошел снегопад, нужно отправлять уборочную технику на расчистку улиц. Через нашу платформу муниципальные власти могут отслеживать нагрузку и передвижение машин, сколько раз они были на конкретных участках и т. д.

Другой востребованный у наших клиентов продукт — промышленный IoT. Мы понимаем, что не может быть одинакового «коробочного» IoT-решения для сталелитейного завода и для производителя печенья. Это очень разные технологические процессы. Поэтому мы делаем качественную облачную платформу, а уже на базе нее производители стали или печенья интегрируют свой SaaS, который помогает решать их текущие задачи.

— Кто основной потенциальный клиент ваших продуктов и решений?

— Сейчас мы ориентируемся на сегмент крупнейшего и крупного бизнеса и госсектор. Мы, как банк, как один из крупнейших потребителей IT в России, очень хорошо понимаем нужды таких компаний, их архитектуру, требования по надежности, безопасности, защищенности. Но в будущем любой потребитель IT — это наш клиент.

— В сегмент малого и среднего бизнеса (SMB) выходить планируете?

— Мы планируем это в 2020 году. SMB — очень интересный рынок с точки зрения количества потребителей, очень динамичный и открытый для новых технологий.

— А государственные ведомства, министерства?

— В рамках программы «Цифровая экономика» мы участвуем в рабочих группах по созданию гособлака. Мы видим большой потенциал в этом. Мировая практика показывает, что коммерческие операторы гособлака могут сделать для государства предложение, которое позволяет ему быть более открытым и решать свои задачи более эффективно.

— Сейчас в России объявлен курс на импортозамещение. Происходит ли этот процесс в сфере облачных сервисов и насколько успешно?

— В контексте импортозамещения сейчас в России очень много внимания уделяется развитию opensource-решений, но проблема в том, что пока большинство из них не оптимизированы под конкретные задачи государственных структур и российских компаний. В этом направлении у нас есть большой задел в виде накопленной внутри команд Сбербанка и SberCloud экспертизы работы с opensource. Комбинация opensource и нашей экспертизы дает нам проверенные решения, которые в ближайшее время мы предложим рынку.

— Это что касается программных продуктов, а в части «железа», например, как быть с локализацией аппаратных решений? Вы будете использовать российское «железо»?

— Наше облако может строиться как на российском «железе», так и на зарубежном — у нас есть и то и другое. Но первоочередной критерий — это не происхождение, а его технические характеристики, работоспособность и отказоустойчивость.

Есть несколько компаний в России, которые делают российское оборудование. Дальше вопрос уровня локализации. Если это качественный российский R&D и работа над архитектурой, это круто, то мы готовы в это инвестировать, а где-то уже делаем.

— Недавно Сбербанк подсчитал, что убыток от кибератак для компаний по всему миру составил $1,5 трлн, а в текущем году цифра может увеличиться еще на $1 трлн. Как SberCloud обеспечивает безопасность клиентов, какие решения используются и какая именно доля расходов идет на обеспечение?

— Чьи решения — я не могу сказать: это наше ноу-хау по архитектуре и защите. У нас есть набор инструментов, часть из них предоставляется по умолчанию, часть — за дополнительную плату. Но это отдельный закрытый разговор с каждым клиентом в зависимости от его требований к уровню защиты данных.

У SberCloud есть важное преимущество: как я ранее уже говорил, наши продукты и технологии созданы на основе разработок Сбербанка. В том числе нам доступна экспертиза банка и в области кибербезопасности — а это такой уровень компетенций, которых нет больше ни у кого.

Интервью взял Дмитрий Шестоперов

информационные технологии

Кванты на пороге лаборатории

— наука и бизнес —

Квантовые технологии стали одной из главных тем технологического дискурса последних лет. Государства и бизнес уже не могут игнорировать эту тему — такая недальновидность может обойтись слишком дорого. Эксперты считают, что наступил переломный момент: от лабораторных исследований квантовые технологии переходят к решению реальных задач.

Правительства разных стран разрабатывают долгосрочные планы по развитию квантовых технологий. Крупнейшие мировые корпорации вкладывают огромные деньги в изучение этой области. Появляются стартапы, зарабатывающие на квантовых технологиях. При этом настоящий квантовый компьютер все еще не создан, а доказательства квантового превосходства не представлены. Так почему же эта тема так важна?

Речь идет ни много ни мало о новой технологической революции. Квантовый компьютер сможет обрабатывать информацию быстрее и решать такие задачи, с которыми принципиально не могут справиться классические вычислительные системы. IBM, Microsoft, Intel, Google, Alibaba, Baidu и другие корпорации вкладывают миллиарды долларов в разработку квантовых компьютеров и наращивание их мощностей, которые измеряются в кубитах. Уже совершен переход от квантовых машин с двумя-пятью кубитами к 20-, 50-кубитным системам. Недавно Google объявила, что достигла 72 кубитов. В Мэрилендском университете готовят квантовый компьютер мощностью около 100 кубитов. Группа Михаила Лукина в Гарварде близка к этому уровню.

IBM прогнозирует, что переход от лабораторных испытаний к коммерческим версиям квантовых компьютеров состоится в срок от трех до пяти лет.

От исследований к реальному применению

В России план развития квантовых технологий разработан до 2024 года. Он предусматривает вложения в эту область более 43 млрд руб. Проект «дорожной карты» в мае представили Российский квантовый центр (РКЦ) и НИТУ МИСиС совместно с привлеченными экспертами.

Внимание к квантовым технологиям возникло не внезапно, говорит гендиректор РКЦ кандидат физико-математических наук Руслан Юнусов. «Планомерная работа ведется последние шесть-семь лет, чувствуются интерес и поддержка государства и крупных компаний. Но в последние пару лет наметилось серьезное изменение: из теоретических ожиданий квантовых компьютеров стали появляться первые реальные случаи их использования для решения серьезных задач. Пока это еще не достижение „квантового превосходства“ в классическом понимании, но уже практическая польза»,— рассказал он „Ъ“.

Например, Volkswagen с Google и D-Wave используют квантовые компьютеры для решения задач оптимизации городского трафика. Другая проблема, которую человечество надеется решить,— построение емких аккумуляторов для создания электромобилей. Если бы аккумуляторы были всего в десять раз более емкими, это перевернуло бы рынок. Но классические вычисления пока не решили эту задачу. Одной из основных сфер применения квантовых компьютеров на первых этапах называют моделирование новых материалов.

Переход из ожиданий фундаментальной науки к инженерным задачам, который случился в последние два года, не позволяет «оставить все как есть». «Нам всем нужно решать насущные технологические проблемы. Те же новые материалы, работа с большими данными, безопасность — все это необходимо нашей стране, и этими вопросами надо заниматься сейчас. Поэтому квантовые технологии — одна из обязательных частей программы „Цифровая экономика“»,— пояснил Руслан Юнусов.

Вычисления и не только

Квантовые технологии — это не только и не столько квантовый компьютер. Под этим определением скрыто три уровня: квантовые вычисления, квантовые коммуникации (криптография) и квантовые сенсоры. Направление квантовых сенсоров уже активно развивается в промышленности, рассказал „Ъ“ вице-президент по науке и образованию фонда «Сколково» Николай Суетин. «Есть несколько сенсоров, уже нашедших реальные применения. Атомные часы построены на квантовых принципах. Современные квантовые технологии активно используются, например, в высокоточных оптических измерениях, для счетчиков единичных фотонов, для детектирования слабых магнитных полей в медицине и других целей»,— пояснил он.

Если вернуться к квантовым вычислениям, то есть несколько аргументов за их развитие. Традиционные компьютеры выходят на предел своих возможностей: закон Мура перестает действовать — удвоения вычислительных мощностей каждые два года уже не происходит. Некоторые задачи, стоящие перед человечеством, принципиально невозможно решить с использованием современных вычислительных архитектур.

Свои квантовые вычислители совместно с университетскими центрами создают все ведущие мировые IT-корпорации: Intel, Google, IBM, Microsoft и др. Более того, некоторые компании предлагают внешним исследователям тестировать свои разработки на их устройствах и использовать их для решения сложных вычислительных задач. Почему бизнес приходит к квантовым вычислениям? Можно выделить три большие сферы: оптимизация процессов, задачи машинного обучения, моделирование новых материалов и востребованных химических соединений. С помощью квантовых эмуляторов можно моделировать поведение реальных физических систем, например узнать, как в реальности проходит химическая реакция. Благодаря этому ученые надеются оптимизировать процессы каталитического синтеза, например производство аммиака.

Один из самых известных примеров применения квантовых вычислений для решения реальных задач — компания D-Wave. Пока вокруг спорят, насколько ее компьютер действительно квантовый, компания зарабатывает вполне настоящие деньги. Она работает с различными индустриями: автопромом (Volkswagen), космической сферой (NASA), медициной.

Превентивная защита

Следующий уровень квантовых технологий — квантовые коммуникации. Несмотря на то что квантовый компьютер еще не создан, уже существует потенциальная угроза потери важной информации, когда он появится.

Эта проблема актуальна для организаций, которые хранят и передают информацию, актуальную в долгосрочной перспективе — 10–15 лет, объясняет руководитель проекта по квантовому машинному обучению РКЦ, PhD по теоретической физике Алексей Федоров: «Если при передаче таких данных через интернет злоумышленник получит к ним доступ, то он ничего не сможет с ними сделать, кроме как сохранить их. Но в момент, когда появится квантовый компьютер, он сможет получить ключ и получить доступ к информации. Если время актуальности данных у организации больше, чем ориентировочное время появления квантового компьютера, то уже сейчас надо внедрять квантовую криптографию».

Несколько сотен километров защищенных квантовых сетей уже проложено в Китае, в Швейцарии, в США. В России тоже есть экспериментальные сети, построенные с применением квантовых коммуникаций.

Испытания решений из области квантовой криптографии уже проводят Сбербанк и Газпромбанк. Активно развивает направление и «Ростелеком»: он недавно провел тестирование ведущих российских разработок в области квантовых коммуникаций. В нашей стране есть три научных центра, которые независимо друг от друга ведут разработку в области квантовой криптографии: РКЦ с «дочкой» QRate, Центр квантовых технологий МГУ совместно с компанией «Инфотекс» и Университет ИТМО вместе с центром в Казани. Для общемировой картины это довольно весомый показатель — в Китае такими разработками тоже занимаются три компании, в Европе на все страны всего несколько игроков, и один успешный разработчик в США.

Квантовые коммуникации будут востребованы как государством, так и бизнес-структурами, считает вице-президент по стратегическим инициативам «Ростелекома» Борис Глазков. С 2018 года оператор начал тестирование решений из области квантового шифрования на своей волоконно-оптической линии между дата-центром М10 в Москве и лабораторией университета Сколтех в «Сколково» длиной 58 км. По словам Бориса Глазкова, в обозримом будущем квантовое шифрование сможет использоваться для передачи критически важных данных: «Такие технологии важны финансовым организациям, банкам для проведения защищенных трансакций. Такая защита нужна и для передачи медицинской информации, и для обмена данными госслужб».

Тестирование решений российских разработчиков на сети «Ростелекома» показало, что технических ограничений для организации квантово-защищенной передачи данных в городских сетях нет. Однако говорить о коммерческой эксплуатации подобных решений рано: их создателям предстоит непростой путь по доработке, а затем и сертификации каждого конкретного комплекса. Также предстоит стандартизировать интерфейс для передачи ключей в систему криптографической защиты информации. Но уже сегодня можно сказать, что квантовые коммуникации из лабораторной стадии скоро выйдут на уровень практического применения.

Что может пойти не так

Сегодня квантовые компьютеры находятся на том этапе, на котором были классические компьютеры в 60-е годы XX века. «Когда меня спрашивают, будет ли нужен квантовый компьютер в принципе, вспоминается история, как на заре компьютерной эпохи один из руководителей IBM — Томас Уотсон — сказал, что миру не нужно будет больше чем пять компьютеров,— говорит Алексей Федоров.— Так же можно сказать сегодня про квантовые компьютеры. Нужно ли будет больше пяти таких компьютеров на весь мир? Породят ли они новые индустрии? Я верю, что да, но прогнозировать будущее сложно».

Фундаментальных ограничений для того, чтобы построить квантовый компьютер, нет. Но это не отменяет сложности задачи. «Что может помешать — так это сверхвысокие ожидания. Китай вложил $12 млрд в развитие квантовых технологий, Европа — €3 млрд, США вкладывают десятки миллиардов долларов — это накладывает на сообщество огромную ответственность. Сейчас действительно многого ждут, но не так много можно продемонстрировать. А это перегревает ожидания инвесторов. Думаю, такие колебания могут помешать прогрессу. Но они его точно не остановят»,— резюмирует представитель РКЦ.

Марина Эфендиева

Review

s8.capital

Счастливый билет

Воспетая в фильме «Спортлото-82» любовь советских граждан к лотереям никуда не делась. Даже спустя почти четыре десятка лет миллионы россиян все так же испытывают свою удачу, только теперь для этого не обязательно даже приобретать бумажный билет — квиток с нужными цифрами может вполне быть и электронным. А желающих получить миллионы взамен 100–200 руб. в последнее время становится все больше. Только за последний год число наших соотечественников, участвующих в лотереях, по данным GfK, выросло с 20 млн до 39 млн человек. Правильно распорядиться огромной аудиторией, чтобы предложить ей то, что нужно, задача не из легких. Решить ее операторам лотерей сегодня помогают IT-технологии.

PHOTOXPRESS

— автоматизация клиентского опыта —

Владеть миром

Натан Ротшильд — человек, очевидно знавший, как зарабатывать деньги,— говорил, что миром владеет тот, кто владеет информацией. Развитие цифровых технологий привело к тому, что в распоряжении частных лиц и компаний теперь есть терабайты данных. Например, у холдинга S8 Capital, управляющего брендом «Столото», на сегодня скопились данные примерно о 20 млн клиентов. Но сами по себе эти знания об участниках двух десятков лотерей, распространяемых компанией, не сделают бизнес S8 эффективнее. Ими еще нужно научиться управлять. В этом на помощь бизнесу приходят три волшебные буквы — CRM (Customer Relationship Management).

На рынке сегодня есть множество CRM-систем, а пользуются ими компании, представляющие все возможные отрасли: от строительных до развлекательных. Лишь пара показательных примеров, демонстрирующих эффективность инсталляции таких технологий. Так, в декабре прошлого года оператор мобильной связи Tele2 объявил о внедрении в свой бизнес системы Microsoft Dynamics CRM. Она была необходима оператору для облегчения работы с корпоративными клиентами. В условиях стремительного роста клиентской базы Tele2 нуждалась в универсальном инструменте, который помог бы управлять и составлять прогнозы по корпоративным продажам. Кроме того, система должна была синхронизироваться с внешними базами данных о клиентах и обеспечивать своевременное получение информации в кратчайшие сроки. В результате внедрения CRM-системы, по данным оператора, время подключения корпоративных клиентов сократилось в два раза.

До этого автоматизированную систему управления взаимоотношениями с клиентами внедрила сеть магазинов «Пятерочка». Торговая сеть использовала платформу SAS Customer Analytics для создания программы лояльности. Так появилась «Выручай-карта». Компания и без нее демонстрировала приличные показатели роста бизнеса, однако для дальнейшего развития ритейлеру нужны были дифференциация бизнеса и стратегия по удержанию клиентов. Это должно было позволить компании не только повысить среднюю сумму чека покупателей, но и их частоту посещения магазинов сети. В итоге технологии помогли нарастить число участников в программе лояльности до 30 млн человек.

S8 Capital, чья клиентская база выросла с 2 млн до 20 млн человек за четыре года, также пришла к необходимости управления взаимоотношениями с клиентами. В результате был реализован проект по внедрению системы аналитического CRM на базе платформы SAS Marketing Automation. «Руководство компании исторически рассматривало клиентскую базу как основной актив, потенциал которого можно и нужно было максимизировать. При таком взрывном росте количества клиентов компания нуждалась в инструментах по управлению основными показателями поведения участников лотерей, такими как уровень удержания, средний чек и частота покупки, общий LTV (Life Time Value — один из показателей эффективности продукта: предсказание чистого дохода, связанного со всеми будущими отношениями с клиентом.— „Ъ“),— объясняет Анастасия Сенчугова, руководитель управления CRM холдинга S8 Capital.— По мере развития новых бизнес-направлений в группе компаний на основе накопленного опыта и знаний о поведении клиентов лотерей с помощью внедренного решения мы планируем развивать кросс-продажи, которые позволят как привлечь действующих клиентов в растущие бизнес-направления, так и увеличить кумулятивный LTV на клиента группы компаний. Если сформулировать проще: чем больше услуг мы продадим одному текущему клиенту, тем потенциально выше наш доход и ниже затраты, так как сокращаются издержки на привлечение новых клиентов».

Быстрее, гибче, больше

Внедренное в S8 Capital решение позволяет делать персональные предложения клиентам, составлять индивидуальные предложения и вовлекать клиентов в живое общение, чтобы завоевать их доверие и повысить лояльность. При этом все это делается автоматически за счет выработки плановых решений, основанных на комплексной клиентской аналитике.

Сегодня реализованный функционал платформы позволяет команде CRM S8 Capital создавать единую аналитическую запись о клиенте, включая историю его поведения, склонность к участию в определенных лотереях, вероятность реагирования на предложение компании и т. д. Полученные на основе данных инсайты трансформируются в стратегию управления прямыми взаимодействиями с клиентами: от таргетированных рассылок и специальных акций до персонализации контента цифровых платформ.

«В лотерейном направлении основное внедрение уже завершено, и можно констатировать, что компания получила гибкий современный инструмент для анализа клиентского поведения, сегментирования базы, математического моделирования и управления всеми типами прямого взаимодействия с участниками»,— говорит Сенчугова.

Каждый месяц компания реализует около 70 целевых кампаний, в которых участвуют в общей сложности от 500 до 700 клиентских сегментов. А свыше 400 тыс. посетителей сайта взаимодействуют с персонализированными баннерами. Все это стало возможно благодаря применению системы, которая занимается автоматизированной выдачей баннеров по преднастроенным алгоритмам.

Нешуточный выигрыш

Конечная цель применения автоматизированной системы управления взаимоотношениями с клиентами — это повышение эффективности бизнеса, и внедренное решение в лотерейном бизнесе S8 Capital уже оправдало себя. «С точки зрения финансовых показателей внедрение системы окупилось в течение первых трех месяцев эксплуатации, кратно позволило увеличить количество сегментов клиентов, с которыми мы взаимодействуем в рамках директ-маркетинговых коммуникаций (СМС, e-mail, push-уведомления и т. д.) и позволило существенно нарастить долю выручки компании, получаемой от директ-маркетинга,— отмечают в компании.— Кроме того, внедрение системы обеспечило увеличение уровня удержания клиентов и дало возможность оптимизировать затраты на ряд коммуникаций за счет более точного их таргетирования».

В S8 Capital не собираются останавливаться на достигнутом: во-первых, холдинг намерен обогатить собственные базы данных информацией из внешних источников, что позволит еще больше усовершенствовать предиктивные модели, а во-вторых, в планах компании — расширение списка сфер применения CRM-системы. Уже в прошлом году опыт, полученный в лотерейном бизнесе, был использован для создания аналогичной платформы для букмекерского бизнеса. «Среди сфер интересов S8 Capital есть страхование, телекоммуникации, цифровые медиа, иные бизнесы. Все прямые и целевые взаимодействия с клиентами в сегменте B2C можно так или иначе проводить с помощью внедренного решения,— рассуждает Сенчугова.— Глобальная цель холдинга, утвержденная акционером Арменом Саркисяном,— обеспечить максимальное покрытие потребностей клиента сервисами и услугами, основанными на информационных технологиях, в самых разных сферах жизни. Поэтому расширение использования инструментов аналитического CRM в новых сферах — это первый и очень важный шаг в сторону организации единой экосистемы сервисов для клиента, а также необходимое условие реализации концепции клиентоцентричности на уровне кросс-продуктового предложения группы компаний».

В компании рассчитывают, что уже через три года вся клиентская база холдинга будет получать целевые предложения через внедренные инструменты. Объединение данных о клиентах разных бизнес-подразделений на базе единой аналитической платформы позволит получить синергетический эффект и создать единую экосистему управления взаимоотношениями с клиентами всего холдинга.

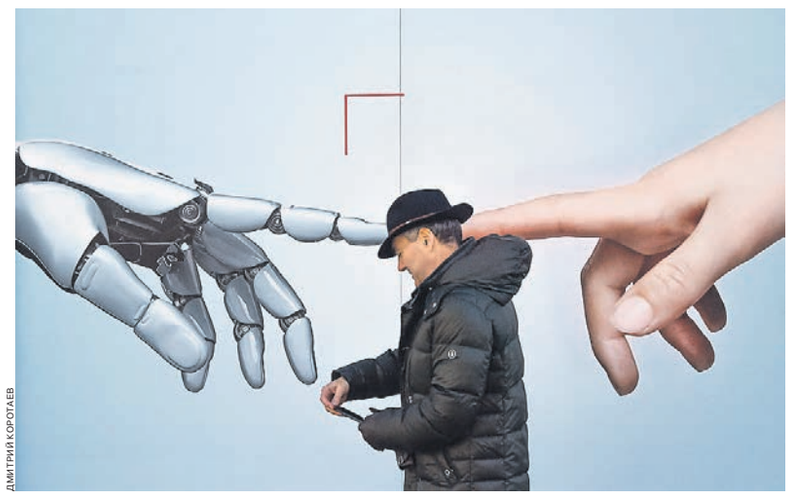
Кирилл Сарханянц

информационные технологии

Берегите голову

— алгоритмы —

Искусственным интеллектом (AI) восхищаются, искусственного интеллекта боятся. Но ограничиваются эти страхи, как правило, вариантами двух сценариев: научно-фантастического и социально-экономического. В первом все плохо, потому что превзошедший человека интеллектуально на несколько порядков AI решает либо вообще избавиться от человечества, либо обустроить нашу жизнь очень неприятным для нас образом — например, как мы обустраиваем короткую и несчастливую жизнь бройлеров на птицефабрике. Во втором AI звезд с неба не хватает, остается под контролем людей, но позволяет так лихо автоматизировать производство и оптимизировать бизнес, избавившись от 95% белковых работников, что опять-таки все плохо. По крайней мере — у этих 95%.


ДМИТРИЙ КОРОТАЕВ

Третий сценарий

В феврале BCG исследования «Дивиденды зрелого цифрового маркетинга». Один из самых впечатляющих выводов: внедрение алгоритмов машинного обучения в некоторых кейсах приводило к 50-процентному росту онлайн-продаж. Основанный на анализе данных маркетинг в случае умелого использования ведет к росту выручки на 20% и сокращению затрат на 30%.

Повсеместное внедрение любой технологии, оказывающей такой впечатляющий эффект на бизнес, неизбежно. Более того, компании будут буквально наперегонки стараться собрать максимальный объем данных о клиентах, скормить их алгоритмам и сделать так, чтобы инновационный «зрелый» маркетинг дотянулся до всех, кого можно подтолкнуть расстаться с деньгами. В противном случае конкуренты вырвутся вперед, а акционеры найдут более динамично мыслящих топ-менеджеров.

«Люди с радостью готовы отдать свое самое ценное — персональные данные — в обмен на бесплатный сервис электронной почты или смешные видео с котиками. Немного напоминает то, как африканские и американские племена, не осознавая того, продавали европейцам целые страны в обмен на разноцветные бусы и дешевые безделушки» — пишет автор бестселлера Sapiens профессор Юваль Ной Харари в своей новой книге «21 урок для XXI века».

В интервью Wired и многих других публикациях Харари предупреждает: знания об устройстве человеческого сознания и технологии интерпретации генерируемых нами данных уже достигли или вот-вот достигнут важного рубежа. А именно: бизнес или государство смогут понять нас, наши желания, мотивацию, чувства и переживания лучше, чем мы понимаем их сами. И теперь интернет и машинное обучение могут вывести эффективность манипулирования на принципиально новый уровень.

Предложение, от которого нельзя отказаться

Образцово-показательный пример бизнеса, превращающего данные и алгоритмы в топливо для роста,— Amazon, которая уже несколько месяцев с переменным успехом бьется с Apple и Microsoft за титул самого дорогого бизнеса в мире. Компания Джеффа Безоса за четверть века выросла из скромного онлайн-магазина книг в огромный онлайн-рынок, крупнейшего поставщика облачных услуг и лидера рынка «умных» домашних устройств.

Серверы Amazon Web Services выполняют 40% всех облачных вычислений для мирового бизнеса, а микрофоны 100 млн смарт-колонок Amazon Echo внимательно слушают, что происходит в домах их владельцев. Компания активно строит экосистему «умного» дома, в последние 12 месяцев дополнив ее «умными» дверными звонками Ring: они облегчат доставку посылок, когда клиентов нет дома, а также роутерами Eero.

Зачем Безосу роутеры? Чтобы сделать экосистему более завершенной, но, возможно, не только для этого. Роутер знает, стоит он в богатом доме или победнее — об этом расскажут модели подключающихся устройств. А если изучить историю просмотров в интернете пользователей, не составит труда узнать их лучше, чем они знают себя сами, и хакнуть их мозг, нежно навязав ненужные (или выгодные Amazon) покупки. Корпорация получит в руки данные, не сильно уступающие по ценности тому цифровому золоту, которое Google намывает из наших поисковых запросов и кликов.

Зная все о предпочтениях клиентов в покупках и просматриваемых ими сайтах, ритейлер сможет постоянно делать им предложения, от которых они и не подумают отказываться. Предложенное покажется внезапным откровением, простым и понятным ответом на чаяния, которые человек сам толком не осознавал. Чтобы дотянуться до маячащего перед носом счастья, останется сущий пустяк — в пару кликов расстаться с деньгами.

Мы новый мир построим

Недавно выяснилось, что похожие варианты развития цифровой экономики (да что там — цивилизации в целом) рассматривают и в Google. Весной 2018-го журналисты обнаружили ролик (легко найти в YouTube по запросу «selfish ledger»), сделанный в корпорации несколькими годами ранее и, по утверждению авторов, представляющий собой не более чем мысленный эксперимент.

В видео выдуманное приложение «Google Намерения» помогает выбрать цели («полноценно питаться», «беречь природу», «поддерживать местный бизнес»), а потом подталкивает действовать в русле этого приоритета. Как именно, кого и когда подталкивать, решает некий «реестр», руководствующийся результатами анализа больших данных и чем-то крайне неопределенным, названным в ролике «ценности Google как организации».

Чтобы быть всемогущим, «реестру» нужны данные о подопечных, чем больше — тем лучше. И в ролике ему дают возможность придумывать новые способы их собирать, например, создать именно такие «умные» весы, которыми большинство потребителей захотят и будут регулярно пользоваться, информируя реестр о своем весе. Цель у этого всего самая благородная: максимально тщательно проанализировать человека как вид и помочь людям решить самые разные проблемы — от депрессии до бедности.

Антиутопия это или утопия — зависит от точки зрения и отношения пользователя к «ценностям Google (Amazon, Apple, Компартии Китая, Русской православной церкви — нужное подчеркнуть) как организации». Но вне зависимости от ценностей будет очень страшно, если такой уже почти ставший реальностью инструмент попадет в руки людей, руководствующихся сильно упрощенными и поэтому очень опасными взглядами на мир.

Что делать?

Не будет ли нам всем в итоге лучше под опекой внимательного и мудрого искусственного интеллекта? Ведь можно настроить управляющий обществом алгоритм на целевые значения, соответствующие очевидным ориентирам человеческого благополучия. Счастье алгоритм вряд ли подарит, но вот уменьшить совокупность страданий в мире ему точно по плечу.

Красивая мечта, но пока что главная цель всех алгоритмов такого рода — зарабатывать больше и быстрее. Для ритейлеров искусственный интеллект решит задачу максимизации прибыли. Аналогично, только с настройкой на монетизацию человеческого внимания, работает уже сейчас и YouTube.

То же и в политике, какими бы прозрачными и демократичными ни были механизмы выборов. Не важно, кто именно будет президентом. Важно, какая из групп влияния сможет более эффективно использовать алгоритмы соцсетей, чтобы манипулировать информацией и вызывать нужные эмоции.

В этом «светлом будущем», которое вот-вот наступит, стоит каждую минуту помнить: на ваш мозг нацелен суперкомпьютер, задача которого обыграть вас, заставив действовать в чужих интересах. И шансов выиграть у AI гораздо больше, чем у человека.

Осознавать власть алгоритмов лучше, чем пребывать в неведении, но человек не сможет постоянно обыгрывать AI, даже замечая все невидимые нити, тянущиеся с экрана смартфона к разным участкам его мозга. Алгоритмы воздействия полагаются на нейронные цепи, которые эволюция создала на десятки, а то и сотни миллионов лет раньше, чем рациональное мышление Homo sapiens. Так что осознание того, что человека можно «взломать»,— лишь первый шаг.

По мнению Юваля Ноя Харари, быть на один шаг впереди тех, кто воплощает в реальность гегемонию алгоритмов, поможет медитация. А не дать им преобразовать мир в угоду своим интересам позволит активное участие в политических процессах в составе коллектива единомышленников (потому что так эффективнее, чем в одиночку) и поддержка тех политиков, которые осознают угрозу.

Николай Белкин

Тематическое приложение к газете «Коммерсантъ» («Информационные технологии»). Учредитель: АО «Коммерсантъ». Адрес: 127055, г. Москва, Тихвинский пер., д. 11, стр. 2. | **Владимир Желонкин** — генеральный директор АО «Коммерсантъ», главный редактор газеты «Коммерсантъ» | **Сергей Вишневский** — руководитель фотослужбы | **Рекламная служба:** Тел. (495) 797-6996, (495) 926-5262 | **Владимир Лавицкий** — руководитель службы «Издательский синдикат» | **Роман Рожков** — выпускающий редактор | **Наталия Дашковская** — редактор | **Сергей Цомык** — главный художник | **Екатерина Липатова, Галина Кожеурова** — фоторедакторы | **Екатерина Бородулина** — корректор | **Адрес редакции:** 121609, г. Москва, Рублевское ш., д. 28. Тел. (495) 797-6970, (495) 926-3301 | Ограничение: 16+