Почему бизнес все чаще обращается к услугам предиктивной аналитики | 14

ИТ

Тематические страницы газеты Коммерсантъ

Информационные технологии

Вторник 13 декабря 2022 №231 (7432 с момента возобновления издания) kommersant.ru



15 | Как государство пытается спасти российскую микроэлектронику

15 | Что поменялось на рекламном рынке после вступления в силу новых поправок

16 | Какие недостатки интернета призвана исправить новая модель Web3

Без учений — тьма

Российские власти в 2022 году несколько раз заявляли, что ведется подготовка российского сегмента интернета к возможному отключению от глобальной сети. Для этого регулярно проводились киберучения с участием банков, операторов связи и крупнейших интернет-компаний, которые подтвердили, что российский сегмент сети сможет работать автономно. Подобные действия властей потенциально могут свидетельствовать о подготовке к новым санкциям и в целом эскалации ограничения доступа к информации, считают аналитики.



ВЛАД ШЕКРАСОВ

— инфраструктура —

Российский сегмент интернета в случае отключения от общей сети сможет работать автономно, заявил в конце октября Сергей Хуторцев, директор Центра мониторинга и управления сетью связи общего пользования Главного радиочастотного центра (ГРЧЦ, подведомственен Роскомнадзору). По его словам, такой результат показали учения, которые были проведены в августе. Список их участников в текущем году был расширен, в него вошли в том числе владельцы крупных интернет-ресурсов: СМИ, финсектор, RuTube.

Учения актуальны, признают власти, тем более в свете геополитической ситуации. Число кибератак на Россию увеличилось в нынешнем году на 80%, докладывал президенту РФ 24 октября вице-премьер РФ Дмитрий Чернышенко: «Причем если в прошлом году основной целью кибератак был финансовый сектор, то в этом году — госсектор». По его словам, более 25 тыс. кибератак на госресурсы и 1,2 тыс. инцидентов на критической инфраструктуре были «успешно ликвидированы»: «Понятно, что эта борьба будет продолжаться всегда — против нас воюют кибервойска всех недружественных стран».

На сентябрьской конференции в Сочи Kaspersky Industrial Cybersecurity Conference 2022 представитель Национального координационного центра по компьютерным инцидентам при Федеральной службе безопасности (ФСБ) Алексей Новиков открыто заявил, что в текущем году был период, когда в правительстве всерьез обсуждалось отключение рунета от остального интернета: «Настолько серьезной была ситуация». По его словам, волна кибератак на пользовательские интернет-ресурсы и инфраструктурные элементы российского сегмента сети началась 24 февраля. С тех пор, отметил эксперт, атаки с переменной успешностью продолжаются по сей день, причем подавляющее большинство инцидентов пришлось на DDoS-атаки. Они представляют собой огромный объем трафика, генерируемого легитимными интернет-пользователями. «Надо отдать должное той стороне: им удалось очень быстро построить эффективный механизм вовлечения пользователей в эту деятельность»,— сообщил господин Новиков.

Косвенно сценарий отключения подтверждал весной и глава Минцифры Максут Шадаев, указывая, что, если Россию отключат от европейских точек обмена, она перенаправит интернет-трафик через Азию. По его словам, такой план рассматривал «Ростелеком». Он напомнил, что несколько международных точек обмена трафиками уже отключили российских операторов. В частности, на фоне СВО точка обмена интернет-трафиком LINX отключила от своих сервисов «Ростелеком» и «МегаФон». Минцифры уверяло, что это не повлияет на скорость интернета. Один из крупнейших магистральных провайдеров — американский Cogent — также стал отключать российских операторов, тогда как американский же облачный провайдер Cloudflare, напротив, отказался прекращать работу в РФ. Госдеп США, в свою очередь, призывал не отключать Россию от интернета, чтобы у россиян оставался свободный доступ к информации.

«Ъ» решил разобраться, из каких этапов состоят учения по отключению российского сегмента интернета от глобальной сети и какие последствия для пользователей они могут иметь.

Зачем проводят учения

Учения проводят в рамках реализации закона о суверенном рунете («О внесении изменений в Федеральный закон „О связи“ и Федеральный закон „Об информации, информационных технологиях и о защите информации“»), принятого в 2019 году. Он в том числе обязывает операторов связи, интернет-компании и владельцев технологических сетей и точек обмена трафиком принимать участие в мероприятиях «по целостности и устойчивости функционирования интернета к негативным внешним воздействиям на территории России не реже одного раза в год». План таких «маневров», которые могут проводиться как на федеральном, так и региональном уровне, утверждает Минцифры совместно с ФСБ, Минобороны, Федеральной службой охраны, МЧС и Федеральной службой по техническому и экспортному контролю (ФСТЭК). Предусмотрено проведение и внеплановых учений в случае появления угроз устойчивости сети — таким образом, они могут проходить несколько раз в год.

Если возникнет опасность нормального функционирования рунета, Роскомнадзор может взять на себя централизованное управление трафиком в утвержденном правительством порядке. Для этого на сетях связи операторов с 2019 года ведомство устанавливает технические средства противодействия угрозам, которые фактически представляют собой оборудование DPI (Deep Packet Inspection — глубокая фильтрация трафика). В случае угрозы операторы должны будут руководствоваться маршрутизацией трафика с учетом точек его обмена из специального реестра. С 1 января 2021 года для операторов связи вступило в силу требование пользоваться национальной доменной зоной. С этой же даты действует положение об обязанности госорганов использовать отечественные средства шифрования информации. Как отметил господин Хуторцев, чтобы российские ресурсы сети функционировали надежно, необходимо обеспечить их независимость от зарубежных программных библиотек и массовое использование отечественных сертификатов ключей шифрования для доступа к российским ресурсам.

Учения по кибербезопасности, объясняет источник, близкий к Минцифры, позволяют проверить, насколько качественно, эффективно и безопасно работают ключевые элементы интернета в стране: реестр адресно-номерных ресурсов, национальная система доменных имен, национальный удостоверяющий центр, который выпускает TLS-сертификаты, а также сети связи общего пользования. К участию в них приглашаются федеральные органы исполнительной власти, операторы связи и организации отрасли связи, например интернет-провайдеры, добавили в министерстве.

Что известно про учения

Первые учения по изоляции российского сегмента интернета в рамках закона о суверенном рунете были проведены в декабре 2019 года. Их задачей было обеспечение устойчивого функционирования интернета в России при любых обстоятельствах. Итоги в Минкомсвязи подвели в тот же день, признав учения успешными. По словам занимавшего на тот момент должность замглавы Минкомсвязи Алексея Соколова, в ходе них было проработано несколько сценариев.

Первый предусматривал обеспечение безопасности абонентов сотовой связи, включая защиту персональных данных и возможность перехвата их трафика и СМС, раскрытия сведений об их местонахождении. Во втором сценарии исследовались риски и уязвимости «умных» устройств, в том числе при использовании на объектах критической информационной структуры. Тогда источники «Ведомостей» рассказывали, что часть учений, в которой были задействованы федеральные операторы связи, прошла не слишком успешно: условному злоумышленнику удалось осуществить 62,5% атак через протокол SS7 и 50% атак через протокол Diameter. Через несколько дней в работе сетей сразу нескольких российских аэропортов возникли сбои.

В 2020 году Минцифры несколько раз переносило учения, которые по плану должны были проводиться в конце каждого квартала. В том году они должны были отрабатывать противодействие атакам с использованием уязвимостей узкополосных сетей интернета вещей, работу в условиях неисправности одного из фрагментов сети связи, а также «внешние дестабилизирующие воздействия техногенного и природного характера», противодействие атакам с использованием уязвимостей протокола BGP (Border Gateway Protocol — протокол граничного шлюза), который применяется для прокладки маршрутов передачи данных между автономными сегментами сети. Примечательно, что именно с помощью последнего механизма украинский оператор Lurenet в апреле после начала специальной военной операции на Украине перехватывал трафик крупнейших российских провайдеров. Из-за атаки сервисы, базирующиеся на этих сетях, были недоступны из разных стран в течение десяти часов (см. «Ъ» от 27 апреля).

В прошлом году, как ранее заявлял Дмитрий Чернышенко, учения проходили на пяти киберполигонах. Он заявлял, что будет расширяться как география, так и количество отраслей, защиту которых предстояло отрабатывать. В 2021 году усилия были сосредоточены на энергетическом, кредитно-финансовом секторе и инфраструктуре государственных органов. Весной 2021-го директор департамента информационной безопасности (ИБ) ЦБ Вадим Уваров сообщил, что киберучения для оценки защищенности российских банков от хакеров будут проходить дважды в год. ЦБ в 2021 году провел киберучения, в которых приняли участие 70 кредитных организаций, сообщил первый замглавы департамента ИБ ЦБ РФ Артем Сычев на «Инфофоруме-2022».

В 2022 году учения стали масштабнее относительно прошлых лет, говорит источник, близкий к Минцифры: «Они отличились числом привлеченных организаций (более 30) и количеством отработанных угроз. Эти учения показали готовность российского сегмента к устойчивой автономной работе». На учениях провайдеры выявляли угрозы и отрабатывали методы противодействия. Также рассматривали ситуацию отзыва/отказа в выдаче зарубежными центрами сертификации российским компаниям TLS-сертификатов. Учения показали, что российские ИБ-специалисты готовы отражать кибератаки и обеспечивать устойчивое функционирование российского сегмента, подчеркнул собеседник «Ъ». В частности, «Ъ» в феврале узнал, что на фоне сообщений о возможных санкционных ограничениях США по поставкам в Россию новой электроники и поддержке существующей технологические учения проводил Сбербанк. На них моделировалось отключение IT-инфраструктуры банка от поддержки Microsoft, Nvidia, VMware, SAP и других компаний. С 15 июня по 15 июля, по данным РБК, «тестировалась возможность физического отключения российской части интернета».

В текущем году также проводились масштабные учения на сетях операторов связи и инфраструктуре СМИ: проверялись сценарии работы в условиях DDoS-атак, изменения маршрутизации трафика, атаки на DNS-серверы, рассказал «Ъ» источник, знакомый с ситуацией. По его словам, всегда используется реальная инфраструктура при участии регуляторов в лице ФСБ, ФСТЭК, ГРЧЦ, Роскомнадзора и Минцифры. Не только моделируются атаки и угрозы, но и отрабатываются сценарии процессов, необходимых для предотвращения последствий — речь идет, в частности, о коммуникациях с регуляторами, ответственными лицами, формировании документации и отчетов, прописывании механизма, что каждый должен делать в конкретной ситуации.

Ключевой параметр, по которому оценивается успешность учений,— время реагирования и предотвращения инцидента, объясняет собеседник «Ъ»: «Второй важный показатель — количество неучтенных сценариев и уязвимостей, необходимо подготовить список рекомендаций по их устранению». По итогам готовится доклад в правительство.

А это поможет?

Поэтапные шаги по защите госсайтов от отключения начались еще в марте. Правительство поручило всем государственным сайтам и сервисам до 11 марта перейти на использование российской системы доменных имен, отказаться от иностранных хостингов и счетчиков посещаемости сайтов, а также усилить «парольную политику». Но спустя полгода после предписания Минцифры убрать коды, загружаемые из-за рубежа, региональные госсайты продолжали ими пользоваться (см. «Ъ» от 28 октября). Эксперты связывали это с тем, что нарушение грозит всего лишь штрафом 5 тыс. руб., а использование иностранного кода в целом не несет рисков безопасности.

Более чувствительной является проблема использования зарубежных доменов. «Хотя единой кнопки блокировки России нет, можно разделегировать домен .ru — этого будет достаточно как эффективной базовой меры, чтобы наши сайты перестали открываться извне»,— объясняет заместитель гендиректора Zecurion Александр Ковалев. По его словам, в случае перехода на российскую систему доменов внутри страны интернет работать будет, но может потребоваться время на переключение: «При этом большая часть внешних посетителей не сможет получить доступ к таким сайтам, только если будет знать их IP-адрес».

У международного сообщества есть множество инструментов для отключения российского сегмента интернета от всемирной сети, говорит директор АНО «Информационная культура» Иван Бегтин: «Например, можно отрезать доступ в интернет для россиян на уровне оборудования магистральных провайдеров». Но в таком случае последствия для связности всей глобальной сети, отмечает эксперт, будут ощутимыми: «Через РФ идет трафик Казахстана и части азиатских стран». По мнению господина Бегтина, внешнее отключение маловероятно, но не исключено внутреннее ужесточение ограничений доступа и блокировок: «Для этого существуют так называемые белые и черные списки ресурсов». По похожей схеме работает закрытая модель интернета в Китае или Иране, обращает внимание Иван Бегтин: «В этих странах происходит усиленная централизованная модерация контента в сети».

К подобным событиям стали готовиться еще в конце 2018 года, когда был внесен законопроект о суверенном рунете, говорит независимый IT-специалист Филипп Кулин. По его мнению, отключение России от глобальной сети невыгодно ни российским, ни зарубежным разведывательным службам, поскольку это осложнит сбор информации. Тем не менее, говорит он, технически такая возможность есть, и наиболее жестким вариантом будет разделегирование доменов. «Одной из возможных целей киберучений могла быть как раз проверка ключевых информационных сервисов, например „Госуслуг“, банков на возможность работы в подобных условиях»,— отмечает господин Кулин.

Также, полагает он, власти формируют список таких критически значимых ресурсов, работа которых в случае отключения рунета будет обеспечена. Не исключено также, что идет подготовка к новым санкциям, которые осложнят работу телекоммуникационного бизнеса, говорит Филипп Кулин: «Если ГРЧЦ продолжает упоминать тренд на возможное отключение рунета, значит, возможна эскалация этого процесса».

Юлия Тишина

Общение с предсказаниями

— ликбез —

По оценкам Reportlinker Consulting Group, мировой рынок решений предиктивной аналитики с $12,4 млрд в 2020 году вырастет до $40,3 млрд в 2027-м. В России все больше компаний видят в аналитике, основанной на собранных больших данных и методах машинного обучения, практическую пользу. К примеру, согласно подсчетам McKinsey, внедрение решений предсказания отказов промышленного оборудования может увеличить срок его службы на 20–40% и сократить время простоев на 30–50%. Как это работает, сколько это стоит и кто этим занимается в России?

В чем смысл

Предиктивная (прогностическая) аналитика используется уже практически во всех отраслях: от финансового сектора и ритейла до промышленности и логистики. Банкам и страховщикам она позволяет минимизировать риски, в промышленности — сокращать потери от простоя оборудования и затраты на ремонт, в недвижимости и градостроительстве помогает грамотно рассчитывать нагрузку на инфраструктуру, изменение транспортных потоков, востребованность локации у целевой аудитории, перечисляют в МТС: «В телеком-бизнесе — позволяет автоматически проанализировать сотни тысяч потенциальных локаций для новых базовых станций и спрогнозировать их окупаемость».

Возможности предиктивной аналитики открывают для себя все больше компаний, получая очевидные конкурентные преимущества. Например, увеличивается прибыль благодаря автоматизации рутины и оптимизации рабочих процессов и достигается экономия на аварийном ремонте оборудования с помощью алгоритмов. «Машинное обучение активно применяется и в маркетинге, повышая его эффективность. Современные потребители становятся все более требовательными: им важно не только качество продукта, но и своевременная коммуникация от бренда с релевантным предложением,— рассуждает Роман Стятюгин, руководитель аналитических сервисов PREDICT, VK.— Так, алгоритмы помогают бизнесу существенно улучшить клиентский опыт за счет персонализированного обращения к покупателю в актуальный момент времени в удобном канале».

Прогностическая аналитика используется и для того, чтобы верифицировать гипотезы перед запуском продукта: определить объем потенциальной аудитории, ценность технологического решения и возможность его реализации, продолжают в МТС. В результате еще до запуска компания получает представление о емкости рынка, потенциале продукта и необходимых затратах. Это позволяет отказаться от заведомо неэффективных гипотез и оптимально распределить бюджет для разработки продуктов.

«Маленькие компании могут вырасти в разы, если смогут использовать предиктивную аналитику для получения весомого конкурентного преимущества,— размышляет директор по анализу данных X5 Group Михаил Неверов.— У больших компаний в разы вырасти, скорее всего, не получится, но рост прибыли на несколько процентов — а это могут быть миллиарды рублей — вполне реален».

Что нужно для эффективности такой аналитики, какие этапы проходят данные, прежде чем их можно использовать в бизнесе, и во сколько это может обойтись?

Собираем и храним

С развитием технологий и цифровизацией количество устройств, которые могут генерировать данные автоматически, увеличивается. Так, по данным Ericsson Mobility Report, количество подключенных устройств IoT/M2M в мире (без учета технологий short-range — Wi-Fi, Bluetooth и др.) увеличится с 1,7 млрд в 2020 году до 5,8 млрд в 2026-м. Данные с многих из этих устройств передаются по сети на серверы в хранилища данных, где обрабатываются и сохраняются в удобном для предиктивной аналитики виде.

с14

информационные технологии

«В ближайшие десять лет мы окунемся в метавселенную данных»

Глава департамента анализа данных и моделирования банка ВТБ **Максим Коновалихин** — о том, что метавселенная ближе, чем кажется, а также о связи между концепцией Data Fusion и дополненной реальностью.

— экспертное мнение —



ПРЕДОСТАВЛЕНО ПРЕСС-СЛУЖБОЙ ВТБ

Двадцать лет назад сбор больших данных казался прорывной практикой, а бизнес только начинал расширять свои знания о потребителе. Затем технологически продвинутые компании стали задумываться о сквозном объединении этих данных, создавая партнерства. Теперь предстоит совершить следующий шаг в сторону метавселенной данных, которая в перспективе десяти лет может объединить реальный и цифровой миры.

Исторически банки одними из первых научились извлекать ценность из статистических данных о клиентах. Первые модели кредитного скоринга, позволяющие автоматически принимать решения, датируются еще 50-ми годами прошлого века. Неудивительно, что в эпоху Big Data финансовая отрасль входит в число лидеров в задачах работы с данными. Аналитика больших данных — важный инструмент для развития клиентского сервиса, совершенствования банковских продуктов и повышения эффективности работы организации.

На сегодняшний день все успешные финансовые организации используют Big Data в работе. Во многом именно от этого зависит конкурентоспособность организации на рынке. Благодаря Big Data и алгоритмам искусственного интеллекта (ИИ) в банковской сфере произошел важный поворот от продуктоцентричного к клиентоцентричному подходу: для повышения продаж услуги должны быть ненавязчивыми и удобными.

Большие данные являются источником знаний о клиентском поведении и позволяют вычленять закономерности и предпочтения разных категорий потребителей. Именно аналитика больших данных позволяет предлагать клиентам персонифицированные продукты или выстраивать таргетированные коммуникации. В других сферах, например ритейле, большие данные обеспечивают эффективную работу рекомендательных систем, а данные о геолокации, взятые у телеком-операторов, помогают оптимизировать маршруты общественного транспорта.

Сбор персональных данных финансовыми организациями также помогает пресекать мошенничество. Например, когда пользователь со стабильным доходом и накоплениями резко снимает все деньги и пытается перевести их на другие счета, ИИ воспринимает это как подозрительную операцию и подает сигнал тревоги. Тогда банковские операции могут быть приостановлены до момента, когда клиент подтвердит свое намерение сделать перевод. К тому же большие данные — это способ банка обезопасить себя и своих клиентов от трезмерных рисков. Например, геоаналитические модели, разрабатываемые банком на основании объединения внутренних и внешних данных о финансовой активности клиентов, позволяют компаниям более эффективно открывать точки продаж, одновременно минимизируя бизнес-риски и повышая свою доступность для потенциальных покупателей.

Банки уже научились предлагать клиентам персонифицированные продукты, подбирая их на основе клиентского поведения. Автоматические расчеты кредитного лимита, рекомендации по открытию инвестиционных вкладов и даже советы по управлению финансами. Однако в настоящий момент потенциал больших данных раскрыт не полностью. Данные всегда несут большой синергетический потенциал: ни одна из отраслей не способна создать полную картину цифровых следов своих клиентов без синергии с другими отраслями.

И здесь логично упомянуть уже достаточно распространенную концепцию Data Fusion, которая позволяет одновременно использовать не только разные и косвенно связанные массивы данных, но и применять для их обработки сразу несколько технологий. Подход Data Fusion лежит в основе многих процессов: от построения экосистем и формирования стратегии обмена данными между государством и бизнесом до ESG-повестки и создания метавселенных.

Среди направлений, в которых ВТБ применяет объединение данных прямо сейчас,— кредитный скоринг, прогнозирование рисков, разработка новых продуктов, геоаналитические сервисы для эффективного развития бизнеса и выстраивание маркетинговых коммуникаций на основе более узкого сегментирования клиентов по поведенческим группам.

Если говорить о коммуникациях, то внутренние исследования подтверждают эффективность подхода. Разработка креативов, подбор каналов и формата коммуникации в зависимости от особенностей поведения разных сегментов потребителей приводит к росту продуктивности маркетинговых кампаний.

Кроме роста эффективности работы с текущими клиентами и полной замены спама узкотаргетированными предложениями сквозное объединение позволит выйти на новые аудитории. Реализация концепции Data Fusion повышает тонкость восприятия банком потребностей и предпочтений, а значит, позволяет найти идеальный баланс в коммуникации с каждым клиентом в отдельности.

ВТБ ставит перед собой задачу по расширению взаимовыгодных партнерств и источников данных, доступных для совместного использования. Но тут мы сталкиваемся с проблемой существования монополии на данные. Существуют банковские монополии по трансакциям, данные от сотовых операторов, мы видим, что уже возникают монополии в том числе на «умные» устройства и данные от них. Коммерческие организации не торопятся обмениваться между собой данными, опасаясь конкуренции. Но множество устройств никогда не превратятся в цифровую метавселенную вокруг человека, своего рода дополненную реальность, без объединения кросс-индустриальных данных.

При этом мы видим, что с каждым днем человека окружает все больше «умных» устройств и все больше его действий оцифровывается, создавая так называемые цифровые следы. Объединив всю эту информацию, мы можем сделать жизнь человека существенно удобнее. Анализируя данные о человеке — список его покупок в интернет-магазинах, данные фитнес-трекера, его график и другую информацию, возможно формировать для него гиперперсонифицированные рекомендации, строить прогнозы. Таким образом, в ближайшие десять лет мы окунемся в метавселенную данных, где все «умные» устройства, которых мы касаемся, будут накапливать данные и помогать предсказывать наши потребности.

Чтобы это стало возможным, все данные о человеке из разных источников должны аккумулироваться в единой доверенной точке, где их можно было бы анализировать. А поскольку владельцы данных друг другу не доверяют, эта точка концентрации должна находиться на уровне каких-то облачных решений, где информация будет собираться и обрабатываться.

Технология криптоанклавов может стать той самой точкой безопасного объединения данных, метавселенной Data Fusion. Используя криптоанклавы, партнеры передают данные в криптозащищенную область. При этом доступ к их данным отсутствует у других участников анклава, для анализа этих данных применяются строго регламентированные алгоритмы, а на выходе есть возможность получить только результаты применения модели на данных участников, но не сами данные. Если упростить, то криптоанклав — это некий ящик, в который можно положить любые данные, а забрать только то, что разрешено протоколом. Например, для получения медицинского диагноза в криптоанклав можно направить результаты флюорографии. Внутри будет применен AutoML-алгоритм анализа изображения, который обратно вернет диагноз. При этом само изображение останется внутри криптоанклава в зашифрованном виде.

Технология в мире уже применяется, но пока нельзя сказать, что она вышла в большой тренд. Кроме того, самое распространенное решение принадлежит зарубежной компании и его проблематично сертифицировать и использовать в России.

О создании отечественного криптоанклава совместно с МФТИ мы задумались несколько лет назад, осознавая риски возможных санкций. В результате мы работаем над созданием специализированного программно-аппаратного комплекса, который защищен физически и программно. В него можно направить любую информацию и после отработки AutoML-алгоритма получить прогнозы, которые не несут рисков утечки исходных данных. Информация в криптоанклаве хранится в зашифрованном виде. Человек не должен иметь доступ к его данным, а задача извлечения ценности из объединенных данных полностью лежит на плечах AutoML-алгоритмов — роботов внутри криптоанклава, которые извлекают ценность для человека и отдают ее обратно в различные устройства в форме прогнозов и рекомендаций.

Возвращаясь к монополии на данные, криптоанклав дает технологическую возможность обойти такие монополии, не нарушая закона. Но нужно понимать, что для разрушения монополий кроме возможности необходимо еще регуляторное воздействие.

Опытный образец нашего криптоанклава мы планируем протестировать в начале следующего года, а также пройти необходимую сертификацию. Это позволит нам использовать технологию не только внутри банка, но и предложить ее отечественному технологическому рынку.

На первом этапе мы планируем решать задачи классификации и кластеризации в рамках наших партнерств по данным. Пока мы умеем делать очень простые вещи: оценивать риски и говорить, что нужно продавать. Далее задачи могут быть расширены, и мы рассчитываем на интерес к криптоанклаву со стороны компаний из различных отраслей. Например, сфере медицины или госорганам такая синергия данных может быть очень полезна.

Если говорить о влиянии технологии на банковскую отрасль, то изменения будут происходить скорее эволюционно. Предложения для клиентов станут более персонифицированными, рутинные функции можно будет перепоручить цифровому помощнику, который сможет пролонгировать депозиты, контролировать сбережения, предлагать инвестиционные стратегии, исходя из данных о клиенте. Качество планирования повысится, а клиент в результате просто окажется в более комфортной среде.

Общение с предсказаниями

— ликбез —

с13



500 PX / GETTY IMAGES

«Это может быть количество кликов пользователя на сайте, стоимость чека из магазина, температура холодильника или видео камеры наблюдения»,— говорит Михаил Неверов. «Или продажи различных товаров в магазине за день, информация о количестве входящих звонков в колл-центре за каждый час, время ответа чат-бота в чате мобильного приложения за каждую минуту»,— продолжают в сервисе ETNA, разработке Центра технологий ИИ «Тинькофф».

Перед сбором информации нужно определиться с задачами и целевыми действиями, которые важно прогнозировать в рамках конкретного проекта, объясняет Роман Стятюгин. Например, ритейлеры, говорит он, часто хотят заранее понимать, как клиенты отреагируют на предложение в определенной товарной категории, и оценить, насколько предлагаемая скидка влияет на принятие решения о покупке. Банкам важно знать, кто заинтересован в открытии новой кредитной карты, а кто — в инвестиционных инструментах. В этом случае для релевантного предложения от бренда понадобится информация о профиле клиента и трансакционном взаимодействии с ним. В промышленности также достаточно часто используют аналитические сервисы: они помогают предупредить потенциальные аварии и избежать остановки производства и убытков. Специальные датчики отслеживают разные параметры работы и состояния станков, а системы предиктивной аналитики оценивают полученные данные и прогнозируют, какие детали могут выйти из строя.

«Чтобы использовать эти данные, необходимо изменить процессы внутри организации таким образом, чтобы их сбор и накопление стали частью ежедневной работы, не влияя на нее,— подчеркивает Николай Меркулов, заместитель директора по анализу данных и моделированию компании Platforma.— Это может быть использование единой серверной офисной системы вместо разрозненных таблиц на локальных компьютерах, установка датчиков, сбор данных с существующего оборудования. Главное, чтобы эти данные собирались в едином хранилище и по единым стандартам».

Собирать, хранить и обрабатывать данные бизнес может как в собственных системах, так и в частном облаке или в публичных облачных сервисах. Для работы с данными могут использоваться разные решения: от классических баз данных до in-memory технологий и платформ интернета вещей для сбора данных с датчиков, ML-платформ для обучения и тестирования моделей, указывает господин Стятюгин.

Что дальше?

Данные из разнообразных источников в сыром виде агрегируют в data lake — «озере данных» (хранилище данных в естественном или необработанном формате). Их структурируют, фильтруют, проверяют качество и собирают в «витрины данных» — таблицы, из которых алгоритм берет статистику, объясняют в МТС: «Далее строят модели, которые уточняют имеющиеся данные или достраивают знание о неизвестных признаках».

В итоге финальный набор данных становится меньше, чем исходный. И ключевая задача здесь — сохранить ценные инсайты, несмотря на обработку и сокращение объемов признаков, рассуждает господин Стятюгин. После обработки данных нужно подобрать прогностическую модель (алгоритм) и признаки, которые она будет использовать. «Подбор признаков и моделей — большая тема, которой посвящают многочасовые лекции в технических курсах,— говорит Михаил Неверов.— Есть автоматизированные подходы (AutoML), которые решают эту задачу, но чтобы получить максимальную точность, нужна помощь специалиста».

Затем наступает этап эксперимента, после чего аналитики исследуют результаты, детально изучая прогнозы, распределение ошибки, важность признаков с точки зрения модели. «Это нужно, чтобы понимать, чего можно ожидать от прогнозов в будущем,— поясняют в ETNA.— Например, если победившая в результате сравнения метрик модель не учитывает информацию об акциях на йогурты, то нужно понимать, что в будущем она не сможет предсказать пик спроса из-за соответствующей акции». В случае успешного прохождения испытаний предсказательная модель внедряется для регулярного использования или встраивается в существующий сервис, резюмирует Николай Меркулов.

Работа над ошибками

Насколько можно быть уверенным в том, что алгоритмы не ошибутся и подскажут верное решение? Какова вероятность ошибки?

Предиктивная аналитика, как и вся работа с большими данными, строится на статистике и гипотезах, а значит, у нее всегда есть некоторая погрешность, замечают эксперты. Задача — свести ее к минимуму. «Можно быть абсолютно уверенным, что алгоритмы ошибутся, весь вопрос — в величине этой ошибки,— согласен господин Неверов.— Абсолютно точных прогнозов не бывает, только если для тривиальных задач. Люди тысячи лет учатся предсказывать погоду, но точных прогнозов мы так и не получили».

«Вероятность ошибки в алгоритмах во многом зависит от области применения аналитики. При разработке и обучении алгоритмов часто проводятся тесты на ретроспективных данных, а после уже тесты на реальных клиентах,— указывает директор по управлению корпоративными данными „МегаФона“ Сергей Федорченко.— И только после этого происходит масштабирование».

Например, системы распознавания лиц используются для поиска правонарушителей или автоматической оплаты по лицу — цена ошибки в таких системах крайне высока. Разработчики таких решений стремятся свести погрешность практически к нулю. При создании скоринговой антифрод-модели приоритеты расставлены иначе: поиск потенциального мошенника с максимальной точностью и максимально оперативно важнее, чем не зацепить при этом порядочных пользователей, поясняют в МТС: «При условии, что система поможет определить 80% мошенников и фродеров, клиенты готовы на погрешность в 1–2%».

Финансовая сторона

На вопрос, насколько предиктивная аналитика дорогая услуга, эксперты не дают однозначного ответа. Учитывается множество факторов. Все зависит от того, что именно требуется: единичный отчет, регулярное получение услуги, получение продукта или сервиса, в котором есть функционал предиктивной аналитики, или построение функции предиктивной аналитики с нуля внутри компании, перечисляет Николай Меркулов. По его словам, многое зависит от зрелости процессов в компании заказчика: есть ли у него данные, надо ли их покупать, есть ли у него готовый вопрос, который можно задать алгоритму, или сначала этот вопрос надо найти: «В результате стоимость предиктивной аналитики может составлять от нескольких сотен до нескольких миллиардов рублей».

«Важно понимать: чтобы делать проекты с предиктивной аналитикой, в компании должна быть сформирована хоть какая-та культура данных, так как без наличия хороших данных прогнозы не построить,— размышляет Михаил Неверов.— Если данных нет, то нужно начать с построения процессов их сбора и хранения. Это тоже потребует финансовых вложений. И только затем, когда накопятся данные хотя бы за пару месяцев, можно браться за предиктивную аналитику».

Если создавать инфраструктуру предсказательных сервисов с нуля — собирать данные, закупать серверы для их хранения, строить IoT-платформы и нанимать команду, то процесс будет очень дорогим. Речь пойдет о сотнях миллионов рублей, оценивает Роман Стятюгин. Основные причины относительно высокой стоимости решений — высокий порог входа в индустрию. Big Data — одна из самых закрытых областей IT, для которой требуются специальная инфраструктура, дорогостоящие дефицитные специалисты и огромный — в десятки петабайт — объем данных. Стартовые инвестиции исчисляются сотнями миллионов рублей, согласны в МТС с коллегой из VK.

Чтобы сделать технологии доступнее, игроки предоставляют готовые аналитические сервисы по подписке. «Это позволяет даже небольшим бизнесам подключиться к уже проверенным сервисам по приемлемой стоимости,— продолжает господин Стятюгин.— Однако это возможно только в тех случаях, когда процессы и задачи между компаниями относительно унифицированы».

Для предиктивной аналитики нужны два ресурса — люди и вычислительные мощности для обработки данных, говорит господин Неверов. Стоимость решений зависит от сложности аналитики, масштаба работ, потребности в кастомизированной проработке запроса, продолжают в МТС: «Например, геоаналитика может стоить примерно от 7 тыс. руб. для малого бизнеса до нескольких десятков миллионов рублей, если речь идет о долгосрочном доступе к платформе GeoEffect, об анализе данных в разрезе одного или нескольких регионов, анализе ретроданных и консалтинге».

Роман Рожков

информационные технологии

Полупроводников

Начало военных действий на Украине и санкции, как и ожидалось, существенно ударили по российскому рынку высоких технологий. Серьезно пострадали как российские дизайн-центры, которые уже практически год не могут, по крайней мере официально, выпускать чипы на тайваньских фаундри, так и российские производители электроники и микроэлектроники. Последние сейчас из-за санкций вынуждены налаживать альтернативные каналы поставок для ввоза технологического оборудования, нужного для запуска новых производств, и расходных материалов для продолжения текущих. В то же время российские чиновники привычно заявляют: санкции стимулируют развитие отрасли, что постепенно приведет к технологической независимости страны.


АЛЕКСАНДР КОРЯКОВ

— обзор рынка —

Стратегии с национальным колоритом

В ответ на глобальную угрозу зависимости от зарубежных производств полупроводников (в первую очередь от тайваньской TSMC) крупнейшие технологические державы — США, Китай и примкнувший к ним ЕС — разворачивают собственные программы выпуска такой продукции с многомиллиардными бюджетами. Так, американский CHIPS and Science Act подразумевает выделение госинвестиций в размере $280 млрд на развитие полупроводниковой промышленности США ($52 млрд — на развитие производственной инфраструктуры). В феврале Еврокомиссия сообщила о выделении €43 млрд на собственную чиповую инициативу. «В 2015 году Китай запустил программу „Сделано в Китае 2025“, одной из целей которой было создание продвинутых микрочипов,— рассказывает партнер компании „Яков и партнеры“ (ранее McKinsey) Елена Кузнецова.— Уже этим летом было заявлено о появлении микросхем, приближающихся к уровням Тайваня, что побудило США принять собственную программу и ограничить сотрудничество в этой сфере с другими странами».

Пока американские и европейские регуляторы спешно перестраивают индустрию с помощью различных механизмов, российские находятся лишь на этапе планирования развития рынка. Минпромторг только в сентябре подготовил документ под названием «Основы госполитики РФ в области развития электронной промышленности на период до 2030 года и дальнейшую перспективу». В нем регулятор признает зависимость от зарубежных фабрик и технологическое отставание на 10–15 лет. И предлагает участникам рынка координировать «исследования в области передовых технологий», увеличить мощности «в том числе за счет освоения производства микроэлектроники с современными топологическими нормами», создать отрасль электронного машиностроения и отказаться от иностранных архитектур (ARM, x86) при проектировании электроники.

Это уже не первая попытка разработать документ, который определит развитие отрасли на годы вперед. В январе 2020-го Минпромторг подготовил «Стратегию развития электронной промышленности РФ на период до 2030 года». В 50-страничном труде изложены амбициозные плановые показатели. Среди них, например, более чем двукратный рост выручки от продажи продукции российских производителей электроники (с 1,99 трлн до 4,3 трлн руб.), рост объема экспорта российской электроники с $4,4 млрд до $10,09 млрд в год и т. д.

Наиболее смелыми выглядели планы, связанные с модернизацией производственной инфраструктуры и научно-технологическим развитием. С учетом того что на сегодняшний день российские полупроводниковые заводы способны выпускать чипы по топологиям не тоньше 90 нм, Минпромторг рассчитывал разработать «кремниевые технологии производства электронной компонентной базы с топологическими нормами 65–45 нм, 28 нм, 14–12 нм, 7–5 нм и последующий выпуск изделий на их основе».

Член-корреспондент РАН, заместитель заведующего кафедрой микро- и наноэлектроники МФТИ Евгений Горнев подчеркивает: с начала 2000-х Минпромторг разработал ряд стратегий, однако они носили формальный, а не прикладной характер. «Долгое время у индустрии и смежных отраслей — электронного машиностроения, химической промышленности и т. д.— не было единой стратегической цели. НИОКР по этим направлениям шли вразнобой»,— рассуждает он. Еще одной ошибкой, результаты которой сказываются прямо сейчас, стала поддержка проектирования, а не производства: «Средства шли на поддержку дизайн-центров. Теперь мы можем напроектировать микросхем и процессоров, но где их производить?»

Правительство приступило к решению проблемы недофинансированности индустрии в начале февраля текущего года, буквально за несколько недель до начала военных действий на Украине. Источники «Ъ» рассказывали, что Минцифры, Минпромторг и участники рынка планировали разработать отдельный нацпроект для развития российской электронной и микроэлектронной отраслей. Финансирование оценивалось в 3,2 трлн руб. до 2030 года, которые должны были пойти на научные исследования, поддержку производителей через искусственное стимулирование спроса и развитие инфраструктуры. В официальных сообщениях представители Минпромторга признавали эти планы, но говорили, что из 3,2 трлн руб. из бюджета будет выделено только 900 млрд руб., остальная сумма придется на внебюджетные источники.

Других публичных заявлений чиновников о том, какие меры поддержки развития отрасли готовит государство, до сих пор нет. Хотя существенное отставание российской полупроводниковой индустрии от глобальных лидеров очевидно всем.

Макроэлектроника

Согласно ноябрьскому исследованию компании «Яков и партнеры», в настоящее время в России не хватает производственных мощностей для покрытия потребностей в микрочипах даже базового уровня (речь идет о техпроцессах 90 нм и толще). Аналитики оценивают текущий спрос на такие чипы на уровне 30 тыс. 200-миллиметровых кремниевых пластин в месяц, при этом российские предприятия совокупно выпускают лишь 8 тыс. в месяц.

При этом, как отмечают консультанты, сегодня перед российской индустрией и регуляторами стоит задача не только по крайней мере сохранить текущие производственные мощности, но и кратно нарастить их. «В ближайшие пять лет совокупный спрос промышленности на чипы базового и продвинутого уровней может вырасти в два раза и достигнуть 60 тыс. пластин в месяц, а к 2030 году — превысить отметку 100–150 тыс. пластин ежемесячно,— отмечает партнер „Яков и партнеры“ и один из соавторов отчета Тигран Саакян.— Для покрытия столь острого дефицита необходимо срочно запустить простаивающие станки по базовому техпроцессу, а также дополнительно обеспечить импорт технологического оборудования из дружественных стран, в том числе рассмотреть закупку бывшего в употреблении оборудования у производителей из стран Юго-Восточной Азии».

Эксперты подчеркивают: российские предприятия используют лишь 30% от имеющегося оборудования для выпуска полупроводников по топологиям 90 нм и толще. Если бы они запустили все имеющиеся в их распоряжении производственные линии, то ежемесячный объем выпуска чипов можно было бы поднять с 8 тыс. до 26 тыс. пластин.

Впрочем, исполнительный директор Ассоциации разработчиков и производителей электроники Иван Покровский считает приведенные в исследовании показатели и выводы нерелевантными для российского рынка. «Главная трудность — отсутствие инженеров-технологов, способных поставить технологические процессы и обеспечить серийный выпуск микросхем современного уровня»,— уверен эксперт, добавляя, что дефицит таких редких кадров усилился после начала военных действий на Украине и последовавшей мобилизации.

Кроме того, российским властям и индустрии предстоит как минимум довести до конца формирование новых механизмов регулирования и принять ряд протекционистских инициатив. Например, с середины 2021 года Минцифры совместно с Минпромторгом и игроками рынка разрабатывает механизм сквозных проектов в электронике. Он подразумевает создание гарантированного спроса со стороны крупных заказчиков (банков, госкомпаний и т. д.) на еще не выпущенное телеком- и вычислительное оборудование отечественного происхождения. Запуск такого механизма, неоднократно подчеркивали источники «Ъ», позволит производителям вычислительной техники инвестировать в разработку и выпуск российского оборудования, что, в свою очередь, создаст спрос на отечественные компоненты.

Помимо регуляторных механизмов, говорят собеседники «Ъ», необходимо решить ряд критических проблем: наладить серые каналы поставок оборудования, а в перспективе и инвестировать в его инжиниринг, найти стабильных поставщиков расходных материалов, а затем и освоить их выпуск в России и т. д. Наиболее масштабной задачей может стать синхронизация работы не только всех предприятий полупроводниковой индустрии, смежных с ней отраслей и потенциальных потребителей отечественных компонентов, но и профильных институтов и образовательных учреждений, задействованных в проведении НИОКР.

Госпожа Кузнецова считает, что построение независимой от глобальных игроков индустрии вряд ли возможно на горизонте как минимум десяти лет. При этом большой объем необходимых материалов и технологий полностью на своем рынке способны производить и потреблять только США и Китай, что дает им стратегическое преимущество, размышляет эксперт: «Более реалистичный для России сценарий — это развитие производства, которое обеспечивает собственные критические потребности: оборонная промышленность, инфраструктура, часть машиностроения и т. п., а также партнерство с дружественными странами-производителями по остальным направлениям».

Стопроцентная локализация всех поставок не нужна и не реальна, так как требует большого масштаба потребления, который ни одна страна, даже Китай и Индия, не обеспечит, говорит директор по стратегическому развитию АО «Микрон» Карина Абагян. «Во-первых, ряд позиций останутся доступны для импорта, во-вторых, к этой цели нужно идти в альянсе с несколькими странами в плане как R&D-ресурсов, так и объединенных рынков»,— резюмирует она.

Никита Королев

Маркировать строем

— регулирование —

1 сентября в силу вступили поправки к закону «О рекламе». Они предполагают создание единой системы учета всей интернет-рекламы в России и обязательную маркировку каждого объявления. «Ъ» расспросил участников рынка, как им уже пришлось изменить процессы для работы с рекламой в сети и как проект может повлиять на разные сегменты этого рынка.


PIXDELUXE / GETTY IMAGES

Чего требует закон

Закон о маркировке интернет-рекламы меняет процессы закупок по всей цепочке: адаптироваться к новым требованиям приходится и площадкам, и посредникам, и рекламодателям. Все размещаемые в сети объявления должны быть теперь внесены в Единый реестр интернет-рекламы (ЕРИР). Сбор данных осуществляется через посредников — операторов рекламных данных (ОРД; «Лаборатория разработки» «Сбер», «Яндекс Оператор рекламных данных», «ВК Рекламные технологии», «Озон ОРД» и другие).

Для каждого формата рекламы предусмотрена своя система маркировки: объявление должно быть помечено «текстовым идентификатором», который будет означать, что в контенте есть реклама. Под действие закона попадает буквально вся реклама вне зависимости от площадки и формата — даже, например, «кружки» в Telegram попадают под учет, хотя технически их пока маркировать сложно.

Что поменялось в работе компаний

Работу с объявлениями перестроили площадки. С 1 сентября «Яндекс» начал передавать в ЕРИР всю необходимую информацию о рекламе. «На текущий момент в автоматическом режиме маркируются рекламные материалы, размещаемые через „Яндекс.Директ“ и AdFox, поэтапно это реализуется и в „Яндекс Бизнесе“»,— говорят в пресс-службе компании. «Мы сформировали команду, которая занимается разработкой и развитием ОРД. У нас есть весь необходимый запас серверных мощностей, чтобы поддерживать и масштабировать нагрузку на ОРД VK»,— заявил заместитель коммерческого директора по рекламным продуктам и инновациям VK Максим Зенин.

В агентствах технически работа изменилась довольно сильно, особенно процесс усложнился у influence-маркетинга, рассказал основатель рекламного агентства Digital Church Марк Хлуднев. «Теперь необходимо регистрировать каждого участвующего в компании блогера. Это отнимает довольно много времени и увеличивает объем работы сотрудников, при этом новых кадров мы не нанимаем. К примеру, в компании, в которой участвуют 40 блогеров, компания должна занести в ОРД отдельно 40 разных креативов по 40 разным людям по разным соцсетям и т. д.»,— говорит он.

«Были вынуждены взять в штат несколько сотрудников только для задач маркировки и согласования,— объясняет CEO Kokoc Group Александр Шокуров.— Кроме того, новым сотрудникам с координацией сбора необходимой информации помогают все аккаунт-менеджеры группы компаний». Но большинство агентств дартным форматам размещения, где нет возможности добавить кликовую ссылку с токеном или без вреда для объявления добавить требуемые законодательством данные о рекламодателе, отмечает директор по закупкам рекламы в цифровой среде OMD OM Group Ирина Гущина.

Пока до конца не проработаны вопросы маркировки специфических форматов, особенно для мобильных и нативных форматов, указывает директор по технологическим платформам компании «Оккам» Георгий Остапенко. «Странным образом остался непроработанным вопрос отчетности по агентским типам договоров, когда фактически нет бухгалтерского акта закрытия услуг (вместо него есть отчет агента)»,— говорит он. «Остаются не до конца понятной необходимая детализация в части отчетности со стороны агентства/рекламодателя. Например, нужна ли детализация отчетности по поставщикам/площадкам. На рынке, в том числе среди ОРД, есть разные мнения на этот счет»,— добавляет Ирина Козлова.

Больше всего вопросов возникает к активностям у блогеров и в мессенджерах, говорят участники рынка. Как правильно маркировать нативные размещения, партнерские публикации, размещения у блогеров? «На наш взгляд, участники рынка сейчас различно трактуют закон, что вызывает путаницу»,— отмечает аналитик Roistat Виталий Горюнов. «Реклама, интеграция у блогеров, органическая реклама и бартер — это совершенно другой мир, который отличается коммуникацией с аудиторией и многими другими аспектами от стандартной рекламы»,— рассказывает операционный директор платформы по работе с блогерами Perfluence Евгения Казакова. «Токены (в контенте блогеров.— **„Ъ“**) присваиваются некорректно, и в целом происходит какая-то путаница. От таких интеграций рекламодатель и аудитория ждут нативности, а маркировка ее убивает»,— сетует директор группы по диджитал-направлению NMI Group Михаил Дубровин.

Как закон повлияет на нативность инструментов

О нативности в контексте закона о маркировке возникает больше всего споров в отрасли. Пострадают прежде всего сами нативные форматы — размещения у инфлюенсеров, уверены эксперты. «Посевы, посты в каналах блогеров однозначно перестанут выглядеть так, будто их сделал сам автор канала или сообщества»,— утверждает Виталий Горюнов из Roistat. «Все бесшовные и нативно интегрированные в инфополе пользователей механики теперь такими не могут называться. Выдают хештеги вроде #партнерский_пост или #нативная_интеграция. Искренние личные рекомендации авторов постов становятся не такими уж и искренними»,— согласен Александр Шокуров.

Маркировка очень сильно повлияет на нативность рекламных инструментов, также считает Марк Хлуднев. «Мы наблюдаем это прямо сейчас: у нас довольно сильно сбилась точность прогнозов рекламных кампаний, и это проблема. Условно сейчас у нас проходят крупные рекламные кампании, и из-за маркировки мы расходимся по прогнозам примерно на 30–35%»,— делится он.

Впрочем, есть и те, кто считает, что этот страх преувеличен. «Аудитория понимает, что промопосты у блогеров — это реклама, например, как и многие другие нативные форматы»,— более оптимистична в то же время Ирина Козлова. Вряд ли падение доверия к блогерам будет значительным, согласна руководитель российского подразделения партнерской сети Admitad Екатерина Бибик: «Мы ожидаем, что маркировка не должна повлиять на спрос рекламодателей на этот формат. Скорее она скажется на манере или способе представления рекламы блогерами и создателями контента».

Споры по поводу потери нативности возникают и в связи с другими рекламными форматами, не только у блогеров. «Например, видеоанонс мероприятия с указанием всех спонсоров мероприятия. У большого мероприятия могут быть десятки спонсоров-рекламодателей. Если в отношении каждого рекламодателя в креатив интегрировать название и токен, то, да, привлекательность такого ролика может, очевидно, пострадать»,— добавляет директор юридического департамента и комплаенс Group4Media Анна Малиновская.

Изменятся ли объемы закупаемой рекламы

Неопределенность относительно новых правил осенью сказалась на объемах закупаемой рекламы в некоторых сегментах. «В середине августа такое поведение наблюдалось у отдельных рекламодателей, которые не могли решить, как запускать кампании в сентябре»,— говорит Георгий Остапенко. Надзорные органы обещают не штрафовать за нарушения до марта 2023 года, кажется, что это уже сильно успокоило рынок, отмечает Ирина Козлова.

В долгосрочной перспективе новый закон не повлияет на объемы закупаемой интернет-рекламы: они больше зависят от потребностей рынка и количества каналов распространения информации, чем от особенностей регуляторики, считает сооснователь Vinci Agency Мария Лапук. Новый порядок избавит рынок от совсем уж незаконных схем размещения, в остальном исполнение закона на объемы инвестиций не повлияет, полагает Михаил Дубровин: «Те, кто заинтересован в performance, будут и дальше вкладываться в digital».

«Белый рынок никак не поменяется, на сером и черном станет сильно меньше крупных рекламодателей, так как это повлечет за собой сложности в учете расходов на рекламу. После того как все лакуны в законе будут устранены, рынок вернется в равновесное состояние. Но сейчас действительно есть сложности с блогерами, диджитал-аудио и рядом других видов размещений, которые не были однозначно описаны в федеральном законе»,— предупреждает Вадим Мельников.

Валерия Лебедева

информационные технологии

Вселенная токена

В интернете версии 2.0 правят огромные платформы и корпорации, которые устанавливают правила, манипулируют пользователями и обогащаются за счет навязчивой рекламы на основе их данных, а централизованное хранение создает идеальные условия для хакеров и цензуры. Так рассуждают критики парадигмы, в которой сегодня существует интернет. Значит, делают вывод они, ее нужно менять. По словам сторонников преобразований, интернет будущего — Web3 — может и должен стать свободным, безопасным и, главное, децентрализованным, где пользователи будут полноценными владельцами цифровых активов, а не только их создателями и потребителями, как сейчас. Что это — абстрактная идея или действительно новая модель, ростки которой уже пробиваются сквозь асфальт, казалось бы, уже намертво устоявшейся модели?

— феномен —



ЭМИН ДЖАФАРОВ

Апологеты концепции Web3 критикуют крупнейшие IT-компании за то, что они накопили слишком много власти и влияния, активно монетизируя данные своих пользователей

Что предшествует появлению

Около 30 лет назад жизнь человечества перевернулась. С изобретением интернета и его постепенным распространением по планете у людей появились возможности, о которых предыдущие поколения могли только мечтать: стало гораздо проще находить информацию, общаться, делать покупки, учиться или работать онлайн и многое другое. Сегодня без него мы практически не можем представить себе любой наш день: по данным исследования Global Digital 2022, среднестатистический пользователь проводит в сети 7 в сутки, а россиянин и того больше — 7 часов 50 минут.

Чтобы такие цифры и процессы стали возможными, интернет пережил несколько больших этапов, которые кто-то сравнивает по значимости с промышленными революциями. Строго говоря, мы прожили Web 1.0 и сейчас живем в эпоху Web 2.0. Каждый этап кардинально отличается от предыдущего. Так, интернет на заре своего развития, в 1990-х,— это Web 1.0. «Сайты были статичны, весь контент генерировал владелец сайта, который, в свою очередь, создавался разработчиками,— вспоминает директор департамента разработки ПО „Рексофт“ Николай Сокорнов.— Посетитель сайта мог только читать выложенную информацию, в редких случаях — отправить на почту владельцев сайта комментарий, он проходил модерацию и выкладывался администратором ресурса».

В 2000-х с развитием технологий стало доступно динамическое взаимодействие пользователей и интернет-ресурсов и платформ — это и стало рождением Web 2.0. Ключевое отличие от первой версии веба: теперь пользователь мог легко публиковать свой контент без привлечения IT-специалистов (писать комментарии, загружать фото, видео и т. п.). Контент генерирует уже не владелец ресурса, который лишь предоставляет платформу, а пользователи.

Однако за этим «лишь» кроется настоящая революция. Компании стали размещать данные в облаках, арендованных у дата-центров, а соцсети превратились в главный центр общества для обмена новостями, фотографиями, эмоциями и планами, указывает руководитель направления пиринга Eurasia Peering IX Олег Огиенко. «Они также стали диктовать или рекомендовать контент — то, что пользователи хотят посмотреть или купить на основе проставленных лайков, просмотренных или прерванных видео и даже поиска информации,— говорит он.— Учитывается и то, с какой территории мы заходим на ресурс. Все это породило мощный инструмент для маркетинга».

С выпуском iPhone в 2007 году мобильный доступ в интернет значительно расширил как базу пользователей, так и время, которое мы проводим там: от подключения к сети через телефонную линию на несколько часов в день дома мы перешли к состоянию «всегда онлайн»: веб-браузер, мобильные приложения и персональные уведомления теперь были у каждого в кармане.

«Сейчас мы оставляем громадные цифровые следы: предпочтения, банковские транзакции, история поиска, любимые сериалы, рестораны, паблики, тиктоки, фото, игры, семья, друзья — о нас можно узнать все,— рассуждает Даниил Андриянов, основатель True, платформы для вывода брендов в Web3.— Все эти данные о нас нам не принадлежат, они в конечном счете попадают в корпорации, которые успешно продают их рекламодателям. Те, в свою очередь, придумывают хитрые рычаги давления, чтобы указать или даже искусственно создать потребность в определенном товаре или услуге».

Любой пользователь в парадигме Web 2.0, сам о том не подозревая, является активом, за который идет подпольная борьба между брендами. «Web 2.0 породил понятие FANG (Facebook, Amazon, Netflix, Google), в России — МЯСО (Mail, „Яндекс“, „Сбер“, Ozon). Аббревиатурами обозначаются интернет-гиганты, которые фактически владеют контентом и всеми персональными данными, относящимися к нему»,— объясняет Николай Сокорнов.

Такая централизация нравится не всем. В итоге появился тренд, где ценность честности и открытости, желание самому управлять своими активами и контентом оказывается в начале списка приоритетов, говорит Даниил Андриянов: «Этот запрос и стал основной предпосылкой появления Web 3.0».

Как должен выглядеть

Как же, по мнению апологетов новой парадигмы, должен измениться интернет? Например, один из отцов интернета, Тим Бернерс-Ли, считал, что это будет принципиально новый «семантический веб», надстройка для Web 2.0. По мнению же Гэвина Вуда, сооснователя Ethereum, который и ввел в 2014 году термин Web3, это должна быть децентрализованная онлайн-экосистема сервисов и приложений, созданная пользователями для пользователей. Она основана на технологиях блокчейн, делает упор на контент и призвана помочь пользователям контактировать друг с другом более свободно и с большей пользой, говорит директор по маркетингу разработчика ПО «Аурига» Наталья Панина.

Сейчас, заходя в соцсеть, мы в общем уверены, что профиль Ивана Иванова действительно принадлежит человеку, которого мы знаем под этим именем, а продавец мягких игрушек на Ozon или Avito, если что, вернет нам деньги, рассуждает Николай Сокорнов: «И продавца, и Иванова проверили площадки. Если посредников нет, то нужен какой-то инструмент, заменяющий этот механизм. Предполагается, что основой этой технологии выступит блокчейн. А необходимую пользователю информацию в распределенной сети найдет и извлечет искусственный интеллект».

Децентрализация и «отвязка от крупных компаний» — ключевой момент для Web3, указывают эксперты. Станет возможным отказ от хранения данных на серверах корпораций и их размещение на устройствах всех пользователей сети, а приложения и сервисы будут распределены между ее узлами, объясняет гендиректор «Ланит-Теркома» Вадим Сабашный.

По такому же принципу работают сейчас торренты, когда вы загружаете контент не с определенной точки в сети — сервера, а забираете его у тех пользователей, кто успел его раньше скачать, проводит аналогию директор по развитию веб-технологий Artezio Сергей Матусевич: «Такой формат, с одной стороны, гарантирует свободное распространение информации и отсутствие цензуры, с другой — сильно тормозит получение данных». По мнению Вадима Сабашного, расчеты между пользователями будут происходить в криптовалютах с использованием принципа шардирования, когда для ускорения трансакций сеть разделяют на небольшие части. При этом блокировка даже 10–20% узлов не влечет остановки приложений и сервисов.

Технологии, используемые во фронтенде, будут примерно такими же, что применяются сейчас для разработки решений Web 2.0, но с упором на блокчейн, например специализированные языки для написания смарт-контрактов, полагает господин Сабашный: «С ростом популярности Web3 IT-ландшафт значительно эволюционирует, появятся новые технологии и библиотеки. С точки зрения пользователя может увеличиться доля AR/VR/XR в формате представления решений, но будут присутствовать и классические браузерные продукты».

Вариант, который, по мнению CTO CodeInside Владислава Егорова, кажется более вероятным,— перемещение всех тяжелых вычислений в облако и максимальное облегчение терминалов: «ПК, лэптоп, телефон могут стать только дверью в мир Web3, а достаточные вычислительные ресурсы могут предоставляться поставщиком как сервис».

На что способен

Чтобы изменения в модели функционирования интернета происходили, участники этих преобразований должны понимать преимущества этого. На что способен децентрализованный интернет и как эволюция сети может изменить жизнь пользователей?

«Web3 стремится реорганизовать экономику вокруг цифровых активов — новых валют, токенов и форм собственности, таких как NFT (невзаимозаменяемые токены, на которых строится ряд принципов Web3.— „Ъ“), защищенных математикой, а не законом, обычаем или силой»,— пишет Скотт Розенберг из Axios. По его словам, сторонники Web3 рассматривают новую модель как способ «исправить то, что сломано в существующей экономике» — так, с ее помощью можно разрушить концентрацию власти банков, компаний и миллиардеров, предоставить креаторам лучшие способы получения доходов от своей работы, внедрить новые методы совместной работы групп людей и объединения ресурсов как в онлайне, так и в материальном мире.

«Web3 — это те же сайты и сервисы, к которым привык обычный пользователь, только все данные легко проверяемы в блокчейнах. Это ваши права на ваши активы, и никто другой не имеет к ним доступа: ни банки, ни государство, ни кто-то еще. Это отсутствие посредников между поставщиком и потребителем, логика программного кода, которую невозможно подкупить или подменить задним числом»,— перечисляет Даниил Андриянов.

Как рассуждают в своем эссе основатели Fabric Ventures Ричард Мюрхед и Макс Мерш, Web3 — это шаг вперед к открытым сетям, «не требующим доверия и разрешений». «„Открытым“ в том смысле, что они созданы на основе ПО с открытым исходным кодом, созданного сообществом разработчиков на виду у всего мира,— объясняют они.— „Не требующим доверия“ в том смысле, что сама сеть позволит участникам взаимодействовать публично или конфиденциально без доверенной третьей стороны. „Без разрешения“ в том смысле, что пользователи и поставщики смогут действовать без разрешения руководящего органа».

Новая модель устройства сети способна улучшить практически каждую отрасль и направление бизнеса, уверен Даниил Андриянов. «Например, в играх (в частности, NFT) она позволит делать из привычных игровых скинов реальные финансовые активы, которыми пользователь может распоряжаться по своему усмотрению вплоть до перепродажи на свободном рынке,— рассуждает он.— Таким образом, ты получаешь от игры не только развлечение, но и вполне официальную возможность финансового дохода». В благотворительности можно прозрачно проследить, кому ушли конкретно твои деньги, продолжает он.

Основная возможность — появление систем, живущих и эволюционирующих без участия исходного создателя, считает господин Сабашный. «В подходе Web3 могут меняться само решение и правила создания контента. Метавселенные строятся именно на подобных принципах. В силу распределенной архитектуры и возможностей по масштабированию приложения станут более устойчивыми к резкому увеличению количества запросов, атакам и блокировкам,— рассуждает он.— Пользователи все больше будут взаимодействовать с различными вариациями метавселенных, постепенно отходя от статической формы подачи информации. Важность приобретает не только место, но и время, когда она представляется».

Кроме того, важнейшей составляющей Web3 являются алгоритмы искусственного интеллекта и машинного обучения, которые стали достаточно мощными, чтобы создавать полезные, а иногда и спасающие жизнь решения. «Будучи наложенными поверх новых децентрализованных структур данных, дающих доступ к огромному количеству данных, которым позавидовали бы современные IT-гиганты, потенциальные приложения и сервисы выходят далеко за рамки целевой рекламы и распространяются на такие области, как прецизионные материалы, разработка лекарств или моделирование климата»,— пишут Ричард Мюрхед и Макс Мерш.

За что критикуют

Критических стрел, безусловно, в новую модель интернета тоже выпущено предостаточно. Парадигма Web3 предполагает знакомство с криптовалютами, наличие кошельков и средств на них, а это значительно сужает аудиторию. Из-за общей неподготовленности и большого количества противоречивой информации появляются скам-проекты, что негативно сказывается на имидже подобных решений, обращает внимание Вадим Сабашный, добавляя, что в России к тому же нормативная база хождения криптовалют не регламентирована. Использовать сегодня концепцию Web3 повсеместно невозможно, согласен Олег Огиенко, потому что пользователям надо научиться определять и монетизировать собственную выгоду от этого решения.

Осведомленность пользователей пока еще на весьма низком уровне, признают эксперты. «Сфера новая, и не все юзеры знакомы с правилами, из-за чего их легко обмануть,— сетует Даниил Андриянов.— В Web3 безопасность твоего кошелька зависит только от тебя: если ты потерял кодовую фразу, то восстановить ее, позвонив в банк, не выйдет, к самостоятельности надо привыкать».

Едва ли не главная на текущий момент проблема модели — безопасность данных. «Представьте, что мы живем во время Web3, когда сайты злоумышленников нельзя блокировать, как и страницы блогов, новостных лент, когда логин и пароль в виде кошелька можно не просто украсть, но и забрать все деньги,— говорит Сергей Матусевич.— Интернет изменился настолько, что сделать его свободным, отделить от регулирования — это все равно что выпустить джинна на свободу». Он убежден, что найдутся те, кто найдет способ применения благих возможностей во вред другим людям: «В Web 2.0 защита существует, но будет ли она работать с Web3?»

Прозрачность и открытый исходный код создают массу возможностей для недоброжелателей, которые часто этим пользуются для поиска уязвимостей, согласен господин Андриянов. По его словам, централизованные системы более надежны и защищены от атак злоумышленников, ведь, чтобы спланировать атаку, нужно найти тонкое место — в открытых системах это сделать легче, чем в закрытых. «Из-за ранней стадии развития рынка еще очень мало опыта и продуктов, которые помогают выявить угрозы на этапе проектирования систем»,— резюмирует он.

Николай Сокорнов видит «концептуальную проблему» в Web3. «Мы живем в централизованном обществе, а запрос для взаимодействия в сети идет на децентрализацию. С моей точки зрения, так не бывает,— рассуждает он.— Интернет — это виртуальное отражение текущего мироустройства. Мы все далеко не фрилансеры-одиночки, работающие на себя: у нас есть работодатели, которые платят нам зарплату, организуют бизнес. Государство устанавливает законы и правила, но одновременно много чего нам и гарантирует». Децентрализация, по его мнению, поднимает не только вопрос технологий, но и вопросы социального, юридического, государственного порядка: «Мы видим, как поменяли мироустройство технологии Web 2.0. Политики, корпорации строят свои кампании и бизнес с учетом влияния соцсетей, существенно поменялся паттерн человеческого поведения».

Появление децентрализованного интернета приведет к тому, что сеть вообще никто не сможет регулировать и навязывать в ней какие-то правила, считает господин Матусевич. Для пользователей это можно считать позитивным изменением, но интернет, в котором не будет центров влияния, не сможет обеспечивать свою стабильность и выполнение даже базовых норм безопасности, убежден он: «Если сейчас блокчейн можно рассматривать как безопасную технологию, то с приходом в нее значительного числа людей и большого капитала все может измениться».

Каким может быть противодействие

Наивно было бы предполагать, что участники рынка, которых критикуют сторонники Web3 из-за той самой централизации, будут безучастно смотреть, как меняется интернет. Наверняка противостояние будет, «и оно будет непреодолимым», считает Сергей Матусевич: «Переход на Web3 ознаменует потерю бизнеса, который приносит миллиарды долларов компаниям по всему миру». Действительно, согласно оценкам eMarketer, в 2021 году бренды инвестировали в продвижение по цифровым каналам $491,7 млрд (почти на 29% больше показателя прошлого года), расходы на digital-рекламу в России по итогам 2021-го составили $3,9 млрд. Вряд ли кто-то намерен отказываться от участия в разделе такого пирога.

Кроме того, нужно учитывать, что на стороне провайдеров будут правительства стран, которые вложили огромные средства в системы контроля Web 2.0, рассуждает господин Матусевич. Переход к Web3, по его мнению, не только обнулит эти вложения, но и поднимет планку инвестиций в контроль на космический уровень. Вопрос не в том, что поступательному движению к Web3 будут препятствовать некоторые игроки рынка, полагает Наталья Панина, проблема в том, что пока сама идея «сырая и недоработанная как технологически, так и этически».

Впрочем, возможно, что, увидев выгоду от использования Web3 и возможности монетизации, игроки будут адаптировать свои решения под новую парадигму и использовать ее для повышения их популярности, допускает Вадим Сабашный. Сила инерции будет зависеть от того, получит ли Web3 своего рода ранних последователей в лице крупных компаний, которые увидят для себя выгоду в переходе на Web3, полагает директор по маркетингу и коммуникациям цифровой платформы «Ракета» Дарья Зубрицкая.

Даниил Андриянов и вовсе утверждает, что в основном компании не противятся новому, так как видят в Web3 определенные преимущества: новые источники дохода и механики для вовлечения аудитории, снижение расходов на маркетинг, трендовое восприятие бренда. «Они скорее пытаются навязать свои правила игры, пока рынок еще молодой и развивающийся»,— говорит он, напоминая, что уже многие известные бренды успешно используют Web3 для продвижения продукции и общения с покупателями и контрагентами. Так, Nike вошел в число гигантов, выпустивших фирменную NFT-коллекцию: на рынок она вышла в апреле 2022 года, а продажи токенизированных кроссовок принесли компании $185 млн.

На самом деле список крупнейших компаний, которые экспериментируют с новыми технологиями Web3, руководствуясь принципом «если это невозможно остановить, это нужно возглавить», довольно обширен. Несколько примеров навскидку. Так, в феврале Spotify разместил на LinkedIn вакансию разработчика, ориентированного на Web3, в марте American Express подала заявку на товарный знак для логотипов Metaverse и NFT, в мае Google Cloud объявил о создании нового подразделения для инфраструктуры Web3, а eBay — о выпуске коллекции NFT-токенов с Уэйном Гретцки. Чуть позже Binance привлекла $500 млн от DST Global, Breyer Capital и неназванных семейных офисов и корпораций в фонд для развития проектов в Web3.

Как бы то ни было, эксперты сходятся в одном: хоть отдельные технологии Web3 уже сейчас присутствуют в текущей версии веба, полноценное введение новой модели не так уж и близко и горизонт планирования составляет годы. «Сейчас Web 3.0 в самом зачатке. Как интернет конца 1990-х: вроде он был, но немногие еще понимали, зачем он нужен,— говорит Даниил Андриянов.— Так и сейчас: немногие понимают смысл децентрализованных приложений и принципов открытости данных. Но уже через несколько лет, как только пользовательские интерфейсы будут понятны рядовому пользователю, никто не будет воспринимать эти технологии как нечто незаурядное».

Роман Рожков

Тематические страницы газеты «Коммерсантъ» («Информационные технологии»). | **Владимир Желонкин** — генеральный директор АО «Коммерсантъ», главный редактор | **Сергей Вишневский** — руководитель фотослужбы | **Рекламная служба:** Тел. (495) 797-6996, (495) 926-5262 | **Владимир Лавицкий** — директор «Издательского синдиката» | **Роман Рожков** — выпускающий редактор | **Ольга Еременко** — редактор | **Сергей Цомык** — главный художник | **Галина Кожеурова, Екатерина Репях** — фоторедакторы | **Екатерина Бородулина** — корректор | Ограничение: 16+