За счет чего растет объем российского рынка видеоигр и как он будет развиваться в будущем | 16

ИТ

Тематические страницы газеты **Коммерсантъ**

Информационные технологии

Среда 16 октября 2024 №190 (7880 с момента возобновления издания) **kommersant.ru**

14 Как ключевые отрасли справляются с дефицитом IT-кадров и как подбирают специалистов

20 Оправдаются ли прогнозы по росту IT-рынка в РФ

21 Как традиционные поисковые сервисы конкурируют с системами поиска на основе искусственного интеллекта

Хома sapiens

Одним из главных феноменов 2024 года стали криптоигры в Telegram, обещающие пользователям реальные деньги за действия в игре. Так, игра Hamster Kombat, где пользователи «тапают» ставшего знаменитым хомяка, 26 сентября уже разместила свой токен HMSTR на нескольких крупнейших криптобиржах. Однако эксперты предупреждают, что игры в мессенджере может ждать судьба других популярных криптопроектов. „Ъ“ разобрался, откуда появились такие игры, как к ним добавился блокчейн и по какой экономической модели они работают.

— игры в мессенджерах —

АНТОН НОВОДЕРЕЖКИН

Весной текущего года в соцсетях завирусилась созданная внутри мессенджера Telegram игра Hamster Kombat, в которой пользователям нужно кликать на экран и зарабатывать внутриигровую валюту. Эта простая P2E-игра (где пользователь выполняет разные действия и получает за них виртуальную валюту) за несколько месяцев стала одной из самых популярных мобильных игр. Она стала доступна в марте, а уже 31 мая число пользователей достигло 60 млн человек, из которых 24 млн играли ежедневно. К 14 июня количество пользователей удвоилось. Создатели отчитались о том, что более 150 млн игроков «нажимают на хомяка» в надежде заработать.

26 сентября токен Hamster Kombat, HMSTR, добавили на несколько крупнейших криптобирж, включая Bybit, Binance, OKX. Ранее пользователи массово жаловались на конвертацию внутриигровой валюты. Например, сумма за 100 тыс. монет составила около $10, а наиболее активные игроки получили в среднем более 1 тыс. руб.

С чего начались криптоигры в Telegram

Первые криптоигры, которые работают на блокчейне, появились еще в 2010-х годах, одной из самых популярных стала CryptoKitties, выпущенная в 2017 году. Там пользователи могли покупать и продавать виртуальных котят, а саму игру запустили на Ethereum. Количество ее пользователей превысило 1,5 млн человек.

Первые же игры в Telegram появились в 2016 году. Тогда в мессенджере появились простые чат-боты с HTML5-играми (запускаются прямо на странице браузера), в которые можно поиграть с собеседником, в группах или приватных чатах. Однако большой популярности такие игры не получили. Затем в 2018 году Павел и Николай Дуровы запустили блокчейн-экосистему TON — сокращение от Telegram Open Network. Два года спустя они отказались от проекта из-за судебных разбирательств с Комиссией по ценным бумагам и биржам США.

В апреле 2022 года у Telegram вышел первый релиз Web Apps в рамках обновления Bot API 6.0, который позволил пользователям запускать сайты (веб-приложения) внутри диалога с ботом, не покидая мессенджера, рассказывает аналитик финансового холдинга VG Group Виталий Будич. В 2023 году была добавлена возможность открывать веб-приложения в Telegram по прямой ссылке.

Также был создан игровой проект Notcoin — его запустили разработчики Open Builders (платформа для разработчиков) и поддержала Ton Foundation, организация, которая стояла за развитием сети The Open Network, выросшей, в свою очередь, из проекта Telegram Open Network разработчиков Telegram, объясняет гендиректор Tehnobit Александр Пересичан.

Ее развитию помогла грамотно выстроенная маркетинговая кампания: игру активно продвигали через инфлюенсеров и каналы, связанные с криптовалютой, говорит главный аналитик Bitget Research Райан Ли. «В течение первой недели после запуска количество игроков Notcoin достигло 5 млн, а к апрелю превысило 30 млн. Важным показателем для таких игр является и количество активных пользователей в сутки (daily active users, DAU.— „Ъ“). У Notcoin к весне этот показатель достигал 6 млн DAU. После успеха Notcoin стали появляться другие игры-тапалки, среди них самой популярной стала Hamster Kombat»,— отметил господин Ли. Первой криптоигрой на основе Telegram можно считать Notcoin, но основным периодом развития игровых мини-приложений в Telegram стал 2024 год, заключает он.

Цена аудитории

Весной 2024 года Notcoin вышел на ряд международных бирж, и пользователи смогли обменивать монеты NOT, которые получили бесплатно в приложении, на валюты USDT и TON, рассказывает Александр Пересичан. «Это стало почвой, на которой выросла и популярность Hamster Kombat: пользователи почувствовали возможность заработать монеты, которые в дальнейшем могут иметь какую-то цену»,— добавляет он.

Успех Hamster Kombat связан и с тем, что игра появилась в нужное время, сопровождалась качественной маркетинговой кампанией и предлагала игрокам нужный им игровой опыт, объясняет Райан Ли. «У Hamster Kombat очень хорошо продуман геймплей, то есть игровой процесс. С одной стороны, он понятный и доступный даже ребенку: нужно кликать по экрану. С другой — нужно постоянно прокачивать своего игрока, покупать за заработанные монеты улучшения. С первым популярным Telegram-кликером Telegram сделал ставку на продвижение Notcoin внутри собственной платформы и не стал работать с внешними источниками трафика»,— говорит он. По словам Райана Ли, причиной успеха Hamster Kombat стало и активное продвижение у блогеров на YouTube и на других платформах.

С этим согласен Виталий Будич: «Роль сыграли хорошая проработка игровых и социальных механик, а также использование темы „хомяков“, которая привлекает пользователей, маркетинг и реклама — активное продвижение игры и связанного с игрой контента блогерами по разным каналам (от Telegram до TikTok, YouTube и криптобирж)».

При этом бизнес-модель подобных простых игр — это продажа рекламы многомиллионной аудитории, объясняет Александр Пересичан. «Поэтому главная их цель — быстро нарастить пользовательскую базу. Также эти игры имеют реферальную программу: пользователь, пригласивший в игру друга, получал единовременное вознаграждение во внутриигровой валюте и часть от заработанных монет»,— говорит он.

При этом в Hamster Kombat монетизация была больше сконцентрирована на продаже рекламных мощностей в YouTube, приложении и Telegram-канале, добавляет Райан Ли. «Среди рекламодателей были такие гиганты, как ВТБ и „Яндекс“. По сути, бизнес-модель похожа на то, как зарабатывают поисковики. Пользователей Hamster Kombat сначала мотивировали с помощью вознаграждений подписываться на каналы игры, а затем в этих каналах появлялась реклама различных компаний и сервисов»,— говорит он.

Сезонность модели

История успеха Notcoin показывает, насколько эффективны экосистемы Telegram/TON для разработчиков приложений,— писал в мае Павел Дуров в своем Telegram-канале. «Telegram предлагает разработчикам больше свободы, чем любая другая платформа, предоставляя непревзойденные возможности для использования социальных взаимодействий для вирусного распространения. TON, в свою очередь, обеспечивает масштабируемость и гибкость любого блокчейн-проекта».

Тем не менее опрошенные „Ъ„ эксперты сомневаются в устойчивости бизнес-моделей игр, созданных по принципу Hamster Kombat, в долгосрочной перспективе. «Когда запущен токен и заканчиваются экономические стимулы, у пользователя меньше ценности продолжать играть»,— говорит Виталий Будич. По его словам, это может случиться сразу или через некоторое время — как, например, происходило с корреляцией цены токена и количества активных пользователей после снижения стоимости токена в play-to-earn проектах Axie Infinity и STEPN из прошлых циклов рынка. «Без доработок такую модель можно применять только для ограниченных сезонных акций, где нет потребности удержать внимание пользователя долгое время»,— заключает он.

«Вызывает опасение и качество самой аудитории игры. В Hamster Kombat активно играют школьники — они не представляют ценность как аудитория для рекламодателей»,— считает Александр Пересичан. К тому же любая игра сталкивается с кризисом: игрокам хочется чего-то нового, и уже знакомый игровой процесс не приносит им удовольствия.

Хайп без дела

Вечером 24 августа Павла Дурова задержали в аэропорту Ле-Бурже во Франции. Вскоре прокуратура Парижа заявила, что господину Дурову предъявлены обвинения, среди которых соучастие в администрировании онлайн-платформы для совершения незаконных трансакций организованной группой, отказ от предоставления уполномоченным органам сведений или документов по их запросу, а также сокрытие преступлений в составе группы.

Опрошенные эксперты не считает, что дело Павла Дурова повиляет на перспективы криптоигр в Telegram. «На следующий день после его ареста приложение Telegram заняло вторую строчку в разделе „Соцсети“ в США по количеству скачиваний в магазинах приложений, во всем мире выросло количество общих загрузок iOS на 4% по сравнению с прошлым днем, следует из данных TechCrunch»,— говорит Виталий Будич.

Он добавляет, что на текущий момент Telegram сохраняет лидерство с точки зрения платформы с самым большим потенциалом по онбордингу (адаптация пользователя к продукту) в мир Web 3.0. «Уже сейчас каждому из 900 млн пользователей Telegram доступен встроенный кошелек Telegram Wallet и мир мини-приложений, а значит, он находится буквально в нескольких шагах от получения первого опыта взаимодействия с блокчейн-технологиями: игры, токены, NFT и прочее»,— говорит Виталий Будич.

«Думаю, хайп вокруг игр-тапалок в Telegram угаснет ближе к концу года. И связано это будет не с делом Дурова, а с обычным жизненным циклом любой технологии: сначала взлет, затем падение и медленное развитие или угасание. Можно вспомнить ажиотаж вокруг блокчейн-игр в 2017 году или play-to-earn игр с NFT в 2021 году. Например, легендарная NFT-коллекция Bored Ape Yacht Club потеряла 91% своей стоимости за два года»,— добавляет господин Пересичан.

«Дело Павла Дурова, скорее, может негативно повлиять на интеграцию TON и Telegram, развитие криптовалютных сервисов, таких как криптокошельки или биржи на блокчейне TON внутри мессенджера, так как один из пунктов его обвинения — это незаконные трансакции»,— заключает Райан Ли.

Алексей Жабин

Технологиям добирают внешние факторы

— правила игры —

По итогам первого квартала 2024 года IT-рынок в России показывает устойчивый рост: по данным аналитиков ВШЭ, объем реализации товаров и услуг год к году вырос на 32,6%, до 1,7 трлн руб., а инвестиции в основной капитал — на 79%, до 724 млрд руб. Однако ряд трендов, в том числе растущая ключевая ставка ЦБ, говорит о том, что в ближайшее время рост IT-рынка может замедлиться, а сам сегмент ждут сделки по слиянию и поглощению. Участники IT-рынка предполагают, что целями M&A станут компании, которые при росте рынка на фоне импортозамещения не рассчитали свои силы, нарастили затраты и потеряли контроль над маржинальностью.

IT рынок разогрелся цифрами

Согласно отчету Института статистических исследований и экономики знаний НИУ ВШЭ «Российский сектор ИКТ в I квартале 2024 года», индустрия информационных технологий (в эту категорию аналитики института включают разработку софта, производство электроники, телекоммуникационный рынок, а также сектор оптовой торговли ИКТ-товарами) наращивает темпы роста. Так, например, объем реализации товаров работ и услуг по итогам первого квартала вырос на 32,6% год к году, до 1,7 трлн руб. Динамичнее всего растет IT-отрасль (+58% год к году, до 792 млрд руб.). В целом же показатели почти всего сегмента, судя по отчету ВШЭ, остаются «зелеными» (см. инфографику).

Тренд в институте связывают с «продолжающимся наращиванием объема собственных разработок и реализации отечественных продуктов и услуг в IT-отрасли», а также с ростом инвестиций в создание сборочных линий в секторе производства электроники.

Но уже со второй половины 2024 года рост сегмента может замедлиться, и в первую очередь речь может идти о снижении инвестиций компаний в основной капитал, а также в научно-исследовательские и опытно-конструкторские работы (НИОКР). По сравнению с 2022–2023 годами, когда чувствовалась активная финансовая поддержка, во многом обоснованная низкой ключевой ставкой ЦБ, инвестировать в НИОКР могли себе позволить любые компании: от стартапов до крупнейших игроков рынка, рассуждает аналитик Directum Наталия Башурова.

Но с конца 2023 года, продолжает она, все стали осторожнее в своих инвестициях и переходят к более консервативным стратегиям. Крупные компании с сильными финансовыми показателями менее чувствительны к изменению ставки и продолжают инвестировать в НИОКР. Стартапы и малый бизнес, которые еще не достигли стабильной прибыльности, судя по снижению числа новых решений на рынке, начали испытывать больше трудностей с привлечением финансирования и сократили инвестиции в НИОКР.

При этом на российском IT-рынке можно отметить сразу две глобальные тенденции, которые в перспективе могут существенно повлиять на индустрию. С одной стороны, рынок ждет постепенное укрупнение, а с другой — снижение темпов роста и развития.

IT-сектор ставит на красное

Центробанк 26 июля повысил ключевую ставку с 16% до 18% годовых. Это шестое повышение ставки подряд с лета 2023 года — уже тогда, напомним, действия ЦБР привели к сбоям в работе механизмов господдержки в IT-секторе. Речь идет об исчерпании лимитов для субсидирования ставок в рамках программ IT-ипотеки (Минцифры удалось оперативно решить эти проблемы), а также исчерпании лимитов по программе льготного кредитования производителей электроники в рамках 704-го постановления правительства. Из-за этого крупнейшие производители вычислительной техники вынуждены обслуживать изначально льготные кредиты по рыночным ставкам, которые могут доходить до 20–22% годовых, говорят источники „Ъ“. В сентябре ставка ЦБ выросла до 19%.

Судя по словам главы ЦБ Эльвиры Набиуллиной, ставка может быть повышена еще раз для контроля инфляции. «Если потребуется, мы не исключаем и дополнительного повышения ключевой ставки. Это отражено в обновленном прогнозе, где траектория ставки существенно повышена на ближайшие три года»,— сказала глава ЦБ (цитата по «Интерфаксу»). Опрошенные „Ъ“ участники IT-рынка говорят, что такая ситуация приведет к заморозке инвестиций IT-компаний в развитие, исследования и разработки.

Повышение ключевой ставки, как правило, приводит к удорожанию кредитных ресурсов, что заставляет IT-компании пересматривать свои инвестиционные стратегии, говорит директор по инвестициям «СКБ Контур» Сергей Зарипов. В условиях высокой стоимости заемных средств некоторые компании могут сократить расходы на НИОКР, другие же продолжат финансирование, особенно те, кто имеет финансовую подушку.

«Причина — потребность формирования долгосрочных активов. Недостающую в текущей ситуации рентабельность большие игроки, в особенности публичные компании, перекроют за счет размещения свободных денег в депозитах. Поэтому глобальных снижений темпов инноваций в отрасли, скорее всего, не произойдет. Однако стоит отметить, что некоторые компании могут в таких условиях оптимизировать свои процессы для повышения эффективности деятельности»,— уточняет он.

Спокойно себя будут чувствовать компании с собственным накопленным капиталом, рассчитывающие на свои силы и не имеющие высокой кредитной нагрузки. Но некоторые планы развития все же могут быть нарушены. Например, компании, рассматривающие выход на IPO, поставят эту задачу на паузу, добавляет гендиректор Content AI Светлана Дергачева.

С учетом того что цикл разработки программного обеспечения составляет три-пять лет, использование финансовых ресурсов со ставкой 20% и более просто невозможно, настаивает основатель фонда «Стриго Кэпитал» Дмитрий Комиссаров: «Кредитов с льготной ставкой очень мало, и требования к ним таковы, что получить их могут только крупные компании».

с20

Больше чем SOC Forum — целая Неделя кибербезопасности

«Киберкультура» — для граждан, «Кибербез-ликбез» — для студентов профильных вузов, выставка экспортных ИБ-технологий — для иностранных делегаций, встречи с инвесторами — для ИБ-стартапов, Кибербитва за Марс и три дня практического контента и оживленных дискуссий — для представителей отрасли. С 5 по 9 ноября в Москве пройдет Неделя кибербезопасности, главным событием которой станет SOC Forum.

— события —

ГРУППА КОМПАНИЙ «СОЛАР»

Кибербез в новом свете

Одно из важнейших событий в сфере информационной безопасности (ИБ) — 10-й, юбилейный SOC Forum — состоится 6–8 ноября в конгресс-центре Центра международной торговли. За десять лет форум трансформировался из узкопрофильного в одно из крупнейших мероприятий, посвященных комплексной безопасности. В 2024 году с выходом на новый уровень традиционная аббревиатура SOC (Security Operations Center, «центр информационной безопасности») получает новое прочтение — Security Opportunities and Challenges («возможности и вызовы в сфере информационной безопасности»).

На одной площадке соберутся компании—лидеры ИБ-индустрии, представители бизнеса из различных отраслей и регуляторы, чтобы обсудить актуальные вопросы кибербезопасности. Участники форума познакомятся с лучшими практиками защиты на реальных примерах, узнают, как вырастить эффективную команду кибербезопасников и какие навыки сейчас востребованы среди работодателей, а также обсудят развитие и экспорт отечественных ИБ-решений.

В прошлом году мероприятие длилось два дня и собрало более 5 тыс. офлайн- и 20 тыс. онлайн-участников. Ожидается, что 10-й SOC Forum привлечет еще больше посетителей. Увеличится и контентная часть форума: спикеры подали 354 заявки на выступления, что почти на 80% больше, чем годом ранее. Из них в программу был отобран 141 доклад. В жюри вошли десять известных ИБ-специалистов из ведущих российских компаний.

SOC Forum включает в себя множество форматов: от дискуссий и докладов до практических воркшопов, питч-сессий и персональных встреч с ведущими ИБ-экспертами. Эти форматы и разнообразие тем позволят представителям государства, крупных компаний и СМБ ознакомиться с трендами киберугроз, разобраться в вопросах обеспечения комплексной киберзащиты при разном уровне бюджета, узнать векторы развития SOC и получить доступ только к качественному контенту, «без воды».

Организаторы SOC Forum 2024 — ФСБ России и ФСТЭК России при поддержке Минцифры России и Банка России, соорганизатором выступает ГК «Солар».

Три дня SOC Forum — три ключевые темы

Каждый день SOC Forum посвящен своему тематическому треку: комплексной кибербезопасности для бизнеса и государства, новейшим технологиям защиты, а также практическому разбору кейсов кибератак и проектов по оценке защищенности.

Первый день форума откроют доклады и дискуссии по бизнес-ориентированному подходу к ИБ. Экспертам предлагается порассуждать, что IT-директора крупных компаний ждут от отрасли, каким образом ИБ влияет на бизнес-процессы и как «подружить» цифровизацию со стратегией защиты от кибератак. Также специалисты смогут обсудить, как обеспечить кибербезопасность малого и среднего бизнеса без миллионных вложений.

Актуальной темой первого дня станет и построение карьеры в ИБ (направления отрасли, востребованные навыки и т. д.). Помимо этого, компании поделятся советами, как растить свою команду и как ее удержать, когда сотрудники уже стали опытными и смотрят «на сторону».

Представители госорганов в рамках регуляторного трека расскажут об актуальных законодательных изменениях в ИБ, обсудят взаимодействие ИБ-компаний и государства и ответят на вопросы рынка.

На площадке SOC Forum 6 и 7 ноября развернется настоящая Кибербитва: по легенде команды киберзащитников и нападающих сразятся за колонизацию Марса. В Кибербитве примут участие 40 команд из почти 250 экспертов в сфере реагирования и расследования киберинцидентов, тестирования на проникновение и независимые игроки из отрасли ИБ. Кибератаки в режиме реального времени будут направлены на цифрового двойника колонии на Марсе. Соревнования пройдут на базе платформы Solar CyberMir 6.0.

Одной из главных тем второго дня станет SOC — «сердце» всей кибербезопасности в условиях постоянной эволюции киберугроз. Например, ИБ-специалисты в ходе выступлений расскажут, как реагировать на разные типы кибератак, в том числе с деструктивными целями, без каких технологий не может существовать современный центр противодействия, какие ахиллесовы пяты в инфраструктуре он не сможет защитить и как комплексный подход к ИБ поможет решить эту задачу. Компании также поделятся опытом построения кибербезопасности с применением облачных технологий и ИИ.

И завершится SOC Forum 2024 практикумом по направлениям Offence и Defense, куда войдут наиболее интересные кейсы по обнаружению уязвимостей, деятельности APT-группировок, безопасной разработке, трендам теневого сегмента интернета и защите от атак supply-chain.

«Постоянно эволюционирующие киберугрозы требуют выстраивания новых процессов в информационной безопасности — как внутри самого SOC, так и за его пределами»,— говорит директор центра противодействия кибератакам Solar JSOC ГК «Солар» Владимир Дрюков. Сегодня под прицелом хакеров находятся как крупные компании и госструктуры, так и МСП, отмечает он. При этом разные типы угроз — от шпионажа азиатских группировок до максимального деструктива со стороны проукраинских хакеров — требуют очень разных методов реагирования. «Именно поэтому юбилейный SOC Forum будет посвящен формированию новых подходов к защите и станет ответом на многие актуальные вопросы: какие компетенции и технологии нужны современному SOC, как обеспечить кибербезопасность на уровне ПО и оборудования, как защититься от кибератак даже небольшим организациям и т. д.»,— перечисляет Владимир Дрюков.

На площадке форума состоится Выставка экспортных решений, на которой лидеры ИБ-отрасли представят свои лучшие продукты и услуги и продемонстрируют гостям мероприятия все возможности российского кибербеза. В дополнение зарубежные заказчики из разных стран обсудят с российской отраслью экспортный потенциал отечественных ИБ-решений. Ожидается до 50 делегаций из стран СНГ, Юго-Восточной Азии, Ближнего Востока и Латинской Америки.

Неделя кибербезопасности

Неделя кибербезопасности пройдет с 5 по 9 ноября. Мероприятие охватит весь спектр полезных тем для широкой аудитории слушателей: от обычных пользователей до технических ИБ- и IT-специалистов, а также топ-менеджмента из различных сфер.

В парках Москвы, столичной подземке и наземном общественном транспорте будет представлен просветительский проект «Киберкультура», который расскажет, как безопасно вести себя в сети, распознавать фишинг, общаться с мошенниками и надежно хранить свои данные.

В технологических вузах столицы пройдет серия образовательных лекций «Кибербез-ликбез». Лидеры ИБ-рынка поделятся реальными историями из своей практики, раскроют особенности работы в отрасли и расскажут о том, как противостоять киберпреступникам. Также для учащихся вузов и молодых специалистов «Солар» проведет День открытых дверей. Посетители смогут узнать о построении карьеры в кибербезопасности, а также попасть на интервью с потенциальным работодателем.

На Неделе кибербезопасности встретятся аналитики, вендоры и инвесторы. Эксперты обсудят векторы развития и меры поддержки начинающих предпринимателей, а фаундеры получат рекомендации по привлечению инвестиций или смогут найти инвестиционного партнера.

Для онлайн-участников будет запущено «Кибербез ТВ» — новый формат единого стрима с пленарными сессиями, докладами и эксклюзивным контентом.

«Тема кибербезопасности давно касается не только ИБ-специалистов компаний и госструктур,— отметил Владимир Дрюков — Сегодня обычный человек может стать как причиной крупной кибератаки в своей организации, так и жертвой злоумышленников дома. Мы считаем, что соблюдение правил кибергигиены должно стать для россиян такой же привычкой, как ежедневное использование гаджетов. Неделя кибербезопасности — один из шагов к формированию этой привычки: широкая аудитория сможет в доступной, запоминающейся форме получить полезную для себя информацию о защите в цифровой среде».

Подробности о мероприятиях Недели кибербезопасности и SOC Forum на сайте forumsoc.ru.

Валерия Романова

ПРОФАЙЛ

Группа компаний «Солар» — архитектор комплексной кибербезопасности. Занимается аутсорсингом ИБ, разработкой собственных продуктов, интеграцией комплексных решений, обучением ИБ-специалистов, аналитикой и исследованием киберинцидентов. Клиенты компании — более 1 тыс. крупнейших компаний и организаций России, включая государственные информационные системы.

«Солар» лидирует среди российских MSSP (Managed Security Service Providers) по объему бизнеса, занимая долю рынка в 30%. Таковы данные исследования iKS-Consulting, посвященного структуре рынка SOC/MSSP в России в 2023 году. В аналогичном рейтинге по Европе «Солар» занимает 5-е место, а по миру — 15-е («MSSP в мире по итогам 2023 года»).

Компания реализует киберзащиту ключевых государственных мероприятий, таких как выборы, ПМЭФ, ВЭФ, форум «Россия—Африка», Всемирный фестиваль молодежи, Игры БРИКС и др. Специалисты центра противодействия кибератакам Solar JSOC обеспечивают безопасность инфраструктуры электронного правительства, включая инфраструктуру федерального портала «Госуслуги». «Солар» совместно с Минцифры в рамках национального проекта «Цифровая экономика РФ» реализует всероссийскую программу кибергигиены, направленную на повышение цифровой грамотности населения.

IT-кадры найдут выход

— кадровый потенциал —

В России сохраняется дефицит IT-специалистов. По оценкам государства, не хватает около 740 тыс. сотрудников, однако бизнес называет цифры до 1 млн человек. Участники рынка считают, что на отсутствие квалифицированных кадров влияют и нарастающие ограничения найма сотрудников с удаленным режимом работы. Среди потенциального решения проблемы эксперты называют применение в работе IT-компаний искусственного интеллекта, релокацию специалистов из разных регионов, а также внедрение гибридного формата работы.

АНАТОЛИЙ ЖДАНОВ

За последние два года в связи со сложной геополитической и экономической ситуациями обострилась проблема оттока из России IT-специалистов, которые и ранее были в дефиците. Всего, по оценке Минцифры, в середине 2023 года в РФ не хватало порядка 740 тыс. IT-специалистов. (см. „Ъ“ от 16 августа 2023 года). В качестве ответного шага власти запустили новые меры поддержки для сотрудников в России, а также стимулирования возврата кадров, в том числе льготную IT-ипотеку, бронь от службы армии и др. (см. „Ъ“ от 11 января 2023 года). В Минцифры „Ъ“ рассказали, что сейчас численность сотрудников в IT-сфере оценивается более чем в 900 тыс. человек.

Руководитель направления подбора персонала компании «Контур» Юлия Мельчугова рассказывает, что оценка дефицита кадров министерства за прошлый год отличается от оценки бизнеса примерно на 300 тыс. человек: бизнес оценивает нехватку IT-специалистов в 1 млн сотрудников. «Точную цифру назвать трудно, однако ситуация на рынке говорит о том, что в ближайшие пять лет она будет только расти».

Нехватка IT-кадров в 2024 году остается на уровне от 500 тыс. до 1 млн человек, оценила менеджер по развитию бизнеса компании IBS Елизавета Сергеева. По ее словам, наибольшим спросом пользуются инженеры информационной безопасности из-за возросшего количества кибератак. За первую половину 2024 года только количество DDoS-атак на российские организации выросло до 355 тыс., что на 16% больше, чем за весь 2023 год (см. „Ъ“ от 9 сентября). Следом после специалистов по кибербезопасности госпожа Сергеева называет разработчиков моделей машинного обучения, системных аналитиков и специалистов по работе с Big Data. «Несмотря на то что на рынок выходит много молодых специалистов, компании предпочитают нанимать опытных сотрудников, что создает дополнительный кадровый дефицит»,— уточняет она. Как писал „Ъ“, из-за нежелания компаний нанимать на работу специалистов начального уровня средняя зарплата IT-сотрудников сократилась на 15% в июле—декабре 2023 года (см. „Ъ“ от 1 февраля).

Удаленный формат

Текущие условия с дефицитом необходимых специалистов увеличили и срок поиска сотрудников компаниями. Так, если в других отраслях экономики срок поиска в 2023 году увеличился в 1,5 раза, то в IT — в два раза (см. „Ъ“ от 21 апреля 2023 года). Вместе с тем в конце февраля того же года в Госдуме проработали возможность запретить IT-специалистам, находящимся за границей, работать на российские объекты критической информационной инфраструктуры (КИИ), государственные информационные системы и участвовать в работе с персональными данными россиян. До этого Минцифры выступало против какого-либо ограничения удаленной работы, так как это может «отпугнуть российских разработчиков» (см. „Ъ“ от 20 декабря 2022 года). В комитете Госдумы по информполитике „Ъ“ не ответили о текущем статусе инициативы и работы над ней.

Поиск сотрудников стал занимать все больше времени, при этом «стоимость найма» также растет, говорит гендиректор IT-компании в сфере HR-Tech Edstein Евгений Обогоров. Среди наиболее дефицитных направлений он выделяет DevOps-инженеров, которые отвечают за автоматизацию процессов и влияют на работу разработчиков, тестировщиков и системных администраторов. «Такие специалисты должны обладать большим техническим бэкграундом и знать большое количество инструментов, поэтому кандидатов на рынке не так много, а спрос на них постоянно растет»,— подчеркивает он. Господин Обогоров добавляет, что все больше кандидатов предпочитают вариант трудоустройства с удаленным форматом работы, где показателем является не количество проведенных в офисе часов, а выполненный проект.

По словам директора компании Ideco Дмитрия Хомутова, в последние несколько лет в РФ, однако, наблюдается тенденция к закрытию возможности удаленно работать. Такие решения некоторые IT-компании могут принимать из-за сложности контроля за выполнением задач, предоставления доступа к конфиденциальной информации, а также стремления к удержанию сотрудников, которые не полностью погружены в корпоративную культуру: «Например, разница во времени может создавать неудобства для коммуникации».

Однако, отмечает господин Хомутов, подобные ограничения существенно уменьшают шансы компаний нанять квалифицированного специалиста, сужая круг потенциальных кандидатов до тех, кто находится в городе, где расположена компания. «Это приводит к тому, что организации становятся менее конкурентоспособными на рынке труда и могут столкнуться с трудностями при поиске нужных профессионалов»,— говорит он.

Наибольшие трудности найма на «далекой удаленке» и зарубежного аутсорсинга наблюдаются у компаний, работающих с госсектором, в сфере КИИ и информационной безопасности, говорит директор Ассоциации предприятий компьютерных и информационных технологий Николай Комлев. По его словам, правительство увеличило прием в вузы по IT-специальностям, однако при таком росте потребности в кадрах университетам придется еще больше расширять количество мест приема.

Также, по словам Елизаветы Сергеевой, работодателям, которые не рассматривают возможность удаленной работы, стоит обратиться к компромиссному варианту и предлагать сотрудникам гибридный формат сотрудничества: часть удаленно, часть в офисе. «Если это невозможно организовать, то стоит сосредоточиться на локальном рынке труда, акцентируя внимание на поиске кандидатов в непосредственной близости от офиса»,— говорит она. Также эксперт считает, что организациям стоит заняться программами переезда и релокирования IT-специалистов: «Это может стать важным инструментом для привлечения талантов в условиях ограничения удаленной работы».

В Минцифры, однако, уверяют, что в министерство не поступала информация о проблемах удаленной работы IT-специалистов. «Решения по формату работы своих сотрудников IT-организации принимают самостоятельно, как правило, исключение для удаленки — проекты по созданию и развитию государственных информсистем и критически важных приложений»,— говорит он, добавляя, что министерство также создает условия для роста количества готовых IT-кадров. Для примера в Минцифры называют проект по бесплатному изучению языков программирования для школьников и студентов колледжей, а также увеличение количества бюджетных мест на «цифровых» кафедрах в вузах в 2,5 раза: «С 2019 по 2024 год на IT-специальности в вузы будет принято более 500 тыс. человек».

Машинальное решение

Дефицит IT-кадров компании решают не только с помощью обучения будущих сотрудников, но и другими методами. Так, «Ростелеком» в течение двух-трех лет планирует возместить нехватку кадров внедряя в работу искусственный интеллект (ИИ) (см. „Ъ“ от 27 сентября). Нехватка кадров в IT-секторе объясняется высоким спросом на цифровизацию бизнеса, ростом стартапов, а также быстрым развитием технологий, и нельзя сказать, что какая-то определенная специальность выделяется на этом фоне, говорит старший вице-президент по информационным технологиям «Ростелекома» Дарий Халитов. По его словам, на данный момент интеграция ИИ в работу компании проходит тестовый режим в рутинных задачах: обработка обращений, ведение документооборота и выполнение стандартных операций. «Мы активно обучаем сотрудников навыкам работы с нейросетями, так как внедрение ИИ может значительно повысить эффективность работы и снизить нагрузку на сотрудников»,— говорит он, добавляя при этом, что нейросеть не способна полностью заменить IT-сотрудников.

Гендиректор «Сикрет Технолоджис» Леонид Бондаренко согласен с тем, что ИИ способен упростить и ускорить деятельность IT-специалистов. «Однако использование ИИ также вызывает ряд рисков, например уязвимости или закладки, которые могут появиться в коде, написанном нейросетью, или нарушение конфиденциальности данных»,— подчеркивает он.

Тимофей Корнев

Яндекс Go для бизнеса 0+

Сервис на все руки

В 2024 году растет спрос на экосистемные решения для бизнеса. В рамках одного интерфейса они позволяют, например, доставить еду в офис, заправить рабочий автомобиль или отправить документы, при этом отчетность по всем операциям будет сформирована автоматически. Вместе с Яндекс Go для бизнеса „Ъ“ разобрался в особенностях B2B-экосистем и их продуктов.

— технологии для бизнеса —

ПРЕДОСТАВЛЕНО КОМПАНИЕЙ ЯНДЕКС.

До трети мировой экономики к 2030 году будет принадлежать экономике экосистем, следует из прогнозов McKinsey. По мнению аналитиков, экосистемы способны перестраивать рынки, потому что работают как шлюзы: «уменьшают трение», когда клиенты переключаются между сервисами. Бизнесу удобнее работать с одним поставщиком, так как не нужно тратить ресурсы на поиск, анализ и переговоры, чтобы выбрать более подходящий сервис. Оптимизируя административные процессы, компании могут высвободить время, ресурсы и энергию для стратегических задач: поработать над эффективностью производства, найти новые точки сбыта или расширить пул клиентов.

По прогнозам аналитиков, B2B-сегмент в ближайшие годы будет одним из главных драйверов роста экосистем в целом независимо от страны или особенностей оказываемых услуг. Как считают в J'son and Partners, число пользователей платформенных решений среди компаний будет расти, так как юридическим лицам будет выгодно получать комплексные решения у одного поставщика. Также будет расти объем предложений услуг в экосистемах. «Игроки будут стараться определить наиболее востребованные сервисы именно для своих клиентов в зависимости от стратегии развития экосистемы»,— прогнозируют аналитики.

Привычные продукты, новые возможности

Тенденция проявляется и на российском рынке. Один из примеров экосистемы сервисов для юрлиц — Яндекс Go для бизнеса. Это платформа, которая закрывает большинство административных задач в режиме «одного окна». Уехать на такси на встречу, отправить курьером документы, поужинать с клиентом в ресторане, заказать еду в офис на корпоратив, купить авиабилет, забронировать отель на время командировки и многое другое — все это доступно с платформой. Компании получают доступ к единому личному кабинету, в котором могут управлять сразу девятью сервисами. Достаточно пополнить корпоративный счет, добавить сотрудников и настроить для них лимиты: открыть сразу все сервисы или несколько, указать сумму с расчетом на день или другой период, установить геозоны использования.

Так, на сентябрь 2024 года у Яндекс Go для бизнеса уже более 100 тыс. активных клиентов в месяц. По словам директора по продукту Екатерины Никитиной, это юрлица с разными оборотами: от самозанятых и ИП до крупных энтерпрайз-клиентов, и каждая компания использует сервисы по собственному сценарию.

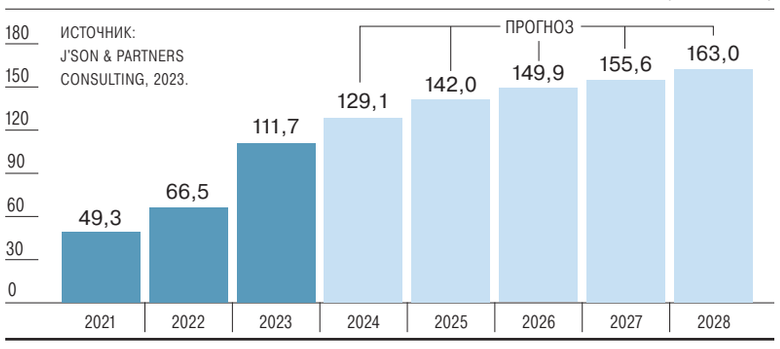
«Мы по факту являемся неким окном для бизнеса внутрь Яндекса,— говорит Екатерина Никитина.— При этом сотрудники корпоративных клиентов могут пользоваться сервисами через привычные приложения. Просто у них появляются новые возможности, например оплатить доставку или такси с корпоративного счета».

Контроль расходов: автоматизация вместо ручного режима

Сбор каждого чека «руками» — самая частая проблема, с которой сталкиваются предприниматели. По мере роста оборотов и штата появляется необходимость делегировать эту часть задач, однако сделать это всегда тяжело. Ведь должно быть лицо, которое контролирует весь бюджет компании — думают многие.

Яндекс Go для бизнеса дает возможность оплачивать услуги с корпоративного счета, не выходя за рамки бюджета. Сотрудники платят, например, за бензин через приложение Яндекс Заправки, и владелец при этом видит каждую трансакцию, объясняет Екатерина Никитина. Чеки не будут потеряны, так как вся информация о них сохраняется автоматически в личном кабинете компании. Их можно скачать в случае, если нужно отчитаться перед налоговой.

ОБЪЕМ РЫНКА ЭКОСИСТЕМНЫХ РЕШЕНИЙ, В ЧИСЛЕ КОТОРЫХ — ДЛЯ B2B (МЛРД РУБ.)



Документооборот: один отчет на все

Предпринимателю, который, например, торгует на маркетплейсах, нужно забрать товар от производителя и доставить его на склад, а после того как поступил заказ — доставить его потребителю. Так появляются минимум две логистические цепочки, объясняет Екатерина Никитина. Для того чтобы проверить качество товара и документацию, нужно приезжать лично на эти точки. А с масштабированием больше точек для проверки — больше и отчетности.

«Часто компании заключают партнерские договоры с сервисами доставки. Получается, для закрытия какого-то доставочного сценария есть компания, которая организует доставку. С ней нужно заключить договор, обсудить условия, а после следить за процессом оформления и принимать закрывающие документы. А если таких контрагентов не один, а десять? Это очень большой объем работы. Для этого часто не хватает ни ресурсов, ни времени»,— говорит Екатерина Никитина.

С Яндекс Go для бизнеса эта проблема исчезает. Так, например, в рамках платформы можно закрыть практически любые логистические сценарии, будь то обычное такси для клиентов или грузовая доставка оборудования. В конце месяца предприниматель получит закрывающие документы за все услуги на почту, одним пакетом, не потратив и нескольких минут на их формирование.

Платформенное решение как инструмент для HR

В большинстве отраслей существенно выросла конкуренция за опытных специалистов, поэтому компании ищут новые подходы к привлечению и удержанию сотрудников. Если раньше все решалось на уровне зарплаты, сейчас тренд на дополнительную, нематериальную ценность. Корпоративное питание, кофе-пойнт в офисе, компенсации такси, каршеринга и топлива — по словам клиентов Яндекс Go для бизнеса, такие возможности мотивируют сотрудников и укрепляют их лояльность, а также делают вакансию более привлекательной.

Опираясь на этот тренд, в Яндекс Go для бизнеса разработали корпоративное питание, которое становится частью соцпакета компании, рассказала Екатерина Никитина. Причем сервисы «подстраиваются» под режим сотрудников или, наоборот, его формируют. Например, работодатель настраивает сумму из расчета на день, указывает геозону или конкретные адреса, по которым сотрудники заказывают перекусы из Лавки или полноценные обеды в Еде.

По мере проникновения продукта на рынок для сотрудников такие преимущества становятся все более значимыми, говорит Екатерина Никитина. «Конечно, сейчас в большинстве случаев подобные льготы предлагают крупные компании. Но с каждым годом число представителей среднего и малого бизнеса, которые предоставляют такой социальный пакет своим сотрудникам, растет, что нас очень радует. Компенсация части затрат — на дорогу, на питание — снова становится нормой»,— добавила она.

Особенно это удобно в деловой поездке, когда нет времени на поиски места для обеда или вариантов того, как добраться до новой встречи. Через Яндекс Командировки можно оплатить проживание и билеты заранее, а в поездке — думать только о важных делах: оплата за такси с аэропорта, деловой ужин с партнерами или доставку еды в номер спишется с корпоративного счета. После командировки работодателю не придется принимать десятки чеков и проверять, насколько они правильно оформлены — все в личном кабинете.

Придумать идею для подарков на праздники партнерам или способ поощрить сотрудника — тоже вызов для предпринимателя, хоть и не каждодневный. Повторяться не хочется, как и дарить то, чем не воспользуются. Для этих целей есть промокоды, которые можно оформить на разные сервисы Яндекса и дарить клиентам, использовать в качестве призов при проведении акций, а также наполнять бонусный пакет компании.

Есть запрос — находится продукт

Некоторые решения Яндекс Go для бизнеса вырастают из реальных потребностей клиента, рассказала Екатерина Никитина. Например, услуга Час+ — возможность взять такси от одного до восьми часов. Она нужна, если за день нужно побывать в нескольких местах. Стоимость известна заранее, а ограничений по километражу, времени ожидания и количеству остановок нет.

«Мы часто анализируем, как наши клиенты пользуются сервисом, чтобы выявить гипотезы для новых продуктов. Так получилось с одним нашим клиентом — медицинской лабораторией. Мы заметили, что сотрудники лаборатории регулярно заказывают такси с большим количеством промежуточных точек, что для корпоративного клиента нетипично. Решили уточнить, и оказалось, по утрам медработник выезжает на забор анализов и, чтобы не вызывать каждый раз новую машину, заказывает одну и указывает несколько остановок, а после возвращается в лабораторию. Мы подумали: такой сценарий может быть востребован и в других компаниях. Так и появился Час+»,— рассказала Екатерина Никитина.

Из похожих наблюдений возникло другое решение — возможность развоза сотрудников. «Каждый день примерно в 12 часов ночи в одном из регионов далеко от города резко возрастал спрос на такси. Мы долго не понимали, с чем это связано, а потом выяснили: есть колл-центр, где смена заканчивается в полночь. В это время транспорт уже не работает, поэтому все 300 человек массово пытаются вызвать такси. Локация в отдаленности от города, машин в округе мало, потому и ждать приходится долго. Для таких кейсов мы придумали сценарий, когда нужно много сотрудников из одной точки А развести во много точек В — он называется массовый развоз»,— говорит Екатерина Никитина.

Услуга оказалась востребованной не только у крупных заказчиков, но и у малого бизнеса. Так, ресторан «Гусь» в Краснодаре смог на 30% сократить время, которое тратится на организацию развоза персонала после смены. Ресторан также избавился от проблем с документооборотом и контролем поездок, так как скорректировать лимиты сотрудников и сформировать счет для оплаты можно в личном кабинете.

Если у компании есть свой автопарк, Яндекс Go для бизнеса помогает управлять им максимально эффективно. Благодаря «Управлению автопарком» вызвать машину для деловой поездки по городу или в командировке так же просто, как такси в приложении Яндекс Go, но на заказ назначается автомобиль из корпоративного автопарка. Сервис помогает оптимизировать внутренние процессы заказа транспорта на предприятии, лучше утилизировать автомобили, сократить их холостой пробег — за счет этого снижается себестоимость одной поездки.

Юлия Макарова

ЯНДЕКС GO ДЛЯ БИЗНЕСА – ПЛАТФОРМА ДЛЯ РЕШЕНИЯ АДМИНИСТРАТИВНЫХ ЗАДАЧ

ИСТОЧНИК: ЯНДЕКС GO ДЛЯ БИЗНЕСА.

ЛАНИТ

На IT к успеху: стратегический консалтинг

В динамично меняющейся IT-среде компаниям важно быть открытыми к внедрению новых практик, уметь оперативно интегрировать новые цифровые продукты и составлять гибкую стратегию развития исходя из внешних факторов. Для более эффективной работы бизнес все активнее прибегает к услугам стратегического IT-консалтинга. „Ъ“ совместно с группой ЛАНИТ выяснил, какие задачи эксперты в этой области помогают решить уже сейчас и почему спрос на IT-консалтинг будет только расти.

— аналитика —

GETTY IMAGES

В России стремительно развивается экономика данных, растет доля IT в ВВП страны: за 2023 год показатель составил почти 2%, по данным НИУ ВШЭ и Минцифры РФ. При этом объем реализации собственных продуктов и услуг в IT-отрасли увеличивался в среднем на 26% с 2019 по 2023 год и в прошлом году достиг 3,1 трлн руб. В этом секторе экономики уже работают не только профильные компании—разработчики цифровых продуктов и сервисов, но и предприятия критической информационной инфраструктуры (КИИ) и другой крупный бизнес.

Однако за последние два года IT-отрасль столкнулась с рядом ощутимых рисков: массовым уходом зарубежных вендоров, постепенным отключением компаний от их продуктов, в том числе системно значимых, ограничениями на поставки импортных комплектующих и т. д. На этом фоне кратно вырос спрос на российское программное обеспечение (ПО) и другие цифровые решения, при этом время на переход у бизнеса оказалось очень ограниченным.

Чтобы успевать отвечать на вызовы рынка, быстро адаптироваться к меняющимся условиям и технологическому окружению, компаниям стали необходимы сторонняя поддержка и опыт. В условиях нехватки кадров и времени эти задачи помогают решить команды, которые специализируются на IT-консалтинге, предоставляют экспертизу в разработке стратегии цифровизации, автоматизации бизнес-процессов, построения цифровой инфраструктуры.

По оценке экспертов НОРБИТ, объем открытого рынка IT-консалтинга составляет 70–90 млрд руб. В основном его делят между собой крупные интеграторы со штатом сотрудников от 500 человек и более, а средние и небольшие компании работают во втором эшелоне, рассказывает управляющий директор НОРБИТ Владимир Вертоградов.

Драйвером роста рынка стали в первую очередь миграции на отечественное ПО, новые заказы по замене решений, перечисляет Владимир Вертоградов. Второе: адаптация существующих ландшафтов под российские серверы, операционные системы и средства безопасности. Третье: скорость преобразований возросла колоссально, бизнес обязан быстро реагировать. Для этого нужно поменять старую привычную модель, в рамках которой сначала на проект привлекались консультанты по изменениям, а затем уже по IT. «Со временем все поняли, что на втором шаге часто приходится все переделывать, и компании накопили достаточно опыта по проектам цифровой трансформации, поэтому, как правило, сразу начинают со второго этапа»,— говорит Владимир Вертоградов.

Консалтинг сейчас покупают вместе с технологиями: нужно не просто заниматься трансформацией, но и понимать, какие изменения произойдут в диапазоне нескольких лет, какие будут требования, как добиваться технологического суверенитета в конкретной компании, заключает эксперт.

«Дорожная карта» к успеху: производство оборудования

К НОРБИТ обратилась крупная отечественная компания, занимающаяся производством высокотехнологичного оборудования. Задачей было трансформировать систему закупок, снабжения, взаимодействия с поставщиками и смежных процессов: финучета, планирования, бухгалтерии.

Первым этапом были проведены аудит ситуации внутри компании, а также оценка, в какой регуляторной среде она работает. На этом этапе заказчик сразу получил варианты технологий, на которых идет прототипирование предлагаемых изменений. Также была учтена корпоративная специфика: культура, регламенты и т. д. Как отмечают в НОРБИТ, важно сохранить уникальные стороны компании, а не перевести всех на «стандартные рельсы».

По итогам были готовы описание целевого состояния функции закупок и план мероприятий по переходу к нему. Был сформулирован набор предложений по развитию, который ранжировался с учетом ценности, важности и эффективности. На его основе определяются этапы «дорожной карты», которая затем реализовывается. Результатами проекта стали экономия затрат, организация эффективных цепочек поставок и снижение рисков их срыва и роста цен.

Выбор осознанного бизнеса

В «ЛАНИТ — Би Пи Эм» рассказывают, что потребность в IT-консалтинге не зависит от масштаба компании и каждый бизнес сможет найти для себя преимущества привлечения IT-консультантов. Малый бизнес, кроме квалифицированной и профессиональной IT-поддержки, сможет повысить экономическую эффективность, так как не будет необходимости нанимать в штат IT-специалистов. Средний бизнес сможет оптимизировать IT-процессы и получить инновационные решения. Крупные компании приобретут большой опыт сторонних IT-консультантов, работавших на масштабных проектах.

К IT-консультантам обращаются в случаях, когда необходимо запустить новый IT-продукт, найти точки роста, выйти на новый сегмент. А также когда необходимо подобрать или разработать новое ПО и внедрить его в бизнес-процессы компании, модифицировать или заменить имеющееся ПО, мигрировать с устаревшего или зарубежного. Кроме этого, в пул задач IT-консультантов могут входить интеграция корпоративных систем, автоматизация процессов, разработка IT-стратегии и проведение анализа IT-рынка.

Есть несколько признаков, которые говорят о том, что компании необходима помощь IT-консалтинга, перечисляет директор по развитию бизнеса «ЛАНИТ — Би Пи Эм» Максим Волошинов:

бизнес-процессы в компании не автоматизированы, рутинные операции приводят к увеличению затрат, снижению скорости и не дают прозрачности деятельности;

требуется создание новых IT-продуктов/решений или новых технологий;

используемые IT-продукты неисправны, технологически устарели, не могут обеспечить потребности бизнеса, требуют дорогостоящей поддержки.

Еще один блок задач в области IT-консалтинга связан с анализом IT-инфраструктуры. Это направление помогает выявить избыточные или неэффективно используемые ресурсы и определить области для сокращения расходов без ущерба для ключевых бизнес-процессов, рассказывает директор технического департамента компании «ЛАНИТ-Интеграция» Олег Аксенов. Анализ IT-инфраструктуры также помогает повысить уровень зрелости и эффективности бизнес-процессов, спланировать решение точечных задач модернизации, сформировать основу для создания комплексных IT-стратегий, направленных на долгосрочный рост и повышение конкурентоспособности компаний в будущем, добавляет Олег Аксенов.

«Дорожная карта» к успеху: промышленность

Запрос на сложный IT-консалтинг в 2024 году сформировался со стороны российской промышленной компании: задачей было не просто провести обследование IT-инфраструктуры, а сосредоточиться на оценке зрелости IT-процессов и выявлении в них проблемных точек.

Результатом проекта, реализованного «ЛАНИТ-Интеграцией», стали практические рекомендации, которые в том числе помогли разработать, согласовать и защитить план развития IT-инфраструктуры с существенным увеличением бюджета, разработать каталог IT-услуг и информсистем компании (порядка 500 строк), планы оптимизации процессов управления IT-услугами (10 процессов).

«Инвестиции на горизонте одного года являются операционными затратами и, конечно, должны исходить из общей стратегии развития компании»,— комментирует Олег Аксенов. Но если вследствие внешних и внутренних факторов стратегия потеряла актуальность, то аудит IT-ландшафта поможет выявить слабые места, например неэффективное использование ресурсов, и актуализировать ее. «Определение приоритетных направлений инвестиций должно основываться на утвержденной в стратегии карте IT-инициатив и учитывать тактические и операционные задачи компании»,— отмечает эксперт.

Запрос федерального масштаба

Экспертиза и участие IT-консалтеров в 2024 году актуальны и для проектов федерального уровня, в том числе в сфере КИИ, строительства, логистики и т. д. В ЛАНИТ напоминают, что любой крупный и сложный проект невозможно сделать в короткий срок и небольшой командой — в нем будет задействовано много ресурсов, которые нуждаются в организации и координации. Резко повышается важность планирования и управления изменениями. «Именно эти параметры определяются в процессе консалтинговых работ»,— рассказал руководитель направления аналитических систем и платформенных решений ЛАНИТ Вячеслав Солопов.

Федеральный проект, как правило, является территориально распределенным. Ключевой фактор его успеха — раннее определение общих и специфических параметров процессов, которые должны быть реализованы на уровне региональных или структурных сегментов. Здесь, помимо анализа существующей ситуации и проектирования целевого решения, важным аспектом является идентификация различий. И дальше — техническая реализация выявленного многообразия или унификация (типизация) за счет поиска и внедрения лучших практик, которые должны быть определены на этапе консалтинга и апробированы всеми участниками процесса.

Как правило, методологическая, консалтинговая проработка не только предваряет такие проекты, но и постоянно их сопровождает в течение всего времени их реализации. Это делается, чтобы постоянно сверяться с целями и задачами проекта и обеспечивать целевую эффективность, не допуская, с одной стороны, умножения сущностей, а с другой — обеспечивая создание систем и сервисов, которые имеют необходимый и достаточный уровень покрытия для решения поставленных задач в рамках всех региональных сегментов.

Татьяна Исакова

Играть по полной

— рынки —

Объем российского рынка видеоигр, по разным оценкам, к концу года может достичь от 130 млрд до 187 млрд руб., подсчитали профильные аналитики и представители индустрии. В первом полугодии рынок стабилизировался после кризиса 2022 года и демонстрирует рост, отмечают в компаниях. „Ъ“ разбирался, чем обусловлены текущие показатели, какие законодательные изменения повлияли на отрасль в январе—июне и какие риски видят для себя разработчики.

ЕВГЕНИЙ ПАВЛЕНКО

Объем рынка видеоигр по итогам 2024 года увеличится на 6,1% и достигнет 187 млрд руб., подсчитали в Strategy Partners и Организации развития видеоигровой индустрии (РВИ). Так, мобильный сегмент займет 44% рынка (81,2 млрд руб.), ПК — 48% (89,8 млрд руб.), консольный — 8% (15,4 млрд руб.). В Lesta Games (игры «Мир танков», «Мир кораблей», Tanks Blitz) приводят более консервативный прогноз — 130–140 млрд руб. (см. «Ъ» от 11 сентября).

«По итогам прошлого года доходы индустрии выросли на 4,7% год к году и составили 176 млрд руб.,— отмечают в Strategy Partners.— Однако этот рост также был обусловлен ростом цен на зарубежные видеоигры ввиду более сложных способов их оплаты, а также девальвацией рубля». Так, в долларовом выражении рынок видеоигр в прошлом году снизился на 2,5%. До 2022 года российский рынок видеоигр измеряла компания My.Games (в 2022 году объявила об уходе из РФ). Последний отчет датирован 2021 годом: тогда объем рынка My.Games оценивала в 177,4 млрд руб. (речь идет о выручке от продажи всех игр в РФ).

Инициативы в игре

За последние два года отечественные разработчики видеоигр перешли от модели работы на международной арене к развитию продукта на локальном уровне и экспансии на азиатские рынки и в страны СНГ, отмечают опрошенные „Ъ“ участники отрасли.

После начала конфликта на Украине российский рынок покинули все ведущие международные компании, в их числе Activision Blizzard (игры — Call of Duty, Diablo, StarCraft и др.), Electronic Arts (Sims, Fifa, Need for Speed), Ubisoft (Far Cry, Assassin's Creed, Watch Dogs). «Российские разработчики, которые ориентировались на глобальное продвижение, тоже либо полностью ушли, либо открыли в РФ дочерние компании, либо разделили бизнес»,— комментируют в Strategy Partners. «Сейчас в РФ остались компании, которые имеют российскую юрисдикцию, работают на нашем рынке и в странах СНГ». «В 2022 году также умер рынок аутсорсинга видеоигр в России — это те, кто работал на западных заказчиков, поскольку стало проблематично «приземлять деньги» в России,— объясняет экс-директор по продукту Wargaming Вячеслав Макаров. Однако, по его мнению, это «не затормозило развитие российского рынка видеоигр, а переструктурировало его».

В правительстве уже обратили внимание на игровой сегмент IT-рынка: на разработчиков распространяются как продленные льготы для IT-сотрудников, так и льготный НДФЛ для компаний. «Безусловно, нас радует тот факт, что продлили льготы, но для развития отрасли»,— поделился руководитель юридической службы Lesta Games Александр Смирнов. Он также выделил как значимую инициативу об оплате сверхурочных, о которой стало известно в апреле (соответствующий закон вступил в силу уже с 1 сентября). «Мера, безусловно, коснется нас, поскольку, ставя в приоритет комфорт игроков, мы проводим профилактические регламентные работы на оборудовании в ночные часы, когда наши игроки спят»,— поясняет он.

Руководитель РВИ Василий Овчинников отмечает принятие нового закона о креативных индустриях (одобрен президентом РФ Владимиром Путиным в августе). По словам господина Овчинникова, это первый законодательный акт, в который включены видеоигры: «Можно сказать, что их производство узаконено; мера должна открыть доступ к принятию видеоигровой разработки, что в дальнейшем позволит рассчитывать индустрии на поддержку». В этой связи он отмечает, что в августе было подписано соглашение между Россией и Китаем о совместном производстве и продвижении видеоигр.

При этом в Astrum Entertainment считают, что с начала года в игровой индустрии не произошло каких-либо серьезных законодательных изменений. Российское законодательство в отношении видеоигр делает акцент на соблюдении интеллектуальной собственности и авторского права, говорят в компании: «Сейчас в разработке проект по добровольной маркировке видеоигр на предмет чувствительного контента. Важно, что инициатива исходит от игроков отрасли, которые обсудили свои предложения с регуляторами и запустили объемный проект, удовлетворяющий запросам всех участников процесса».

Игровая атмосфера

Условия, в которых оказались участники российской отрасли после ухода зарубежных игроков, привели к сплочению индустрии, считают в Astrum Entertainment. В качестве примера представитель компании приводит создание Ассоциации профессионалов индустрии оперирования и разработки игры (входят VK Play, Astrum Entertainment, United Games). «Профессиональные разработчики и издатели поняли, что необходимо не просто зарабатывать деньги, но и вкладываться в развитие рынка: кадровым потенциалом, экспертизой, финансами»,— заверяет руководитель московского подразделения группы Lesta Games Гаухар Алдиярова. Так, компания занимается обучением стажеров в рамках специальных программ. «Например, в „Леста Академии“ мы участвуем в индустриальных мероприятиях, выставках,— рассказывает она,— так как знаем по опыту, что без питательной среды в итоге вокруг останется выжженная земля и не будет развития рынка и индустрии».

В целом за семь месяцев количество размещенных вакансий среди разработчиков игр в России увеличилось на 23%, подсчитали в HeadHunter (см. «Ъ» от 7 августа). По словам участников рынка, рост спроса связан с новыми проектами отечественных студий и активностью азиатских компаний, работающих в РФ. Некоторые разработчики допускают, что тренд обусловлен и поручением президента РФ Владимира Путина о разработке отечественной игровой консоли (см. „Ъ“ от 27 марта). О готовности начать ее разработку и производство уже объявили «Ростелеком» и «Бештау» (см. „Ъ“ от 15 июля).

«Кроме того, в поисках новых решений в области инфраструктуры, разработки, сервисов и услуг приходится искать новых партнеров, находить новые точки соприкосновения»,— отмечает Гаухар Алдиярова. По ее словам, раньше в глазах государства геймеры были частью большой сферы IT, «теперь мы на стыке IT и креатива». Аудитория в России по-прежнему интересуется играми, люди готовы играть и готовы за это платить, говорят в Astrum Entertainment. В компании считают, что «из-за сложностей с оплатой в зарубежных сторах многие потребители перешли на отечественные площадки, что открывает дополнительные возможности перед российскими разработчиками, упрощая доступ к российской аудитории геймеров, а магазины приложений, в свою очередь, готовы предоставлять инструменты для продвижения локальных продуктов».

Гонка на замедление

«В сложное время игры становятся одним из самых доступных видов развлечений»,— отмечает операционный директор «Мира танков» ГК Lesta Games Борис Синицкий. Этот фактор особенно важен в тот момент, когда доступность международного рынка снижается для российского потребителя в силу ограничений издателей и платежных систем, объясняет топ-менеджер: «При этом указанные ограничения хотя и снижают конкуренцию для отечественных разработчиков и производителей, развитию рынка не способствуют, поскольку замедляют приток новых или возвращение прежних потребителей игрового контента».

Сейчас в отрасли известно минимум три группы, которые готовятся консолидировать рынок и публично выйти на него, например, через торговлю акциями на Московской бирже, говорит Василий Овчинников: «Но в сегодняшней экономической ситуации это сложно — высокая ключевая ставка влияет на деловую активность и, конечно, отсрочивает эти инициативы». Негативно влияют на рынок и новые санкции, волна «ухода сервисов», перечисляет он, таких как Notion, ClickUp, Miro, а также «изменения в государственном регулировании».

Среди негативных факторов, влияющих на развитие рынка, в Astrum Entertainment называют общемировой дефицит инвестиций от профильных и непрофильных инвесторов, что усложняет выход на рынок локальных компаний и проектов. «Кроме того, есть риск потери технологической автономии разработчиков и издателей от западного программного обеспечения, отмечают в компании. Однако на данный момент ситуация стабилизировалась благодаря использованию аналогов и разработке собственных технологий».

Юлия Юрасова

«Важно не пытаться ограничивать заказчиков технологиями только одного вендора»

Информационная безопасность в современных условиях стала одним из основных факторов развития IT-индустрии: в качественном продукте со своевременной поддержкой нуждается не только государственный сектор, но и бизнес любого уровня. О том, как развивается российский софт для кибербезопасности, как на него влияет искусственный интеллект (ИИ) и чего ожидать в 2025 году, рассказал технический руководитель Центра мониторинга и реагирования на кибератаки МТС RED SOC **Ильназ Гатауллин**.

— мнение —

— Какие сервисы кибербезопасности предлагает МТС RED и какие обязательства берет на себя в рамках оказания обеспечения защиты?

— МТС RED (ООО «Серенити Сайбер Секьюрити») предоставляет компаниям экосистему технологий кибербезопасности. Это сервисы Центра мониторинга и реагирования на кибератаки МТС RED SOC, а также управляемые сервисы кибербезопасности (Managed Security Services): защита от DDoS-атак и атак на веб-приложения, шифрование каналов связи по ГОСТу, сервис многофакторной аутентификации, повышение киберграмотности сотрудников компаний (Security Awareness). Сервисы поставляются из облака либо в гибридной модели, когда часть программного обеспечения или оборудования устанавливается непосредственно у заказчика. Важно, что это не просто технологии из облака, а экспертные сервисы, то есть вместе с решениями крупнейших вендоров рынка информационной безопасности заказчик получает дополнительную ценность в виде знаний и опыта специалистов по кибербезопасности МТС RED. Они берут на себя поддержку и настройку правил выявления и отражения киберугроз, ведь их надо сохранять в актуальном состоянии. Экспертный сервис — это фактически готовая функция кибербезопасности «под ключ».

Все сервисы кибербезопасности МТС RED поставляются в соответствии с условиями SLA (Service License Agreement), которые мы оговариваем с заказчиками. Например, специалисты Центра мониторинга и реагирования на кибератаки МТС RED SOC обязуются принять меры реагирования в течение получаса после выявления критически значимого инцидента информационной безопасности. Ни один другой центр мониторинга на рынке не делает этого быстрее.

И в целом подключение всех сервисов дает наглядные результаты. Например, сервис МТС RED Anti-DDoS может подключаться для защиты веб-сайтов непосредственно во время атаки и таким образом практически в моменте восстановить их доступность. А по результатам работы сервиса МТС RED Security Awareness за первый месяц процент уязвимых сотрудников в компаниях снижается на 50% и более.

— Почему МТС RED делает ставку именно на сервисы кибербезопасности, а не на продукты, которые компания разворачивает у себя?

— Мы разрабатываем собственные продукты в сфере кибербезопасности, но нам кажется правильным не пытаться ограничивать заказчиков технологиями только одного вендора. Ни один разработчик на рынке не делает одинаково качественные решения во всех сферах защиты от кибератак, каждый хорош в чем-то своем. Мы даем заказчикам возможность выбора.

Но главное — сервисная модель решает ряд проблем, которые сейчас мешают компаниям создавать надежную эшелонированную защиту от кибератак. В частности, это сложности с дефицитом и высокой стоимостью квалифицированных специалистов по кибербезопасности. Разворачивая решения у себя, компания должна набрать штат сотрудников, которые будут их поддерживать и сопровождать. Покупая экспертный сервис, заказчики избавляются от этой необходимости. Кроме того, расходы на оплату сервисов — операционные, а не капитальные затраты, и это важно с точки зрения финансового планирования и отчетности. Наконец, с учетом роста числа атак на российские компании большую значимость приобретает вопрос сроков внедрения технологий кибербезопасности. Мы можем взять компанию под защиту прямо в момент, когда она находится под атакой. Классические же проекты внедрения длятся месяцами, а то и дольше.

— По вашим данным, насколько увеличились кибератаки за последние два года и на что конкретно?

— В 2022 году все компании сферы кибербезопасности говорили о взрывном росте числа хакерских атак, в СМИ регулярно появлялись новости о взломе тех или иных крупных компаний. Казалось, что это пик возможного числа попыток вредоносных кибервоздействий на Россию. Однако уже в 2023 году МТС RED SOC зафиксировал двукратный рост числа атак по сравнению с 2022 годом, а с начала этого года наш Центр мониторинга отразил более 70 тыс. кибератак — в полтора раза больше, чем за весь 2023 год.

С начала этого года МТС RED SOC отразил более 70 тыс. кибератак — в полтора раза больше, чем за весь 2023 год

Также очень интенсивно от года к году растет количество DDoS-атак на веб-ресурсы российских компаний. Так, в 2023 году МТС RED отразил свыше 6 тыс. DDoS-атак на ресурсы своих заказчиков, а с начала 2024 года — уже более 20 тыс. За это время заметно изменилась направленность таких атак. Если в 2023 году атакам, нацеленным на прерывание работы интернет-ресурсов, были более подвержены сайты промышленных предприятий (23% атак), банков (22%) и лишь затем — IT (21%), то за девять месяцев текущего года IT-сфера стремительно вырвалась на первое место, отодвинув промышленность и финансы на второе и третье соответственно. Только за третий квартал наш сервис защиты от DDoS-атак зафиксировал свыше 6,8 тыс. DDoS-атак на веб-ресурсы IT- и телеком-организаций. То есть тренд к росту числа атак развивается: Россия стала настоящим полигоном для хакеров.

— Есть ли какая-то отраслевая или региональная специфика у кибератак?

— Мы видим, что бОльшая часть критически значимых атак направлена на отрасли, относящиеся к критической информационной инфраструктуре (КИИ) России. В этом году на них пришлось 69% от общего числа атак высокой критичности, то есть таких, которые способны были вызвать длительный простой бизнеса или ущерб на сумму от 1 млн руб. И этот показатель растет: в первом полугодии 2023 года на КИИ пришлось только 46% таких атак. В первую очередь под удар попали промышленность, телеком, банки, но также мы видим серьезный рост числа атак на здравоохранение. В первом полугодии 2024 года Центр мониторинга и реагирования на кибератаки МТС RED SOC отразил на 32% больше критичных атак на эту отрасль, чем за аналогичный период прошлого года.

Ни один разработчик на рынке не делает одинаково качественные решения во всех сферах защиты от кибератак

Если говорить об отраслевой специфике, то здесь методы атак зависят от цели хакеров. Например, атакуя промышленность, хакеры стараются как можно дольше оставаться незамеченными и осуществлять шпионаж, скрытно собирая информацию, которой обладают промышленные предприятия. В первом полугодии почти половина всех атак на промышленность пришлась на выходные и праздничные дни или нерабочие часы. При этом доля критических инцидентов в ночное время заметно возрастала: с 12% в рабочие часы компаний до 25% — в ночные.

ПРЕДОСТАВЛЕНО МТС RED

В организациях сферы здравоохранения хакеры чаще всего пытаются похитить персональные данные пациентов или остановить рабочие процессы клиник и лабораторий. Поэтому такие организации чаще сталкиваются с утечками персональных данных или вирусами-шифровальщиками.

Что касается региональной специфики кибератак, она обусловлена в первую очередь разным уровнем цифровизации регионов и традиционно более высокой концентрацией бизнеса в столицах и городах-миллионниках. Например, по числу DDoS-атак несколько лет подряд лидирует Центральный федеральный округ с Москвой и Московской областью. В третьем квартале 32,9% всех DDoS-атак пришлось именно на этот регион. На столичные компании были зафиксированы и самая мощная (свыше 200 Гбит/с), и самая длительная (свыше 72 часов) DDoS-атака за последние три месяца. Однако, кроме этого, злоумышленники активно атаковали веб-ресурсы организаций Уральского и Сибирского федеральных округов, где много промышленных предприятий, которые сейчас активно наращивают цифровизацию производства. Именно промышленность стала второй по популярности после IT мишенью для DDoS-атак в третьем квартале текущего года.

— Какие есть тренды в кибератаках, как они изменились за последние два года и с чем чаще всего вы сталкиваетесь?

— Наверное, главный тренд — это попытки атаковать организации через их IT-подрядчиков. Они выступают таким промежуточным звеном, своего рода троянским конем. Если компания, которая является истинной целью киберпреступников, хорошо защищена сама по себе, они пытаются взломать ее IT-подрядчика, который имеет легитимный доступ в инфраструктуру конечной жертвы. Пользуясь этими доступами, хакеры проникают в компанию, минуя все средства защиты, и таким образом могут долго оставаться незамеченными. Специалисты МТС RED SOC отмечают, что в ходе таких атак злоумышленники могут очень искусно маскировать развитие атаки под легитимные и привычные действия IT-подрядчика вплоть до того, что они «работают» строго в периоды согласованных «технологических окон».

Заметным трендом этого года стало повышение качества фишинговых атак на сотрудников компаний. Это во многом связано с распространением технологий искусственного интеллекта. С развитием ИИ стало труднее распознавать фишинговые сообщения, так как генеративные модели уже могут написать вполне правдоподобный текст в стилистике публичной личности.

Мощность и продолжительность DDoS-атак тоже стабильно растет. Если в начале 2023 года мы редко фиксировали атаки на веб-ресурсы заказчиков интенсивностью 100 Гбит/с, то сейчас атаки свыше 200 Гбит/с уже не редкость.

— Какие типы кибератак сложнее всего отразить на данный момент?

— Те же атаки через подрядчика, о которых я уже говорил, очень сложно выявлять. Поскольку в такой схеме атаки хакеры проходят «ниже радаров» стандартных средств защиты, компаниям необходимо тщательно контролировать все события внутри своей инфраструктуры и перманентно заниматься поиском аномалий. Иных инструментов пока нет, ведь IT-подрядчики не попадают под какое-то отдельное регулирование, а заказчики слабо влияют на их уровень защищенности.

Вообще же сложности в отражении кибератак часто связаны не с техническими возможностями компаний или их сервис-провайдеров, а с подходом к проектам по кибербезопасности. Чтобы центр мониторинга мог обеспечить бизнес-результат в виде устойчивости заказчика к кибернападениям, под мониторингом должна находиться вся значимая IT-инфраструктура компании. Заказчик же порой хочет сэкономить на защите и в результате оказывается в ситуации, когда хакеры успешно атакуют те сегменты, которые SOC не мониторит, то есть проект реализован, а итоговая бизнес-цель не достигнута.

И, конечно, в современных реалиях очень важно круглосуточно контролировать события в инфраструктуре. Выше я говорил о специфике атак на промышленность, где почти половина критических атак начинается в нерабочее время. В других отраслях мы видим ту же картину, просто не в таком масштабе. Но ведь достаточно и одной серьезной успешной атаки, чтобы нанести драматический ущерб бизнесу. Чтобы этого избежать, атаку необходимо выявить и заблокировать на самых ранних стадиях, а для этого нужен круглосуточный мониторинг инцидентов.

При этом самым эффективным способом проникновения хакеров в IT-инфраструктуру организаций остаются фишинговые письма в адрес ее сотрудников. Пользователи не умеют распознавать уловки мошенников и сами скачивают на рабочие станции вредоносное ПО, которое позволяет хакерам развивать атаку дальше по сети компании. К сожалению, нельзя раз и навсегда научить пользователей выявлять фишинг. Методы и подходы злоумышленников эволюционируют, они активно эксплуатируют меняющуюся информационную повестку. Поэтому компании, особенно крупные, должны постоянно проводить среди сотрудников мероприятия по повышению навыков противодействия фишингу.

Возможно, именно ИИ поможет центрам мониторинга сделать следующий большой шаг на пути к максимально быстрому и качественному выявлению и отражению хакерских атак

— В каких отраслях сервисы кибербезопасности сейчас пользуются наибольшим спросом и почему?

— Совокупно по всем сервисам нельзя выделить какие-то отрасли, эта модель применяется повсеместно. Но можно выделить тренды в разрезе отдельных решений. Например, сервисы Центра МТС RED SOC активнее всего используют заказчики из сфер промышленности, IT, ритейла, телекоммуникаций. При этом за последний год пул заказчиков активно прирастал компаниями сферы девелопмента, здравоохранения, СМИ, HoReCa. Сервисы МТС RED Anti-DDoS и МТС RED WAF сегодня необходимы, по сути, любой организации, имеющей веб-ресурсы, но в особенности тем, функционирование которых напрямую зависит от их бесперебойной работы и защищенности. Это и финансовая, и транспортная сфера, и онлайн-ритейл, и госсектор. А шифрование каналов связи при передаче по ним конфиденциальной информации (ГОСТ VPN) напрямую предписано законодательством государственным органам, субъектам КИИ, операторам персональных данных, компаниям сферы электроэнергетики, финансов, медицины.

— Каковы перспективы применения ИИ в SOC? Как вы развиваетесь в этом направлении? Чем ИИ может быть полезен?

— ИИ может стать отличным инструментом автоматизации работы центров мониторинга и реагирования на кибератаки, а также помочь в выявлении неочевидных человеческому глазу паттернов на базе того огромного потока данных о событиях информационной безопасности, которые ежедневно обрабатывает SOC. Мы активно исследуем различные гипотезы и возможности в данном направлении.

Например, все центры мониторинга сталкиваются с задачей по минимизации числа ложноположительных срабатываний — когда нормальные действия пользователей ошибочно принимаются за признаки кибератаки. Это не недостаток сервисов, а следствие того, что в различных компаниях приняты различные же бизнес-процессы. Скажем, в одной компании подключение сотрудника к корпоративным IT-ресурсам из-за границы будет нормой, а в другой это же событие будет говорить о том, что учетная запись этого сотрудника взломана и к IT-инфраструктуре пытается получить доступ злоумышленник. Поэтому правила выявления инцидентов сейчас приходится кастомизировать вручную, это нагрузка на специалистов и заказчика, и центра мониторинга. Мы считаем, что ИИ может автоматизировать этот процесс, выделяя критерии отнесения срабатываний к ложным или «боевым», и — обязательно под контролем человека — свести число ложноположительных срабатываний к минимуму.

Кроме того, если заказчик предпочитает применять меры реагирования силами своей команды специалистов, центр мониторинга передает им отчет о зафиксированном инциденте и рекомендации по его устранению. Для этого аналитики выполняют большой объем рутинных операций: получают из базы данных ретроспективные данные, информацию об инструментах атаки из внешних источников. Когда речь идет о типовом инциденте, анализ которого не составляет труда, все эти операции можно поручить ИИ, а человек будет только верифицировать итоговый документ. Это дает преимущество в скорости реагирования на кибератаку, что всегда имеет определяющее значение для минимизации ущерба.

Что касается обработки больших объемов данных и выявления определенных паттернов, здесь мы исследуем возможности ИИ в области выявления аномалий и поиска признаков атак, которые остались незаметными для технических средств защиты (Threat Hunting). Возможно, именно ИИ поможет центрам мониторинга сделать следующий большой шаг на пути к максимально быстрому и качественному выявлению и отражению хакерских атак.

— Как планируется развивать сервисы кибербезопасности в 2025 году?

— Мы планируем активно наращивать и спектр различных технологий кибербезопасности, предоставляемых по сервисной модели, и варианты технологий от разных вендоров в рамках одной категории. В частности, в ближайшее время планируем дополнить линейку сервисов технологиями защиты от вредоносных ботов, со временем — привлечь к сотрудничеству новых вендоров, например предоставляющих защиту от DDoS-атак.

Наша цель — создать максимально полное предложение, и не только из атомарных технологий, но и в формате бандлов, адаптированных к потребностям различных отраслей и сегментов бизнеса. Мы хотим, чтобы заказчик мог обратиться к нам и получить как решение конкретной нишевой задачи, так и полный спектр инструментов защиты, отвечающий потребностям именно его компании.

Интервью взял Матвей Кислинский

Голос из прекрасного далека

Объем мирового рынка голосовых роботов к 2027 году достигнет $98,2 млн, увеличиваясь на 18,6% ежегодно. Сегмент будет развиваться за счет растущего внедрения устройств для «умного дома», появления новых вариантов взаимодействия с голосовыми помощниками, а также совершенствования вычислительных мощностей генеративных систем, считают участники рынка. „Ъ“ разобрался, какие новые функции голосовых помощников экосистемы и мобильные операторы предложат пользователям.

— потребительские технологии —

АНАТОЛИЙ ЖДАНОВ

Мировой рынок голосовых помощников переживает этап развития и трансформации. Так, объем глобального рынка голосовых роботов к 2027 году составит $98,2 млн при росте 18,6% ежегодно (совокупный среднегодовой темп роста), следует из исследования аналитической компании IndustryARC о рынке голосовых роботов. Достижение показателя обеспечат увеличивающееся внедрение устройств для «умного дома» со встроенной технологией автоматического распознавания речи, растущее проникновение умных колонок, смартфонов и др.

Сейчас на российском рынке есть несколько представителей голосовых помощников от IT-компаний. Речь идет об «Алисе» («Яндекс»), «Марусе» (VK), «Салюте», «Афине», «Джой» («Сбер») и «Секретаре» (ранее — «Олег», Т-банк). На западном рынке самые популярные примеры — это Alexa (Amazon), Google Assistant и Siri (Apple). Сами голосовые помощники решают сразу несколько задач: упрощение поиска для пользователей, автоматизация повседневных задач, а также возможность для бизнеса оставаться на связи с клиентом 24/7. «Например, при помощи ассистента можно записаться к парикмахеру, врачу, включить сигнализацию и др.»,— перечисляет гендиректор агентства TelecomDaily Денис Кусков.

Голос в каждый дом

Два самых распространенных канала взаимодействия пользователя с голосовым помощником — смартфон и колонка. Рынок голосовых устройств по итогам прошлого года составил 36 млрд руб. против 21 млрд руб. в 2022 году, уточнили в МТС. Прогнозируется, что к 2025 году объем рынка ассистентов достигнет 62 млрд руб., увеличившись по сравнению с 2022 годом на 195%. В целом по итогам года сегмент достигнет 51 млрд руб., следует из исследования оператора. Так, к 2025 году будет продано порядка 7,9 млн устройств, а в этом году — порядка 6,6 млн устройств. При этом эксперты и компании пока затрудняются оценивать рынок голосовых помощников. Их функции пока не монетизируются, уточнил руководитель агентства Content Review.com Сергей Половников: «А рынком можно называть лишь то, что продается».

Среди самых востребованных навыков ассистентов, популярных и у российских, и у зарубежных пользователей, в опрошенных „Ъ“ экосистемах называют трансляцию музыкальных произведений, поисковую выдачу с погодой и новостями, а также управление «умным домом». В целом уровень осведомленности об «умных домах» в России довольно высокий, отмечали во ВЦИОМе. Так, 80% россиян знают о технологии, из них 23% использовали функции «умного дома», оставшиеся 57% знают о системе, но лично не пользовались ей. Кроме вышеперечисленных функций, голосовых помощников используют в роли будильника, напоминающего о важных делах, а также собеседника.

Потребители уже привыкли к ассистентам в колонках и телефонах, чуть меньше — в телевизорах, считают опрошенные „Ъ“ участники рынка. Поэтому в будущем ассистенты будут появляться на новых поверхностях, считает первый вице-президент по телекоммуникационному бизнесу МТС Инесса Галактионова: «Дальше они будут „жить“ прямо в телефонной трубке, могут стать частью умных носимых устройств: микрофонов, очков, корпоративных и офисных платформ». Будущий активный рост использования голосовых помощников подтверждают и данные исследований. Так, каждый десятый абонент мобильных операторов уже сейчас использует голосовых помощников, отмечали в Rambler & Co. Среди полезных функций голосовых помощников респонденты называли прием звонков с возможностью прослушать запись разговора (48%) и отправку ее в мессенджеры (32%), настройку персонализированных ответов (13%), а также выбор голоса и характера ассистента (7%). Дальше сценарий использования ассистентов изменится, считает Инесса Галактионова.

Трое на звонке

Российские IT-компании продолжают совершенствовать своих голосовых помощников. Например, Alexa от Amazon долгое время отличалась развитыми навыками в сегменте электронной коммерции: могла делать заказы, сообщать статус заказов, вести список покупок. Но тот же «Яндекс» сейчас активно развивает своего ассистента в этом направлении — «Алиса» уже может помогать с заказами «Такси», из «Лавки», «Маркета». Для МТС как для экосистемы разработка голосовых ассистентов решает две важные задачи, говорит Инесса Галактионова: «С одной стороны, это расширение пользовательского опыта, добавление совершенно нового функционала, который до нас не делал никто не только в России, но и за рубежом. С другой стороны, это возможность создать новую частотную витрину для развития экосистемы, запуска и монетизации новых сервисов, возможность получить конкурентное преимущество в телекоммуникационном бизнесе».

Сама МТС работает над внедрением умного голосового ассистента, который сможет ответить практически на любой вопрос прямо во время телефонного разговора — ответ услышат оба собеседника. Параллельно технология позволит компании расширить применение технологий искусственного интеллекта (ИИ) и анализа больших данных в привычных голосовых услугах во время телефонных звонков. Ассистент сможет не только дать прогноз погоды на завтра или подсказать адреса ближайших магазинов или кафе, но и сделать резюме разговора, отправив его в виде текста. Так, у абонента появится возможность управлять звонком и вести диалог в режиме реального времени. Уточняется, что в будущем цифровой помощник обзаведется новыми функциями, например сможет переводить разговор на разные языки в режиме онлайн и давать советы по общению. «Мы создаем продукты для взаимодействия абонентов друг с другом и с бизнесом, причем они будут работать в любой модели телефона, не зависят от наличия интернета»,— отмечает Инесса Галактионова.

Нововведение позволит оператору как получить конкурентное преимущество (предлагать что-то большее, чем просто связь), так и «обогатить опыт» своего клиента, считают опрошенные „Ъ“ участники телекоммуникационного рынка. Кроме того, голосовые помощники дают возможности для партнерств с другими бизнесами: «Ассистент может не только рассказать о ресторанах в городе, но и порекомендовать партнерское предложение, может предложить оформить заказ нужного товара в интернет-магазине и др.». Параллельно продажи устройств с голосовыми помощниками ежегодно растут, напоминает Денис Кусков, «учитывая невысокую стоимость и включение их в контур „умного дома“».

«Не просто голос из колонки»

Сейчас уже все экосистемы и IT-компании рассматривают ассистентов в роли набора умных решений, а не просто «голоса из колонки, рассказывающего о погоде». В этом случае голосовой помощник позволяет сокращать время пользователя на рутину, ежедневно решать его задачи в повседневном мире. Помимо уже перечисленных факторов, на рост сегмента повлияет и развитие больших вычислительных и языковых моделей. В числе последних — как языковые, так и мультимодальные, которые «могут „смотреть“ камерами на окружающий мир, „слушать“ и понимать его». Компании в лице Google, Amazon, «Яндекса» и др. продолжают развивать когнитивные способности ассистентов для лучшего взаимодействия с пользователями. Так, появляются новые инструменты, объединяющие модели в «агентские» решения. Последние могут решать комплексные задачи, в том числе в повседневном мире: вызвать такси, забронировать столики и билеты, записаться к врачу, отвечать на телефон вместо пользователя, решать задачи с детьми.

Параллельно благодаря внедрению генеративных нейросетей голосовые помощники становятся более персонализированными, отмечал гендиректор компании «Наносемантика» Станислав Ашманов (см. „Ъ“ от 14 марта). Они запоминают контекст беседы, подстраиваются под пользователя, а в скором будущем могут и предупреждать пользователей о том, что им звонят мошенники. Так, у МТС уже есть сервис по блокировке сомнительных и спам-звонков «МТС Защитник». Само приложение анализирует, от кого поступил входящий вызов, есть ли подозрение на мошенничество. В момент звонка абонент получает голосовое уведомление, которое будет слышно только ему. Технологии искусственного интеллекта проводят проверку, какой голос (синтезированный или живой) используется при звонке. Затем Big Data МТС сверяет биометрию голоса с базой мошеннических голосов и проверяет анализ текста звонящего на предмет мошеннических сценариев.

Последний фактор развития рынка голосовых помощников — совершенствование вычислительных мощностей. Обучение и запуск больших моделей стоит все меньше. Процесс будет ускоряться, и в результате конечные продукты на их основе будут доступнее широкому кругу потребителей, считают в МТС. Любой новой технологии требуется время для широкого проникновения, отмечает Инесса Галактионова: «Но по тому, с какой скоростью новые технологии, о которых мы только вчера узнали, входят в нашу жизнь, можно предположить, что рынок голосовых помощников ждет быстрый рост».

Юлия Датская

Почта ударилась в цифру

— рынки —

АНАТОЛИЙ ЖДАНОВ

Благодаря цифровой трансформации выручка «Почты России» от продаж услуг в цифровых каналах достигла 33%, а внедренные решения позволили автоматизировать расчеты логистических маршрутов. Компания продолжает не только внедрять перспективные решения, но и делает это на отечественном софте, доля которого в 2024 году достигнет 95%. „Ъ“ разбирался, как «Почта России» занимается импортозамещением и каких результатов компании уже удалось добиться благодаря цифровизации логистики.

В сентябре «Почта России» объявила, что переходит с Windows на российскую операционную систему (ОС) «Альт» на базе Linux от разработчика «Базальт СПО». Своим переходом компания начала масштабный проект по импортозамещению программного обеспечения, в результате которого 130 тыс. рабочих мест сотрудников отделений, логистических центров и административного персонала переведут на отечественную ОС.

«„Почта России“ играет ключевую роль в обеспечении логистических и коммуникационных потребностей граждан и организаций на территории огромной страны. Курс на трансформацию компания взяла еще в 2021 году»,— рассказывает заместитель гендиректора по цифровой трансформации компании Дмитрий Чудинов. Он объясняет, что за это время было внесено множество изменений: внедрение автоматизированных систем сортировки, развитие электронных услуг, создание удобных мобильных приложений и внедрение современных решений для управления логистикой. В целом доля замещенных иностранных решений в «Почте» достигла 87% в 2023 году, а в 2024 году этот показатель прогнозируется в 95%. «Это позволяет обоснованно заявлять об эффективном движении в направлении собственного цифрового суверенитета и импортонезависимости ключевых информационных систем»,— говорит Дмитрий Чудинов.

Транспорт в облаках

Цифровая трансформация обусловлена в том числе изменением стратегии: из почтового оператора компания стремится стать логистической, которая использует в основном собственные IT-решения, объясняет господин Чудинов. Для этого своя IT-компания «Почтатех» занимается развитием и поддержкой внутренних продуктов, без которых оптимизировать существующие процессы невозможно. В условиях быстро меняющегося мира применение технологий становится залогом конкурентоспособности и устойчивого развития компании.

Одним из ключевых продуктов «Почты» станет «Единая логистическая платформа», которая объединит логистические системы компании и функционал по управлению как собственной транспортной и складской инфраструктурой с современным оборудованием для автоматизированной сортировки, так и ресурсами внешних подрядчиков, партнеров и провайдеров услуг.

Платформа, рассказывает Дмитрий Чудинов, включает инструменты математического моделирования и искусственного интеллекта (ИИ), что позволяет эффективно с точки зрения отношения к ресурсам и обеспечения рыночных сроков доставки синхронизировать все логистические мощности. А в онлайн-режиме — строить предиктивные расчеты и анализ отклонений, а также в автоматизированном режиме запускать корректирующие процессы. «Традиционный процесс сортировки почтовых отправлений — трудоемкий и подверженный ошибкам. Мы уже внедрили автоматизированную систему сортировки „Сортмастер“, что позволило повысить точность и скорость сортировки».

Одним из ключевых элементов платформы является модуль расчета мультимодальных маршрутов, объединяющих автомобильные, железнодорожные и воздушные перевозки. «Мы замещаем систему оптимизации Riverlogic на собственную с применением интеллектуальных алгоритмов при поддержке „Сколково“»,— объясняет Дмитрий Чудинов. Первые результаты компания планирует получить уже в этом году. Современные алгоритмы позволят рассчитать оптимальные пути доставки с учетом текущих условий и загруженности транспортной сети.

«„Почта России“ доставляет более 50 видов отправлений всеми видами транспорта между всеми 38 тыс. отделений с использованием точек сортировки, учитывая контрольные сроки доставки. Это миллиарды комбинаций доставки, которые нужно проанализировать, чтобы найти быстрое и экономное решение для доставки отправления»,— добавляет Дмитрий Чудинов.

Поддержку в принятии наиболее важных решений обеспечивает Единая информационно-аналитическая платформа. «Ее использование позволяет выявить реальный сценарий прохождения бизнес-процессов в компании, разработать способы операционной оптимизации, а также повысить эффективность каждого работника и почтового парка»,— объясняют в «Почте России».

«Мы продолжим совместно с партнерами интенсивную работу в направлении импортозамещения: создание отраслевых отечественных решений в сфере логистики, электронной торговли и других, ИИ и робототехники, а также инновационную деятельность по поиску и тестированию инструментов и продуктов, подходящих под специфику „Почты“. Без этого невозможен технологический суверенитет, что чревато уязвимостями в информационной безопасности компании»,— заключает Дмитрий Чудинов.

Алексей Жабин

Совершенно не секретная информация

— информационная безопасность —

Утечки данных не перестают быть актуальной угрозой для компаний как в России, так и в мире. По данным исследователей киберугроз, в первой половине 2024 года каждая вторая успешная глобальная атака на организации привела к утечке конфиденциальных данных. „Ъ“ выяснил, чего ждать от угрозы утечек к концу 2024 года, какие данные будут в фокусе у злоумышленников и что может положительно повлиять на ситуацию.

По итогам первого полугодия 2024 года утечкой конфиденциальной информации закончилась половина успешных атак на российские организации. К такому выводу пришли в компании—вендоре решений для кибербезопасности Positive Technologies. Самое частое последствие успешных атак — нарушение основной деятельности организации, на втором месте — утечка конфиденциальной информации, оценивают в компании. Аналитики фиксируют также непрерывный рост этого показателя: в 2022 году утечки составляли 37% последствий атак, в 2023-м — 41%, а в первом полугодии 2024 года — уже 48%. «На данный момент нет никаких предпосылок к тому, чтобы число утечек снижалось»,— считает руководитель направления аналитических исследований Positive Technologies Ирина Зиновкина.

В то же время в первом полугодии Россия возглавила пятерку стран—лидеров по количеству объявлений на теневых форумах с долей 10%, рассказывает госпожа Зиновкина: «Злоумышленников больше всего интересуют свежие базы персональных данных и данные учетных записей сотрудников российских компаний». Чаще всего хакеров привлекают финансовый сектор, IT и сфера логистики, добавляют в компании InfoWatch.

Однако проблема актуальна не только для России. Так, в конце лета стало известно, что на одном из хакерских форумов опубликована база данных почти 2,7 млрд личных данных жителей США. Компания National Public Data, которая собирает и обрабатывает большие объемы личной информации для верификации и предоставления других услуг, позже признала, что часть данных была похищена у нее. Среди них были имена пользователей сети, адреса электронной почты, номера телефонов, номера социального страхования и почтовые адреса, предупредили в National Public Data.

В России же увеличивается доля малых и средних предприятий среди пострадавших от утечек, говорит руководитель направления сервисов защиты облачного провайдера Nubes Александр Быков. Самыми ценными для киберпреступников являются учетные записи граждан и организаций из финансовых сервисов. «Компрометация таких аккаунтов позволяет реализовать большое количество сценариев по извлечению незаконной финансовой выгоды»,— объясняет господин Быков.

В 2023 году из российских финансовых организаций утекло 170,3 млн записей персональных данных клиентов (без учета платежных данных) — это в 3,2 раза больше, чем в 2022 году, подтверждает руководитель направления по перспективным ИБ-решениям компании «Системный софт» Егор Петров. Первое полугодие 2024 года насчитывает более 600 млн записей.

Также «на черном рынке имеют ценность данные, позволяющие получить удаленный доступ к IT-инфраструктуре»,— продолжает руководитель группы OSINT Центра противодействия киберугрозам SOC CyberART компании Innostage Альберт Антонов: «Самой популярной целью злоумышленников сегодня является распространение информации о взломе инфраструктуры организаций».

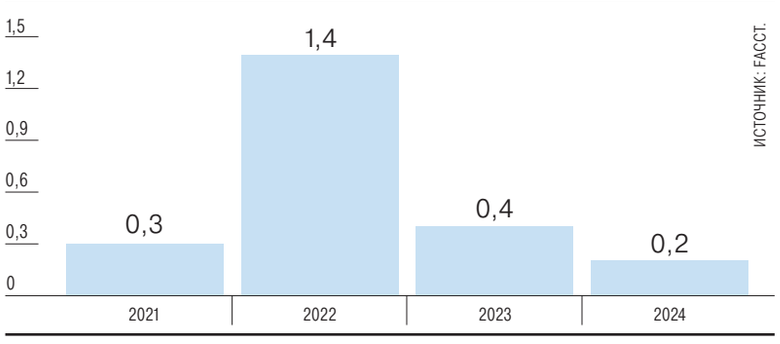
Всплески в количестве утечек до конца года могут произойти вследствие эксплуатации злоумышленниками уязвимостей в популярном программном обеспечении, например как в системах защищенной передачи данных в 2023 году, прогнозируют в Positive Technologies: «Если подобных событий не произойдет, а также будет стабильная геополитическая обстановка, тренды касательно утечек данных останутся теми же».

Опрошенные „Ъ“ эксперты сходятся во мнении, что на ситуацию с защищенностью российских компаний должен повлиять рассматриваемый в Госдуме законопроект о финансовой ответственности бизнеса за утечки данных. В конце января депутаты уже приняли в первом чтении сразу два проекта, ужесточающих порядок работы компаний с персональными данными россиян: о введении оборотных штрафов за инциденты, и о введении уголовной ответственности за кражу и распространение такой информации (см. „Ъ“ от 24 января).

Вступление в действие закона, усиливающего административную ответственность за нарушения при работе с персональными данными, может стать дополнительным стимулом, мотивирующим компании активнее применять меры по минимизации рисков утечек и ответственно подходить ко внутренней безопасности, считает Егор Петров. «По нашим оценкам, к концу года мы увидим положительную динамику снижения допускаемых инцидентов и рисков утечек информации»,— надеется он.

Татьяна Исакова

ДИНАМИКА КОЛИЧЕСТВА СТРОК ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ В УТЕЧКАХ (МЛРД)



GIS ГАЗИНФОРМ СЕРВИС 20 лет вместе

Кибербезопасность по-русски

В Москве и Санкт-Петербурге в седьмой раз прошел масштабный форум GIS DAYS 2024, организованный компанией «Газинформсервис», который стал одним из ключевых событий осени для всех, кто работает в сфере кибербезопасности, а также заинтересован в развитии защиты своего бизнеса. „Ъ“ посетил GIS DAYS в Москве, пообщался с организаторами и участниками форума и убедился: отрасли есть что предложить бизнесу как в рамках импортозамещения к 2025 году, так и с точки зрения технологического развития защиты данных.

ПРЕДОСТАВЛЕНО «ГАЗИНФОРМСЕРВИС»

— информационная безопасность —

В Санкт-Петербурге и Москве 3–4 октября прошел ежегодный форум GIS DAYS 2024 (Global Information Security Days), где отраслевые эксперты и представители крупных компаний подвели предварительные итоги импортозамещения, обсудили последние тренды в построении киберзащиты и актуальные угрозы безопасности. Главной темой события в этом году стали «Уроки RUSSKOГО». Форум также предоставил площадку для обмена опытом, знакомства с новейшими технологиями и продуктами в сфере кибербезопасности. Организатор форума компания «Газинформсервис» показала, что сегодня информационная безопасность не просто техническая задача, а стратегический приоритет для каждой организации и пользователей.

● *«Газинформсервис» — российский разработчик программных и программно-аппаратных решений для информационной безопасности и комплексной инженерно-технической охраны. Компания была основана в Санкт-Петербурге в 2004 году, в этом году ей исполняется 20 лет. Решениями «Газинформсервиса» пользуются госсектор и бизнес не только в России, но и в Киргизии, Белоруссии и Казахстане.*

Первые сессии на GIS DAYS 2024 в Москве 3 октября были посвящены ландшафту киберугроз и изменениям в работе группировок хакеров (APT-группировок и др.), а открыл форум заместитель гендиректора, технический директор «Газинформсервиса» Николай Нашивочников. Он отметил, что с каждым годом форум становится все масштабнее и охватывает все больше тем, волнующих отрасль. Господин Нашивочников также анонсировал ключевые темы технических GIS DAYS в Москве: это киберанализтика и центры мониторинга и реагирования на угрозы (SOC). В рамках последней компания представляет и собственный центр, поэтому технические дни форума были заявлены не только теоретическими, но и практическими.

В Москве 3 октября промежуточными итогами года в области защиты данных и инфраструктуры, а также импортозамещения поделились представители крупнейших вендоров: Positive Technologies, «Кода Безопасности», «Лаборатории Касперского», Zecurion, «ИнфоТеКС», Xello, Fplus, BI.ZONE, R-Vision, UserGate, ГК «Солар», «Аладдина», «АйТи-Бастиона», «Киберпротекта», ГК «ИнфоВотч», «Атом Безопасности» и других.

Как отметил заместитель гендиректора, руководитель департамента организации работ с заказчиками «Газинформсервиса» Роман Пустарнаков, вопрос импортозамещения как в кибербезопасности, так и в IT в целом не просто стал актуальнее для рынка, но и сами его участники заметно продвинулись в решении этой задачи. «Мы идем по пути импортозамещения с 2014 года, события 2022 года заметно ускорили процесс»,— отметил он. Под импортозамещением в сфере кибербезопасности рынок давно понимает не только софт. «Это и так называемое железо, и программно-аппаратные комплексы (ПАК)»,— уточняет эксперт. «Мы эту тенденцию очень четко прослеживаем, и, видя и понимая, насколько нужны и ПАКи рынку, мы создаем интеграции с производителями ПАКов, в том числе сделали недавно интеграцию наших продуктов с SafeNode System Loader — аппаратной платформой одного из производителей, а также сделали ПАК вместе с нашей СУБД Jatoba»,— рассказал Роман Пустарнаков.

Центр реагирования набирает обороты

Со своей стороны компания «Газинформсервис» представила созданный в 2024 году собственный Центр мониторинга и реагирования на киберугрозы G.SOC, который включает в себя работу с большими данными об инцидентах, команду экспертов, работающих над реагированием в режиме 24/7, и другие высокотехнологичные направления. Как рассказал „Ъ“ Николай Нашивочников, SOC от «Газинформсервиса» постоянно совершенствуется, внедряются новейшие технологии и подходы в области информационной безопасности, чтобы обеспечивать максимальную защиту для клиентов в условиях быстро меняющегося цифрового мира. В настоящее время в G.SOC работает команда из 40 высококвалифицированных специалистов по кибербезопасности, которая включает аналитиков по безопасности, инженеров по реагированию на инциденты, экспертов по угрозам, пентестеров и других профессионалов, которые защищают информационные системы наших клиентов от постоянно эволюционирующих угроз.

SOC от «Газинформсервиса» постоянно совершенствуется, внедряются новейшие технологии и подходы в области информационной безопасности, чтобы обеспечивать максимальную защиту для клиентов

Так, центр обеспечивает анализ информации о потенциальных инцидентах и проверку их состоятельности для своевременного подтверждения инцидентов. «Он также уже осуществляет обогащение подтвержденных инцидентов дополнительными сведениями о затронутых активах и источниках возникновения, характере воздействия, возможных негативных последствиях, приоритизации и так далее»,— говорит Николай Нашивочников.

Среди других услуг Центра G.SOC эксперт перечислил следующие:

локализация подтвержденного инцидента, снижение негативных последствий, вытеснение злоумышленника из инфраструктуры и восстановление штатного режима работы;

тестирование инфраструктуры на проникновение;

сканирование инфраструктуры на предмет наличия «известных» уязвимостей, их приоритизация, информирование о выявленных уязвимостях, предоставление рекомендаций по их устранению и контроль;

сбор и поддержание в актуальном состоянии информации об IT-активах, сетях и сервисах, определение взаимозависимостей и критичности активов.

«По своему опыту мы понимаем, что для многих компаний создание собственного SOC может быть слишком затратным (как денег, так и времени) и трудоемким процессом. В этом вопросе не получится просто потратить деньги на оборудование и ПО, а на выходе получить готовое решение — без компетентных людей и отлаженных процессов эти деньги будут потрачены впустую»,— рассказал Николай Нашивочников.

У компании огромный опыт в построении систем защиты информации. «Мы регулярно проводим сравнительный анализ, который показывает, что услуги нашего SOC не просто сравнимы по стоимости с построением собственной информационной обороны аналогичного уровня, но чаще даже дешевле таковой»,— продолжает эксперт. «При этом клиент получит гарантированный уровень экспертности исполнителей при минимальных временных затратах на подключение его инфраструктуры к мониторингу. Это позволяет клиентам сосредоточиться на своих основных бизнес-процессах и существенно сократить затраты на содержание собственной команды по безопасности»,— отмечают в «Газинформсервисе».

«Еще до конца текущего года мы добавим в свой арсенал услугу „Киберразведка“ (Threat Intelligence) — это определение ландшафта киберугроз и ретроспективный анализ данных по свежевыявленным индикаторам компрометации. А на начало 2025 года у нас запланирован старт услуги „Поиск киберугроз“ (Threat Hunting), в рамках которой будет выполняться проактивный поиск угроз в инфраструктуре заказчика»,— рассказал Николай Нашивочников.

Наш конкурс уже третий год подтверждает тезис: в России много качественных проектов в IT и кибербезопасности

ПРЕДОСТАВЛЕНО «ГАЗИНФОРМСЕРВИС»

Не только теория: мастер-класс по безопасной работе с СУБД

В рамках практической сессии «Управление безопасностью данных. Работа с неструктурированными данными. Контроль утечек» 4 октября, где представители крупных вендоров ИБ делились своим опытом построения многофакторной и многоступенчатой защиты в 2024 году, мастер-класс провел менеджер по продукту «Газинформсервиса» Юрий Осипов «Защита информации на уровне СУБД».

Системы управления базами данных (СУБД) являются комплексом программных средств, которые стали незаменимы уже во всех крупных компаниях любой сферы. Юрий Осипов начал свой доклад со статистики:

В 2024 году 95% утечек данных происходят из-за человеческого фактора.

75% всех инсайдерских инцидентов произошло из-за человеческой ошибки, где 50% это халатность, а оставшиеся 25% — действия третьих лиц.

Процент компаний, которые сталкиваются с большим количеством инсайдерских инцидентов, вырос с 67% до 71%.

Как подытоживает Юрий Осипов, влияние человеческого фактора на защиту данных и безопасную работу с ними — один из самых сложных для контроля факторов. «Поэтому в современной СУБД должны быть предусмотрены условия, например, для ограничения прав суперпользователя, расширенные парольные политики, просмотр множественных событий безопасности и оповещения о них профильных специалистов»,— говорит эксперт.

Все эти современные меры обеспечения защиты данных объединяются в СУБД Jatoba компании «Газинформсервис». Также Юрий Осипов упомянул внедренный в СУБД отказоустойчивый кластер, переключающий роли при отказе узла. «Очень важно иметь резервные узлы инфраструктуры, резервные ЦОДы, то есть географически разнесенные центры обработки данных, которые примут на себя нагрузку в случае сбоя одного из ключевых». СУБД Jatoba «умеет работать с несколькими отказоустойчивыми кластерами, в том числе географически разнесенными ЦОДами, и автоматически переключать работу и обмен данными между ними».

И, конечно, важную роль в работе с СУБД играет ее эксплуатация. Расширенные средства администрирования позволяют сократить число сотрудников компании, которые обеспечивают ее функционирование. Это, в частности, автоматизированное резервное копирование данных, формирование отчетности о производительности СУБД, планирование заданий, корректировка запросов и так далее. И также на себя автоматизированная система принимает задачи по выявлению нетипичного поведения пользователей в системе, что значительно снижает риски безопасности данных в СУБД Jatoba.

Молодым везде дорога: кого отметили на «Бирже ИБ- и IT-стартапов»

Конкурс молодых команд «Биржа ИБ- и IT-стартапов» уже стал неотъемлемой частью GIS DAYS. В рамках проекта компании «Газинформсервис» и «Делового Петербурга» отбираются лучшие идеи и решения как начинающих разработчиков, так и готового бизнеса и награждают победителя чеком на 1 млн руб. на развитие проекта. В 2024 году победителем «Биржи ИБ- и IT-стартапов» стал проект «Комплекс решений по обеспечению автомобильной кибербезопасности». Всего на конкурс поступило около 100 заявок от ИБ- и IT-стартапов со всей страны.

«Комплекс решений по обеспечению автомобильной кибербезопасности», который многие эксперты между собой уже назвали «подушкой кибербезопасности», предназначен для защиты автомобилей от кибератак. Проект включает в себя две составляющие: систему по обнаружению несанкционированных подключений к шине данных на основе анализа физических параметров электрической цепи, а также систему, которая позволяет осуществлять детекцию инцидентов и кибератак. Комплекс предназначен для автопроизводителей и операторов MaaS-решений.

В целом на конкурсе в 2024 году финалистами стали пять проектов. Помимо победителя, за победу боролись LLM Security Proxy & Monitoring, «Межсетевой экран следующего поколения Traffic Inspector Next Generation», проект FINDLER, а также «Атретек».

«В этом году мы провели обновленный проект „Биржа ИБ- и IT-стартапов“ с уклоном на кибербез. Нам удалось собрать более 40 крепких проектов по линии информационной безопасности. Особенно порадовало то, что бОльшая часть из них — с использованием ИИ. Этот факт подчеркивает динамичное развитие российского рынка информационных технологий в целом. Также важно, что наш конкурс уже третий год подтверждает тезис: в России много качественных проектов в IT и кибербезопасности»,— отметил Николай Нашивочников.

Безопасность по буквам: почему «ИБ-Пророк» может стать настольной книгой в ИБ-отрасли

Презентация медиапроекта — нечастое событие на ИБ-конфекциях, но исключения случаются. «Газинформсервис» представил на GIS DAYS альманах «ИБ-Пророк», где собрал самые актуальные прогнозы 22 лидеров рынка кибербезопасности. Авторы книги учли опыт последних двух лет, самые актуальные выводы из событий кибербезопасности в России и мире, и попросили лидеров мнений описать обозримое будущее защищенности отечественной инфраструктуры.

Мы идем по пути импортозамещения с 2014 года, события 2022 года заметно ускорили процесс

В написании альманаха «ИБ-Пророк» приняли участие такие эксперты, как Наталья Касперская, Александр Шойтов, Алексей Лукацкий, Рустэм Хайретдинов и другие. Эксперты ответили на актуальные вопросы, в том числе: каких последствий стоит ждать от внедрения технологии ИИ, чем могут быть опасны облачные решения, какую роль криптография начнет играть в мире будущего, станет ли российская отрасль ИБ задавать тренды на мировом рынке.

Также прогнозы экспертов посвящены проблемам и безопасности «цифровой личности», вопросам импортозамещения и защиты критической информационной инфраструктуры, работе топ-менеджмента с ИИ и другим. Как отметила гендиректор компании «„Эксперт“ Центр Аналитики» Кристина Муравьева, благодаря созданию альманаха появился прогноз развития рынка информационной безопасности: «Эксперты постарались заглянуть в будущее и создать основу для принятия управленческих решений. Серия „ИБ-Пророк“ рекомендуется к прочтению всем руководителям, акционерам и собственникам, принимающим стратегические решения».

Татьяна Исакова

КОНТЕКСТ

В 2024 году угрозы кибербезопасности становятся все более изощренными и при этом не менее мощными, чем годом ранее. По данным аналитиков, только за первые полгода количество DDoS-атак (с большим числом запросов к серверу для отказа в обслуживании) на российские организации выросло на 16% относительно всего 2023 года (см. „Ъ“ от 9 сентября).

На сложности в отражении кибератак сказывается и появление их новых видов, таких как атаки с использованием искусственного интеллекта. Но не уступают место и целевые атаки на критически важную инфраструктуру, что делает защиту сложнее и требует новых подходов к ней. Также во всех отраслях экономики возрастает повышенная зависимость от цифровых технологий: цифровая трансформация бизнеса и массовое внедрение облачных технологий приводят к увеличению поверхности кибератак. При этом усложняет ситуацию увеличение количества собираемых данных компаниями: объемы данных, хранимых в различных системах, требуют продвинутых решений для их защиты.

«Голосовая экосистема — преимущество МТС в новой технологической волне»

О том, что российский телеком-бизнес развивается быстрее зарубежного, о помощи агентов искусственного интеллекта в выборе и их интеграции в голосовых помощников в интервью „Ъ“ рассказал вице-президент по цифровым продуктам МТС **Максим Лаптев**.

— мнения —

ПРЕДОСТАВЛЕНО ПРЕСС-СЛУЖБОЙ МТС

— Как сейчас развивается телекоммуникационный рынок в России? Можете перечислить три основных фактора роста?

— Начать надо с конвергентов. Лет 20 назад это слово использовалось для бандлирования (процесс объединения нескольких продуктов в один пакет.— **„Ъ“**) разных телеком-услуг, например для совместной продажи мобильной и фиксированной связи. Сейчас в российском телекоме происходит макроконвергенция: бандлируются разного рода услуги. Так, в тарифных планах уже можно найти развлекательные услуги, сервисы безопасности, кикшеринги (краткосрочная аренда электросамокатов). Например, после приобретения компании «Юрент» мы дали возможность нашим пользователям менять минуты на поездки на самокатах, списывать баллы экосистемы МТС и другие интеграции. С точки зрения сервисов безопасности мы уже предоставляем услуги по защите от спама или персональных данных, скоро будут решения в сферах обеспечения приватности и e-commerce (онлайн-торговли.— **„Ъ“**). Грубо говоря, одна из точек роста отрасли сегодня — это объединение услуг в сфере телекоммуникаций со смежными отраслями.

Вторая точка роста — это IoT (интернет вещей, множество физических объектов, подключенных к интернету и обменивающихся данными.— **„Ъ“**), только в его современной интерпретации: интернет автомобилей, носимых устройств и так далее. Идея в том, чтобы движимые и недвижимые вещи были подключены друг к другу для получения сервисов нового поколения. Например, автомобиль может подсказывать, с какой скоростью нужно ехать, чтобы проехать по всем светофорам на зеленый свет, или некое устройство, которое позволит предотвратить столкновение с самокатом. Ожидается, что в России подобные сервисы будут появляться уже в течение следующих пяти лет.

Третий тренд — использование знания о клиентах и сервисов экосистемы для выстраивания потребительских платформ нового поколения. Я говорю не просто о росте лояльности клиента благодаря выгоде в комплиментарных сервисах: забронировал номер на МТС Travel — получил кешбэк на год бесплатной связи. Я говорю о предсказании следующего пользовательского сценария благодаря новым технологиям и знаниям экосистемы с высокой вероятностью и релевантным предложением нового цифрового опыта.

— Можете ли вы назвать основные различия между нашим рынком экосистем и мировым?

— БОльшая часть мировых экосистем развивалась по открытой модели. Мы тоже работаем над этим направлением. Понятно, что до 2022 года МТС концентрировалась на мировых брендах (Apple, Apple Music, Spotify, YouTube и др.). Сейчас мы переориентировались на локальный рынок. Так, например, за последние два года мы заключили стратегические партнерства с компаниями «Юрент», Belka, «Аэрофлот», «Яндекс» и другими. Здесь мы поддерживаем мировой тренд на открытость цифровых экосистем.

Однако, в отличие от мировых экосистем, мы видим сложность в выходе в определенные сегменты, например гейминг. Мы понимаем особенности российского рынка. То есть производить и дистрибутировать игры на 2% мирового ВВП — это всегда сложная задача. Понимая, что для нашей аудитории этот вид цифрового потребления крайне важен, МТС выбрала два пути. Во-первых, мы предоставляем платформу облачного гейминга МТС Fog Play — первую в России, по данным аналитического агентства SimilarWeb в июле. Во-вторых, мы предоставляем удобный платежный сервис для оплаты сервисов гейминга и стриминга. Этими сервисами мы стараемся обеспечить потребление видеоигр нашими клиентами в привычном формате и с лучшим клиентским опытом.

— Какие еще функции предлагает экосистема МТС пользователям, отличающие ее от других участников рынка?

— Как и все экосистемы, мы предлагаем уникальную цифровую бесшовность и комфорт нашему клиенту. Клиенты могут без ввода пароля и привязывания платежных средств проходить в сервисы самокатов, онлайн-кинотеатр, интернет-магазин и многие другие.

Но, в отличие от других экосистем, мы базируемся на телеком-возможностях. Только мы можем по сети мобильного интернета даже без ввода логина или номера телефона идентифицировать нашего клиента в своем или партнерском сервисе. Мы видим большой потенциал в концепции тотальной цифровой бесшовности, когда наши клиенты будут идентифицироваться по всем сервисам интернета. Но еще больший потенциал мы видим в компетенции и восприятии нашего основного потребления в глазах клиента — голоса. Внутри компании мы активно разрабатываем направление под рабочим названием „голосовая экосистема“, цель которого объединить и сформировать целый набор сервисов вокруг голоса: голосовые помощники, контекстные подсказки на экране вызова и в голосовом канале, сервисы «Секретарь» и «Защитник» и другие сервисы нового поколения.

— По вашей оценке, какой процент пользователей МТС ежедневно использует голосовых помощников?

— Я думаю, 60% интернет-пользователей использует голосовых помощников уже сегодня. Это люди, которые каждый месяц прибегают к их услугам. На мой взгляд, у нас сейчас заканчивается эпоха цифровизации, мы пришли к моменту, когда 90% всего уже цифровизовано: госуслуги, e-commerce, онлайн-кинотеатры и прочее. Кажется, цифровых объектов становится так много, что в итоге люди затрачивают гораздо больше энергии и времени на выбор: фильма на вечер, товара в интернете, чем фактического потребления. Есть теория, что эту ситуацию может изменить новая технологическая волна с так называемыми агентами искусственного интеллекта (AI-агенты). Это и чат-боты, и голосовые ассистенты, и дополненная реальность. Идея в том, чтобы эти AI-агенты добывали для вас информацию либо делали за вас поиск и фактическое целевое действие. Мне нравится идея, когда агент это действие сможет реализовать в живом мире, например по моей просьбе забронировать мне столик в ресторане, действительно позвонить в ресторан и нативным разговором с администратором выбрать стол и осуществить бронь.

Смартфон уже из утилитарного узкого сервиса превратился в аналог «суперприложения» со всеми нужными цифровыми сервисами. Я думаю, что следующий шаг развития цифрового потребления именно в этих разнообразных AI-агентах. Когда голосовой помощник сможет из разговора составить краткий пересказ, добавить в календарь поручения, которые обсуждали на рабочей встрече, купить зимнюю резину для автомобиля — и все это он будет делать на разных поверхностях: в колонках, в автомобилях, в телевизорах и, конечно же, в звонках наших пользователей. Уже сейчас мы, например, сделали партнерство с «Яндексом». Мы запустили звонки на телефонные номера через «Яндекс Станцию». Это первый подобный сервис в России, который предваряет развитие концепции голосовой экосистемы.

По этой же логике мы и разрабатываем нашего «Марвина». Мы видим его как специализированного ассистента, который помогает вам прямо в звонках.

— Чем «Марвин» будет отличаться от других голосовых ассистентов на рынке? Как в целом планируется развивать голосового помощника в ближайшие два-три года?

— Одно из применений «Марвина» — отличное контекстное понимание вас в телефонном разговоре. Для этого не нужен мобильный интернет, он будет жить даже в кнопочных телефонах. Например, клиенту очень важно во время разговора в моменте узнать, где поблизости находится необходимый для него товар по хорошей цене, или получить расшифровку длительного разговора с выводами того, о чем договорились собеседники. Мы уже экспериментируем в этой области. Наша технология уникальна, в мире подобных примеров нет. Такая голосовая экосистема сервисов, где ассистенты живут в контексте коммуникаций C2C и C2B,— это будущее, в которое мы верим. Сейчас проходят альфа-тесты, после мы будем тестировать «Марвина» на небольших группах людей с целью детального дообучения наших больших языковых моделей.

— По вашему мнению, как дальше будет развиваться рынок голосовых ассистентов в России?

— Мое личное видение, что в течение пяти лет голосовые ассистенты станут более прикладными — как раз и превратятся в Copilot и AI-агентов на различных поверхностях. Их возможности по обработке Big Data цифрового мира, гиперперсонализация под носителя и возможность совершения конечных действий в «живом» мире — причины, почему мы верим, что они станут незаменимыми компаньонами, без которых уже не представляется повседневная жизнь.

Юлия Датская

Технологиям добирают внешние факторы

— правила игры —

с13

Инвестиции ищут себе место

Впрочем, повышение ключевой ставки ЦБ и отмена субсидирования льготных кредитов не единственный фактор, оказывающий влияние на объемы бизнеса, капитал и финансовую устойчивость участников рынка. Первый вице-президент «Аквариуса» Дмитрий Титов добавляет, что не ясны будущее ряда действующих субсидий на проведение НИОКР, перспектива продления льгот по налогу на прибыль для производителей радиоэлектроники, а также перспективы отмены параллельного импорта. «И, главное, количество отечественных игроков превысило разумные пределы для российского рынка. Именно это в первую очередь отрицательно сказывается на марже и прибыли, экономической устойчивости отрасли»,— уточняет он.

В таких условиях на российском IT-рынке сложился и другой тренд: крупнейшие игроки IT-сектора стали запускать все больше собственных инвестфондов. В июне «Ростелеком» объявил о запуске венчурного фонда «Консоль» — он займется инвестициями в российских разработчиков ПО на стадии расширения, объем фонда составит порядка 8 млрд руб. Ранее в текущем году о запуске венчурных фондов заявили топ-менеджеры «Аквариуса», компания GS Group. В 2023 году венчурный фонд также запустил основатель «МойОфис» Дмитрий Комиссаров. Партнерами по проекту стали бывший вице-губернатор Санкт-Петербурга Эдуард Батанов, а также основатели и совладельцы производителя электроники F+ tech Алексей Мельников и Владимир Корнев.

Запуск крупными игроками такого числа венчурных фондов может говорить, с одной стороны, об усилении желания крупнейших игроков усилить себя новыми командами и экспертизой, а с другой, если учитывать давление ключевой ставки на рынок, скорой серии громких M&A-сделок. Прим этом в условиях ограниченного доступа к финансированию более мелкие компании могут оказаться в сложном положении и станут искать выход в слиянии с более крупными игроками. Крупные же компании, обладающие финансовыми ресурсами, теоретически могут получить возможность приобретать перспективные стартапы или технологические компании, что позволит им расширить свои продуктовые портфели и укрепить позиции на рынке.

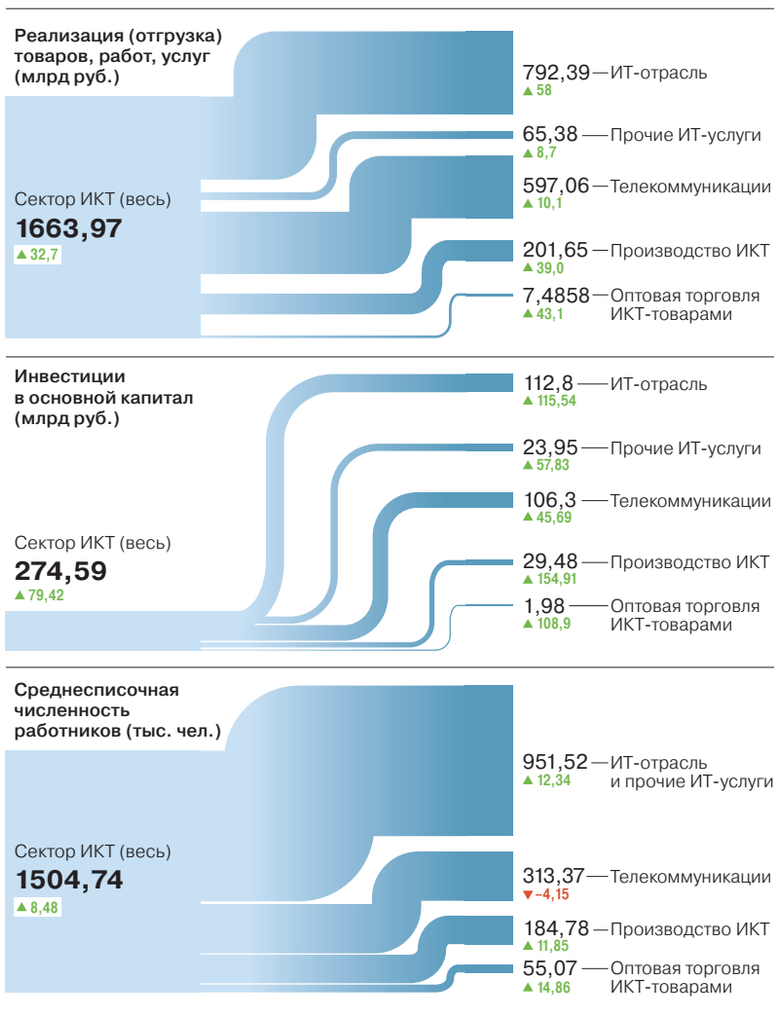
При этом с учетом текущей структуры рынка слияний и поглощений интерес для проведения M&A-сделок будут представлять компании, развивающие решения в области автоматизации предприятий, роботизации, корпоративных мессенджеров и кибербезопасности в B2B, перечисляет первый вице-президент по технологиям МТС Павел Воронин: «Кроме того, важный фактор — рост активности на рынке B2C, где в тренде EdTech, FinTech, а также туризм, медиа и развлечения». Помимо них, топ-менеджер упоминает интерес инвесторов к проектам с искусственным интеллектом: ИИ широко применяется для автоматизации бизнес-процессов, улучшения кибербезопасности, уменьшения затрат, повышения продуктивности, персонализации пользовательского опыта и т. д.

Грядущая консолидация IT-активов на российском рынке с учетом текущих тенденций неизбежна, и вряд ли игроки будут объединяться на добровольной основе, уверен господин Титов. «Консолидаторами могут стать или крупные банки федерального масштаба, или частные холдинги, умеющие работать со стрессовыми активами»,— уточняет он.

С ним отчасти согласен и господин Комиссаров. «Я продолжаю считать, что большинство игроков на рынке операционных систем, офисных пакетов, СУБД, бизнес-приложений обретут стратегических инвесторов. Проводить слияния будут крупные банки, телекоммуникационные компании, такие как МТС и «Ростелеком», а также госкорпорации в разных отраслях, рассуждает Дмитрий Комиссаров.

Александр Мамедов

РОССИЙСКИЙ СЕКТОР ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ПЕРВОМ КВАРТАЛЕ 2024 ГОДА



▲ *Рост год к году (%)* | ИСТОЧНИК: ИНСТИТУТ СТАТИСТИЧЕСКИХ ИССЛЕДОВАНИЙ И ЭКОНОМИКИ ЗНАНИЙ НИУ ВШЭ.

ИГОРЬ ИВАНКО

«Современные корпорации стремятся соблюдать баланс собственных разработок и рыночных решений»

Российские компании, сталкиваясь с потребностью в импортозамещении, прибегают к разным путям развития: от создания решений под собственные задачи до использования рыночных инструментов. Эффективное развитие бизнеса на IT-рынке сегодня требует умения найти золотую середину между своевременным использованием внешних решений и фокусировкой на собственных разработках. О сочетании этих подходов в стратегическом масштабе, о том, какую роль играют большие данные и чем создание универсального продукта отличается от разработки под конкретного заказчика, рассказал „Ъ“ старший вице-президент, руководитель блока «Технологии» Сбербанка **Кирилл Меньшов**.

— мнения —

ПРЕДОСТАВЛЕНО ПРЕСС-СЛУЖБОЙ СБЕРБАНКА

— Два года назад потребители IT-решений переходили на российские «в режиме паники», чтобы обеспечить их немедленную доступность. Что изменилось с тех пор? Что движет заказчиками, которые только сейчас выбирают российские решения?

— Сегодня перед всей страной стоит задача скорейшего перехода на новый технологический стек. И от того, насколько успешно мы ее решим, во многом будет зависеть дальнейшее развитие России. Действительно, некоторые компании только сейчас занялись этим вопросом. Видимо, до последнего надеялись, что западные вендоры вернутся. Конечно, можно законсервировать то, что было доступно несколько лет назад. Можно пытаться обновлять версии через третьих лиц. Но в этом нет стратегии — только тактика и непросчитываемые риски.

Крупные корпорации уже несколько лет наращивают внутреннюю разработку. Так, наши технологические компетенции и самостоятельная разработка всех ключевых банковских систем позволяют «Сберу» уже несколько лет успешно укреплять собственный технологический суверенитет, а также обеспечивать надежность и безопасность продуктов для наших клиентов.

При этом на рынке есть много проверенных российских поставщиков, которые выпускают оборудование, способное дать фору западным аналогам. У нас выстроены отношения с многими российскими поставщиками, вендорами и производителями оборудования. И если мы видим, что решение полностью отвечает нашим потребностям, то внедряем его. За счет такой синергии можно успешно решить поставленную задачу в области импортозамещения.

—С помощью искусственного интеллекта?

— Разумеется. Сегодня главный вызов — не только для «Сбера», но и для всей отрасли — это трансформация создания ПО и обучение команд разработки новым подходам. Нам нужно научиться создавать подавляющее большинство наших решений в полуавтоматическом и даже автоматическом режиме с помощью технологий искусственного интеллекта. При этом есть направления с наибольшим потенциалом ИИ в импортозамещении: генерация и анализ кода для его отладки, автоматизированное тестирование и исправление ошибок, сбор технических требований и проектирование на основе обработки естественного языка и персонализированный пользовательский опыт.

— На днях вы сообщили, что «Сбер» к концу года планирует полностью завершить перевод своих автоматизированных систем в значимых объектах критической информационной инфраструктуры с иностранных СУБД. Какие еще ключевые решения вам удалось полностью заместить и какие планируете?

— «Сбер» уже много лет занимается импортозамещением ландшафта. На конец 2024 года наш IT-ландшафт будет более чем на 80% состоять из целевых импортозамещенных решений, включая собственную облачную платформу Platform V. Кроме того, нами было принято решение отказаться от зарубежной разработки Citrix в пользу отечественного решения, которое обеспечит виртуальные рабочие места для 150 тыс. сотрудников «Сбера». Для импортозамещения ERP-системы на базе SAP мы создаем несколько прикладных платформ по управлению финансами, закупками, недвижимостью и кадрами.

— «Сбер» создавал Platform V сначала под свои задачи, а потом предложил ее продукты рынку. В какой степени это повлияло на архитектуру решений на платформе?

— Platform V подходит для любой индустрии. Платформа уже несколько лет эксплуатируется в самых высоконагруженных условиях и соответствует самым высоким стандартам безопасности, надежности и производительности. В нее входит множество совместимых друг с другом продуктов, которые способны заменить сложные отраслевые решения. Например, платформа процессинга банковских карт собственной разработки уже позволила нам отказаться от отраслевого решения зарубежного вендора.

— Каких принципов стоит придерживаться компаниям, которые решают переориентировать созданное для себя решение для нужд рынка? Или, может быть, есть какие-то типовые ошибки?

— Создание универсального продукта сильно отличается от разработки под конкретного заказчика. В продукте для всего рынка нам нужно собрать пожелания множества потенциальных клиентов, определить необходимый функционал, проверить итог на соответствие универсальным требованиям. Собрать требования с одного заказчика и пройти с ним приемо-сдаточные испытания гораздо проще. К тому же рыночный продукт требует маркетинга и технического сопровождения на годы.

— Большие данные в финансовой сфере сегодня имеют решающее значение для бизнеса. Как использовать их наиболее эффективно и каких результатов можно добиться?

— У любого бизнеса две задачи: увеличить доходы и снизить затраты. Большие данные эффективны и для того, и для другого. Их применяют в финансах, телекоме, ритейле, девелопменте, агропроме и других отраслях. Находясь в основе предиктивных моделей и рекомендательных систем, они помогают банкам привлекать новых клиентов, увеличивать средний чек и число продуктов на одного клиента. Использование больших данных в операционных процессах — управлении очередями, загрузке персонала, логистике — сокращает затраты. А ведь даже 1% экономии на больших масштабах дает миллионы рублей. По прогнозу Ассоциации больших данных, объем рынка больших данных к концу этого года достигнет 380 млрд руб., а дополнительный эффект от их внедрения составит от 1 до 1,6 трлн руб.

— Одна из секций форума FINOPOLIS, в которой вы принимаете участие, посвящена будущему российских технологий. Как отечественные финансовые и другие организации могут сохранить и укрепить свое технологическое лидерство? Есть какой-то рецепт?

— Рецепт не скажу, но отмечу направления, на которых стоит фокусироваться. Это импортозамещение и использование искусственного интеллекта в операционных и бизнес-процессах, развитие собственных технологий, выявление лучших поставщиков на российском IT-рынке, сотрудничество с вузами и исследовательскими центрами, создание привлекательных условий труда и стимулирующих программ для привлечения лучших IT-специалистов, финансирование технологических стартапов, а также формирование гибких и адаптивных команд для решения сложных задач.

Интервью взяла Татьяна Исакова

Поисковики чувствуют себя нейрозно

— развитие нейросетей —

Спрос на применение искусственного интеллекта (ИИ) для обработки информации создал почву для специализированных сервисов, объединяющих нейросетевые технологии с традиционным поиском. При этом таким IT-корпорациям, как компания OpenAI, приходится отдельно договариваться с крупными издателями, чтобы избежать обвинений в плагиате. В России собственный ИИ-поисковик развивает «Яндекс», что отличает его от более консервативного в этой части Google. Однако веб-специалисты не считают, что подобные разработки когда-либо станут основным способом поиска информации.

Помощь в изучении научной литературы и публикаций — одна из наиболее популярных задач, которые разработчики возлагают на генеративный ИИ, следует из опроса McKinsey от февраля—марта 2024 года. О таком сценарии использования нейросетевых сервисов сообщили 6% от общего числа респондентов (об использовании ИИ в разработке в целом сообщили 23%). Этот способ использования больших языковых моделей (LLM) сформировался вопреки присущим им недостаткам и рискам.

Компания OpenAI, представляя ChatGPT в 2022 году, еще тогда предупреждала, что сервис может генерировать «ответы, которые звучат убедительно, но являются некорректными или бессмысленными» (такие случаи еще называют «галлюцинациями»). Гиперссылки, которые генерирует сервис, зачастую оказываются неверными и неработающими — даже в тех случаях, когда владельцы веб-сайтов явно договорились с OpenAI о цитировании, сообщила NiemanLab в июне текущего года. Ключевая же проблема использования LLM для поиска информации заключается в самом их характере: в модели не закладывается информация о тех событиях, которые случились уже после окончания их тренировки. Так называемая «дата отсечки знаний» существенно отстает от настоящего времени даже у самых новых LLM — например, у GPT-4 знания о мире ограничиваются октябрем 2023 года.

Нейросетевые сервисы, способные по ходу каждого запроса обращаться к актуальным данным, в этих условиях позиционируют себя как возможную замену классическим сервисам — как ChatGPT и ему подобным, так и поисковым системам вроде Google. В наибольшей степени на мировом рынке о себе дает знать ИИ-поисковик Perplexity от одноименного стартапа. Свой сервис такого же характера под названием SearchGPT разрабатывает и OpenAI, а в России нейросетевые возможности поиска реализует «Яндекс».

Новички задают тренд

Компания Perplexity была основана в 2022 году. Разработанный ей сервис полагается, с одной стороны, на LLM сторонних компаний (OpenAI, Anthropic, Mistral), с другой — на собственные результаты индексирования сайтов в интернете. Со стороны пользователя Perplexity работает следующим образом: в ответ на запрос, который может быть сформулирован и на естественном языке, он отображает «карусель» из сайтов— источников информации и дает сгенерированный на их основе ответ. Позднее подобный интерфейс в своем нейросетевом сервисе реализовал и «Яндекс».

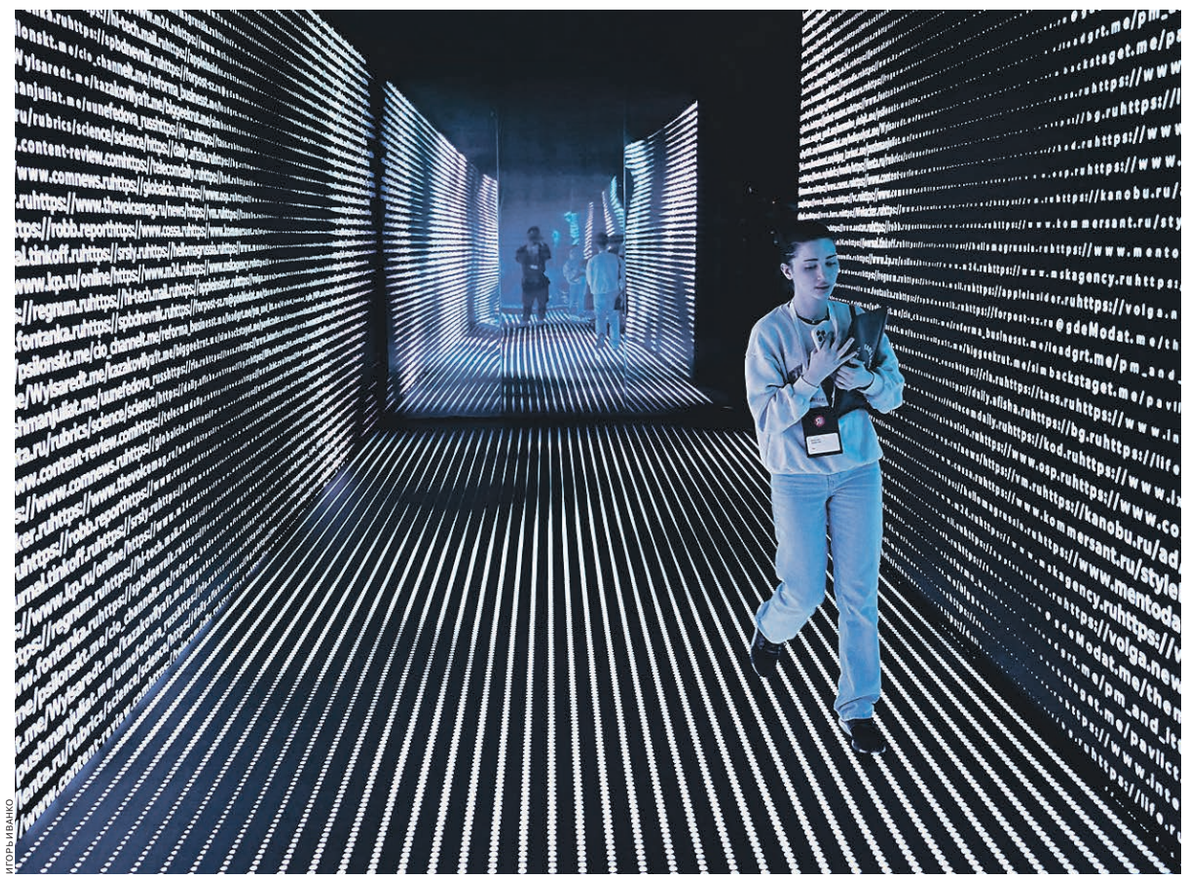
При этом ИИ-сервисам приходится решать проблему, связанную с нежеланием ряда сайтов отдавать свою информацию сторонним компаниям. Модель, по которой работают классические поисковики (свободное индексирование в обмен на поисковый трафик), нельзя полностью перенести на ИИ-сервисы, так как те позволяют пользователям еще и получить пересказ информации с сайта без его посещения. В июне 2024 года американский Forbes сообщил, что Perplexity позволяет получать выжимку из его материалов. После дальнейших обвинений в том, что сервис в принципе игнорирует запретительные директивы в файле robots.txt (описывающие, каким роботам разрешено обходить страницы сайта и какие именно), гендиректор Perplexity Аравинд Шринивас заявил, что их игнорировала не сама компания, а ее подрядчик.

SearchGPT развернут значительно меньшим масштабом, чем Perplexity: OpenAI запустила его в июле на правах прототипа, и воспользоваться им пока может только ограниченное число зарегистрировавшихся пользователей. Его интерфейс в большей степени напоминает стандартное окно чата ChatGPT, при этом пользователи могут отдельно развернуть список цитируемых сайтов. Часть из первых пользователей, по сообщению The Washington Post, считает сервис отстающим как от Perplexity, так и от классического поиска от Google. В числе жалоб, собранных газетой, были некачественная информация из интернет-магазинов, а также случаи «галлюцинаций». При этом пользователи отмечают, что именно в части сгенерированных ответов на вопросы SearchGPT превосходит AI Overview от Google (блоком сгенерированных «быстрых ответов», отображающихся выше стандартных результатов поиска).

И OpenAI, и Perplexity явным образом договорились с крупными издателями об использовании их контента в своих поисковиках: первая — с News Corp, The Atlantic и Conde Nast, вторая — с Time, Der Spiegel и Fortune. Соглашения с Perplexity, как сказал Financial Times ее директор по развитию бизнеса Дмитрий Шевеленко, подразумевают разделение доходов от рекламы. Компания рассчитывает запустить рекламную монетизацию в четвертом квартале, по информации издания, рекламодатели смогут оплачивать показ пары из «спонсорского» вопроса и одобренного ответа на него. Как будет монетизироваться SearchGPT, пока не ясно, при этом в OpenAI сказали The Washington Post, что «бизнес-модель компании основывается на платных подписках».

Первые шаги за нейросетью

К настоящему моменту Google ограничивает свои эксперименты в области скрещивания ИИ и традиционного поиска именно блоком AI Overview. Он заменяет стандартные «быстрые ответы» только в некоторых странах (США, Великобритания, Япония и еще три; России среди них нет) и лишь по части запросов — 7% от общего числа показов, следует из июньского анализа компании BrightEdge.



ИГОРЬ ИВАНКО

В России «Яндекс» добавил нейросетевой вариант составления «быстрых ответов» в сентябре 2023 года, а спустя семь месяцев представил отдельный от классического поиска сервис «Нейро». По состоянию на август с момента запуска сервисом воспользовались около 9,5 млн человек, сообщили „Ъ“ в «Яндексе». Для сравнения: аудитория стандартного поиска — около 100 млн человек в месяц, при этом 3 октября компания встроила в него функции «Нейро». В компании отметили, что к тому моменту сервис был доступен лишь частично, и называли показатели хорошими: «Почти половина из тех, кто воспользовался сервисом, остаются в нем — для нового продукта это очень хороший показатель». В компании уточнили, что 30% запросов к «Нейро» относятся к науке и образованию, а 25% — это «информационные сценарии».

Оценить, какой объем трафика на сайты приходит именно из «Яндекс Нейро», не представляется возможным, говорит руководитель направления поисковой оптимизации ФГ «Финам» Владимир Харев. Это связано с тем, что при переходе по ссылкам из «Нейро» сайтам передается тот же самый параметр, что и у традиционного поиска: «Поэтому такие визиты атрибутируются системами веб-аналитики как переход из органического поиска». В «Яндексе» заявили „Ъ“, что не видят снижения трафика на внешние сайты, а общее количество поисковых запросов во втором квартале 2024 года выросло на 8% год у году: «В том числе, мы уверены, это связано с «Нейро»».

Но будущее поисковиков не за «еще одним сервисом, открывающимся в новой вкладке браузера», считает директор по продукту Just AI Глеб Обломский: «Поиск информации обычно является предпосылкой к какому-то действию. Реальная замена текущим системам — это по-настоящему интеллектуальные ассистенты, которые будут решать задачу, а не искать данные для ее решения». Другой вариант сосуществования поисковиков и LLM — узкодоменные ИИ-помощники: «По сути, ассистенты на основе баз знаний из конкретной области. Например, по массиву корпоративных, юридических, медицинских данных». Говоря же о поиске общего характера, господин Обломский отмечает, что «никто не поменяет привычный и проверенный Google на что-то генеративное только потому, что ответ в нем дает модная LLM».

Говоря о специализированных ИИ-продуктах, стоит отметить, что топ-менеджеры «Яндекса» еще в прошлом году предвосхищали появление специализированных нейросетей для юридических или медицинских целей (см. „Ъ“ от 8 сентября 2023 года). Спустя год компания подтверждала, что работает в области «создания и применения нейросетей в медицине» (см. „Ъ“ от 17 сентября), но не раскрывала характер разработок.

Упрощение поиска идет всем на пользу, но в своем текущем виде ИИ-поисковики пока что не являются массовым продуктом, говорит медиатехнолог Иван Макаров: «Студенты, профессиональные медийщики использует такие возможности в гораздо большем объеме, чем остальные. Массовый же потребитель даже текущими пользуется на очень базовом уровне». По его мнению, ситуация может измениться только тогда, когда разработчики уровня OpenAI представят совершенно новый интерфейс, посредством которого можно искать информацию.

Юрий Литвиненко

Ключевой элемент инфраструктуры

Осенью стартует не только новый деловой сезон, но и интенсивный период в IT-отрасли, когда компании уже начинают планировать будущий год и оценивают, что актуально на рынке. Например, вопрос импортозамещения не перестает быть злободневным, тем более что с 2025 года госорганы, госкомпании и предприятия, у которых есть объекты критической информационной инфраструктуры (КИИ), должны начать работать только на российских решениях. К тому же значение киберугроз для бизнеса и потенциальный ущерб от последствий действий злоумышленников растут ежедневно. Чтобы объединить отрасль для ответа на внешние вызовы, была придумана конференция IT Elements, которая второй год подряд становится не только местом для обмена опытом и общения экспертов, но и площадкой для практической демонстрации возможностей решений российских вендоров.

— события —

Эта осень насыщена в части IT-мероприятий, что в том числе говорит об оживленности рынка, его потребности в обмене опытом и информацией. Одним из заметных событий стала практическая конференция IT Elements, генеральным партнером которой выступила «Инфосистемы Джет». Конференция собрала более 2,5 тыс. представителей IT-блоков крупнейших компаний и более 6 тыс. зрителей онлайн-трансляций. Только в первый день мероприятия в нем приняли участие эксперты из таких крупных компаний, как «Почта-банк», «Вкусно — и точка», «Газпромнефть-Гео», VK, «Сбертех», «РСХБ-Интех» и других.

Как объяснили „Ъ“ формат мероприятия сами организаторы, «у компаний—потребителей IT-решений и вендоров сформировался запрос на личное общение, знакомство и поиск новых контактов на рынке». Поэтому, с одной стороны, IT Elements стала местом для обмена экспертизой, с другой — отраслевой выставкой, где потенциальные заказчики продуктов могут не только познакомиться с их разработчиками, но и опробовать продукты прямо на площадке, рассказывают в «Инфосистемы Джет». При этом, отмечают в компании, на рынке сказывается уход крупных зарубежных организаторов IT-мероприятий, поэтому компания видит своей миссией объединять IT-комьюнити, что и делает уже второй год подряд.

Организаторы выбрали три главных трека для сессий, дискуссий и воркшопов: ими стали инфраструктура, сети и информационная безопасность — ключевые технологические направления, которые сегодня важны для IT в российском бизнесе.

Инфраструктурный трек был сконцентрирован на интеграции с разработкой, что включает в себя новые подходы к созданию современной IT-инфраструктуры: облачные модели построения IT, платформы для разработчиков, оркестрацию контейнеров и DevSecOps. Также эксперты поговорили про развитие отечественных решений и технологий для enterprise-компаний, бизнес которых подразумевает большие нагрузки, высокие требования к надежности, отказоустойчивости и уровню сервиса.

В сетевом треке эксперты и участники рынка обсудили развитие центров обработки данных (ЦОД) в России. Затронули и тему сетевого оборудования для ЦОДов. Состояние российского рынка позволяет, помимо отечественного сетевого оборудования, рассматривать и другие доступные решения — например, эксперты обсудили использование на сетевом оборудовании программного обеспечения с открытым кодом, оценили плюсы такого подхода и преимущества интеграции подобных решений в централизованные системы управления и мониторинга. Самим же системам управления и мониторинга тоже была посвящена отдельная сессия.

ПРЕДОСТАВЛЕНО «ИНФОСИСТЕМЫ ДЖЕТ»

Внимание инженеров на конференции привлек доклад Павла Михайлика, старшего консультанта по сетевому аудиту «Инфосистемы Джет», о проблематике балансирования нагрузки в высоконагруженных фабриках на сетевом уровне, об особенностях выбора и сочетания алгоритмов. Сейчас на российском рынке наблюдается определенный дефицит проверенных решений по сетевой балансировке трафика, доступные на данный момент решения обычно имеют ряд проблем с поддерживаемым функционалом или производительностью. В сегменте оборудования для построения полноценных EVPN-VXLAN-фабрик ЦОДов шоковое состояние уже миновало, однако имеющиеся в наличии продукты от отечественных брендов все еще имеют ряд существенных проблем как с поддержкой требуемого набора функций в принципе, так и с надежностью их работы в каждом отдельном случае.

В ходе дискуссии интеграторов эксперты отметили, что количество отечественных производителей быстро растет, что не может не радовать. Вместе с этим зрелость решений еще далека от известных мировых вендоров. И если раньше можно было выбрать проверенный продукт, взять работы по внедрению от производителя или даже сделать это самостоятельно и получить готовое решение, то сейчас все совсем не так. Не все производители готовы не только выполнять работы по проектированию и внедрению, но и оказывать сервис на необходимых заказчику условиях. К тому же у каждого производителя свои тонкости и нюансы, особенно в части небазового функционала. Сами заказчики тоже не всегда готовы брать на себя ответственность за внедрение отечественных решений. Поэтому при переходе на российские решения так важна роль интеграторов, которые изучают все продукты на рынке, проводят тестирование, проверяют, что работает, а что — нет, и разбираются, как правильно настраивать отечественное оборудование в каждом конкретном случае. Участие интеграторов в проектах уменьшает сроки их реализации и обеспечивает выполнение бизнес-задач заказчиков.

Помимо этого, эксперты обсудили развитие направления корпоративных коммуникаций в компаниях, пригласив на сцену отечественных производителей UC.

Создать безотказно работающую инфраструктуру невозможно без полноценных систем защиты, и в рамках блока, посвященного безопасности, эксперты сконцентрировались на вопросах отечественных ИБ-решений, работе с системами мониторинга угроз и многоступенчатой защиты периметра.

«IT Elements представляет актуальные кейсы и последние тенденции рынка, это позволяет своевременно реагировать и внедрять лучшие решения для наших задач»,— поделился специалист по мониторингу информационных систем «Вкусно — и точка» Станислав Моргаев. Обмен опытом сопровождается спорами, а в спорах рождается истина, напоминает он. «Мне же хотелось поделиться опытом внедрения системы мониторинга, которую мы строили с нуля в условиях ухода международных игроков с рынка»,— рассказал Станислав Моргаев.

Мастер-класс по импортозамещению

На площадке IT Elements не только была организована выставка, но и проходили мастер-классы и тестирование новых технологий в режиме реального времени. Так, в лабораторном зале была собрана VXLAN-EVPN-фабрика из продуктов российских вендоров. «Участники конференции могут подключиться к любому коммутатору, посмотреть настройки и различные выводы команд и при желании произвести донастройку функций»,— рассказывают организаторы. В продуктовой зоне эксперты из МКБ и «Лаборатории Числитель» показали, как собрать enterprise-облако, предоставляющее PaaS-сервисы, всего за 60 минут.

Специалисты «Инфосистемы Джет» в партнерстве с компанией «Аэродиск» продемонстрировали возможности первого метрокластера, собранного полностью на базе отечественных решений. Метрокластер обеспечивает синхронную репликацию данных на уровне систем хранения и практически бесшовное переключение сервиса в случае аварии. Директор центра инфраструктурных решений «Инфосистемы Джет» Юрий Семенюков рассказывает „Ъ“, что спрос российских компаний на решения такого класса постоянно растет. «К конфигурации метрокластера привыкли все крупные компании во времена использования западных решений. Технология обеспечивает высокую степень защиты данных, при этом практически не требует ручного вмешательства в случае переключения»,— говорит он. Для российских производителей реализация метрокластера стала настоящим вызовом, считает Юрий Семенюков.

Представленный метрокластер включает в себя только зарегистрированные в реестрах Минпромторга и Минцифры оборудование и ПО. Эксперт «Инфосистемы Джет» акцентировал внимание на том, что компании, особенно относящиеся к КИИ, уже могут интегрировать метрокластер в свою работу и тестировать в условиях высоких нагрузок. «Технология выполняет базовый функционал и справляется со сценариями отказов в тестовом режиме. Компаниям, которые рассматривают такие решения, необходимо провести полноценные тестирования в своем IT-окружении и при реальных нагрузках. Мы готовы им с этим помочь»,— подытожил он.

Практическая часть конференции подкреплялась обменом мнениями на дискуссиях. На одной из сессий, посвященных инфраструктуре, производству, реализации и эксплуатации ЦОДов, представители крупного бизнеса обсудили выбор оборудования, различия между капитальным строительством центров и модульными решениями, а также подняли вопрос инвестиций в строительство и их окупаемость.

При проектировании новых систем и решений важно опираться не только на технические описания и документацию, но и на реальный опыт тех, кто уже прошел путь внедрения и сформировал пользовательский опыт, считает руководитель направления по цифровому развитию «Газпромнефть-Гео» Виктор Попов. Поэтому чрезвычайно важно делиться друг с другом информацией и опытом для достижения наилучших результатов бизнеса и развития технического прогресса в нашей стране. «IT Elements для этого идеально подходит».

Планирование с безопасностью

Темы защиты данных, безопасного их хранения и построения изначально устойчивой инфраструктуры поднимались практически в каждом докладе или дискуссии. Опыт последних двух лет показал, что одного решения для защиты компании недостаточно, а также, что стратегия защиты IT-инфраструктуры должна постоянно трансформироваться в зависимости от внешних факторов.

В рамках сессии «Сетевая безопасность-2024» представители как заказчиков ИБ-продуктов, так и вендоров обсудили процесс планомерного отключения компаний от иностранных решений, помощь заказчикам в миграции на российские продукты и, в частности, развитие отечественных NGFW. Кроме того, NGFW был отведен отдельный стенд, на котором участники IT Elements сравнили российские решения и провели нагрузочные тестирования.

«Такие мероприятия, как IT Elements, помогают получить концентрированную актуальную информацию из первых уст о современных тенденциях и приобретенном опыте наших коллег в IT-отрасли»,— поделился Виктор Попов. В условиях недостатка времени и информационной инфляции такой формат нельзя недооценивать, заключает он.

Валерия Романова

Реклама уходит с поста

— законодательные изменения —

Вслед за запретом рекламироваться у иностранных агентов аналогичный запрет может распространиться на заблокированные в России площадки, в том числе Instagram (принадлежит экстремистской и запрещенной в РФ Meta). Соответствующий законопроект летом уже был принят Госдумой в первом чтении. Хотя сейчас в соцсети уже невозможно купить контекстную рекламу, у российских рекламодателей оставалась возможность покупать интеграции у блогеров, отмечают участники рынка. По оценке Роскомнадзора, бизнес ежегодно инвестировал в такую рекламу около 900 млн руб. „Ъ“ разбирался, как новый законопроект может повлиять на рынок.

Суть законопроекта

В первом чтении 25 июля Госдумой были приняты поправки к федеральным законам «О рекламе» и «О противодействии экстремистской деятельности». Документ предполагает запрет на размещение рекламы на ресурсах, деятельность которых признана нежелательной. Законопроект также отдельно устанавливает запрет размещать рекламу на ресурсах, принадлежащих экстремистским организациям. В пояснительной записке упоминаются Facebook и Instagram (деятельность Meta по управлению этими сетями объявлена в РФ экстремистской и запрещена). Законопроект может вступить в силу только через полгода после подписания закона в случае его принятия: такие поправки ко второму чтению предложила ранее Ассоциация блогеров и агентств. Один из авторов проекта, замглавы комитета Госдумы по информполитике Антон Горелкин, заявлял, что согласен с предложением.

Новые ограничения, как утверждается в пояснительной записке, являются «последовательным правовым шагом», следующим за ранее введенным запретом размещать рекламу у иноагентов. Там также говорится, что цель проекта — лишить запрещенные в РФ организации доходов от рекламы в России. «У Facebook и Instagram (принадлежат корпорации Meta, которая признана экстремистской и запрещена в РФ) и сейчас большая аудитория в России. Многие продолжают пользоваться этими ресурсами, обходя блокировки через VPN. И это позволяет той же компании Meta (признана экстремистской организацией и запрещена в РФ) зарабатывать на рекламном российском рынке. Немалый доход пускается на создание и распространение экстремистского контента, а также поддержание интереса к этим площадкам»,— пояснял глава комитета Госдумы по информационной политике Александр Хинштейн.

О какой рекламе идет речь

Сейчас рекламный кабинет, позволявший размещать рекламу в иностранных соцсетях (в том числе контекстную), отключен, но остается способ рекламироваться на площадках через рекламные интеграции у блогеров — договариваться с ними напрямую или через сторонние агентства и биржи. Легально покупать такие интеграции в Instagram станет невозможно, если законопроект будет принят в текущем виде. Речь идет о рынке объемом около 900 млн руб.— такую сумму за 2023 год российские рекламодатели потратили на продвижение своих товаров и услуг в Instagram (принадлежит корпорации Meta, запрещена в РФ как экстремистская), сообщали «Ведомости» со ссылкой на Единый реестр интернет-рекламы, оператором которого выступает Роскомнадзор.

После блокировки Instagram (принадлежит корпорации Meta, запрещенной в РФ как экстремистская) в 2022 году значительная часть рекламы оставалась на платформе, несмотря на ограничения, говорит директор по развитию бизнеса Kokoc Like (Kokoc Group) Сабина Исаева: «По моим оценкам, это не менее 50–60% от объема рекламных инвестиций. Важно отметить, что большинство размещений не маркировались и чаще подавались в формате рекомендаций или информирования, что затрудняет точную оценку объемов. Именно такая ненавязчивая реклама и стала доминирующей после блокировки сети».

Соцсеть оставалась актуальной площадкой для множества российских компаний, начиная с крупных FMCG-брендов и сервисов крупных экосистем и заканчивая небольшими бизнесами, представленными по большей части селлерами на маркетплейсах, добавила Сабина Исаева: «Практически все категории бизнеса так или иначе были представлены на этой платформе». Пока запрет не вступил в силу, ближайшие интеграции, по ее словам, не отменяются: продолжать размещение у блогеров еще можно, а отмена текущих интеграций привела бы к упущенным возможностям для брендов. «Однако стоит отметить, что новые рекламные кампании уже не планируются в прежних объемах»,— добавила госпожа Исаева.

Сторонники и противники инициативы

Некоторые участники рынка выступали против законопроекта. «Поправки приведут к росту цен на рекламные интеграции, а также «поспособствуют тому, что недавно обелившейся рынок может уйти в серую зону»,— заявляли „Ъ“ в Ассоциации блогеров и агентств. Что касается блогеров в запрещенной соцсети, то они «потеряют свой ключевой актив — рекламные контракты». В ассоциации добавляли, что владелец соцсети не зарабатывает на интеграциях у блогеров, в то время как российский бюджет «получает с них налоговые отчисления в размере около 1 млрд руб.».

Несмотря на некоторое сопротивление рынка, опрошенные „Ъ“ эксперты прогнозируют, что законопроект не встретит серьезных препятствий на последующих этапах. Принятие законопроекта в первом чтении не означает, что в итоге он будет принят в текущей редакции, рассуждает собеседник „Ъ“ на рекламном рынке: «Однако вероятность принятия проекта высока. Крупные рекламодатели уже живут в реальности, где этот закон будет принят, и начинают продумывать альтернативные возможности для поддержания знания о бренде». До блокировки Instagram (принадлежит корпорации Meta, которая запрещена в РФ как экстремистская) около 40% бюджета на инфлюенс-маркетинг в социальных медиа распределялось в пользу этой площадки, продолжает собеседник „Ъ“. «После блокировки инвестиции упали в два раза, сейчас бюджет составляет около 20%. Возможно, некоторые рекламодатели уйдут в сегмент наружной рекламы, на ТВ, но в первую очередь они, конечно, обратят внимание на российские площадки»,— говорит он.

Вероятность полного запрета рекламы в Instagram (принадлежит корпорации Meta, запрещена в РФ как экстремистская) крайне высока, также считает операционный директор Okkam Creative Аполлинария Двуреченская. Блогерам, для которых это основной источник рекламного дохода, стоит осваивать новые платформы, если они планируют ориентироваться на аудиторию в РФ, или же разрабатывать стратегию по привлечению подписчиков из других стран, которые будут интересны зарубежным рекламодателям. Инвестиции рекламодателей, которые до этого еще «шли» на запрещенную соцсеть, могут уйти в Telegram, VK, YouTube, Nuum и другие платформы, добавила Аполлинария Двуреченская.

Сабина Исаева считает, что законопроект, скорее всего, будет принят в нынешнем виде: «Несмотря на бурную реакцию рынка, я не вижу реальных сценариев, при которых от него откажутся». После его вступления в силу рекламные инвестиции в запрещенных сетях сократятся значительно, прогнозирует она: «На первых порах 80–90% рекламных бюджетов будет перенаправлено или заморожено. Ответственность за нарушение велика как для рекламодателей, так и для распространителей, и большинство участников рынка не пойдет на риски».

Что грозит за нарушение

Если законопроект будет принят, российские компании и блогеры не смогут рассматривать запрещенные ресурсы как легитимную площадку для размещения рекламы, резюмирует главный редактор журнала «Арбитражная практика для юристов» Андрей Набережный. По его словам, реклама на таких ресурсах будет запрещена в любом виде и формате (посты, сторис и т. д.).

За нарушение запрета в первую очередь может грозить административная ответственность, говорит Андрей Набережный. Есть базовые положения статьи 14.3 Кодекса РФ об административных правонарушениях, которая предусматривает штрафы за нарушение законодательства о рекламе рекламодателями, рекламопроизводителями и рекламораспространителями. Размер штрафов для граждан составляет от 2 тыс. до 2,5 тыс. руб., для должностных лиц — от 4 тыс. до 20 тыс. руб., для юрлиц — от 100 тыс. до 500 тыс. руб., говорит Андрей Набережный. Юрист также не исключает возможность уголовного наказания за финансирование экстремистской деятельности (ст. 282.3 УК РФ) или деятельности нежелательной организации (ст. 284.1 УК РФ). «Уголовная ответственность возможна только в отношении граждан»,— добавил Андрей Набережный.

Что делать, пока проект не вступил в силу

Андрей Набережный советует блогерам проанализировать свои рекламные контракты на предмет возможности их расторжения в связи с введением ограничений. «Очень важно выбрать способ расторжения, который позволит не понести дополнительные финансовые потери. В случае введения ограничений продолжение оказания рекламных услуг даже по заключенному ранее контракту будет являться незаконным. Нужно согласовать с рекламодателями условия расторжения договора либо его изменений»,— добавил Андрей Набережный.

Принятие итоговой версии законопроекта возможно быстро, поэтому уже сейчас важно внести необходимые корректировки в договоры и согласовать финансовые условия, говорит господин Набережный: «Например, в договоре можно прописать сохранение условий и переход на другую площадку». Формально сейчас нет запрета на рекламу, поэтому условия соглашения могут предусматривать неустойку в случае одностороннего расторжения, отметил эксперт. Также рекламодателям важно уже сейчас проработать альтернативные рекламные интеграции, чтобы не потерять аудиторию и не получить штраф, если компании не успели снять рекламу и изменить условия договора»,— добавил Андрей Набережный.

Валерия Лебедева

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