Участники IT-рынка обсудили применение нейросетей в кибербезопасности | 14

ИТ

Тематические страницы газеты **Коммерсантъ**

Информационные технологии

Среда 18 октября 2023 №194 (7639 с момента возобновления издания) **kommersant.ru**

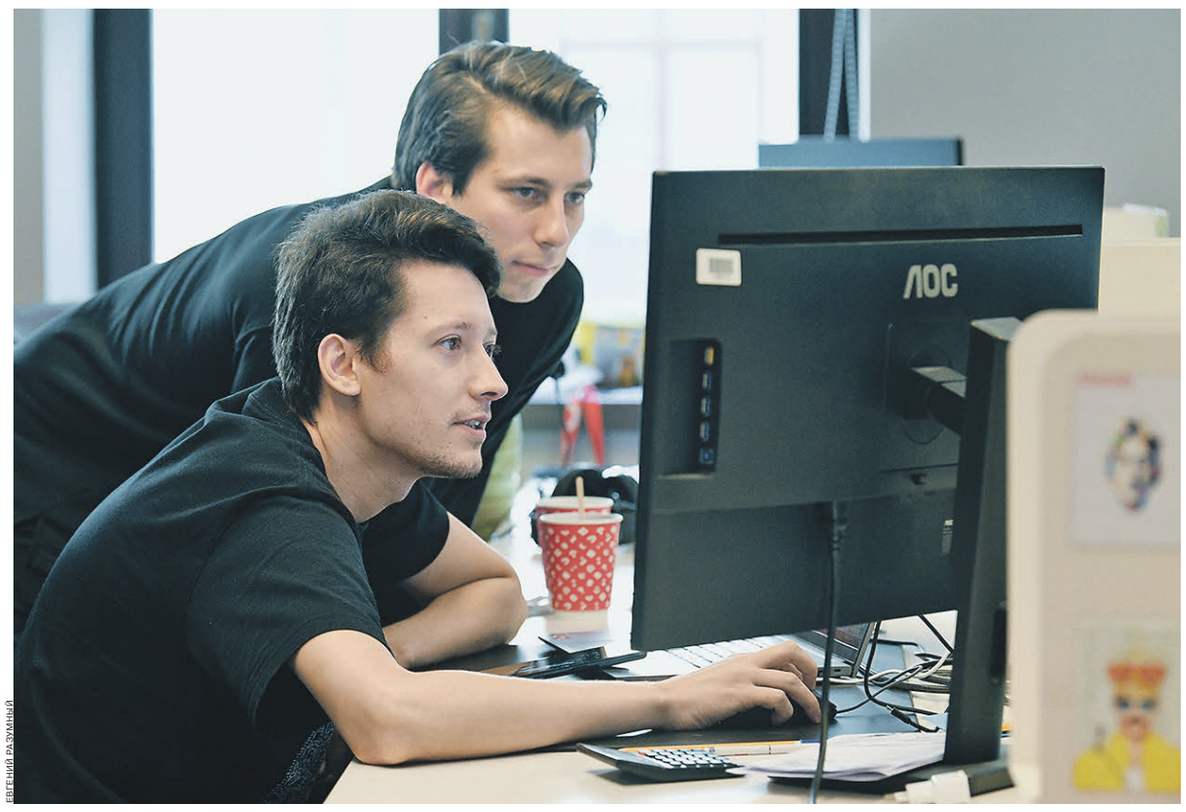
15 | Чем конкуренты Twitter пытаются отличаться от продуктов корпораций

16 | Как в России развивался рынок манги

16 | У бизнеса растет спрос на киберстрахование

Окна оставляют приоткрытыми

В августе стало известно, что американская Microsoft перестанет продлевать подписки корпоративным клиентам в России с конца сентября. В официальных комментариях крупные интеграторы и дистрибуторы говорят, что коробочные версии ОС, которые были закуплены еще до начала военной операции, с одной стороны, подходят к концу, а с другой — пользуются небольшим спросом: их продажи по итогам первого полугодия упали на 78% год к году. Тенденцию связывают с отсутствием техподдержки и переходом компаний на российский софт. Но источники „Ъ“ на IT-рынке говорят, что переход на отечественные ОС и в корпоративном, и в государственном сегментах идет медленно, аналогичная ситуация и в B2C.



ЕВГЕНИЙ РАЗУМНЫЙ

— импортозамещение —

Быстрый рост

Крупнейшие разработчики российских операционных систем по итогам первого санкционного 2022 года отчитывались о рекордных выручках. Так, согласно данным «СПАРК-Интерфакса» и официальным заявлениям компаний, по итогам прошлого года выручка «Русбитех-Астра» (ОС Astra Linux) выросла в 2,5 раза год к году и составила 5,39 млрд руб., чистая прибыль — 3 млрд руб., что в 2,8 раза больше год к году. Выручка «Базальт СПО» (ОС «Альт») по 2022 году составила 893 млн руб. (+173% год к году), чистая прибыль — 492 млн руб. (+418% год к году). В свою очередь, выручка «Ред Софт» (ОС «Ред») — выросла на 122%, до 1,3 млрд руб., чистая прибыль — на 95%, до 160 млн руб.

Положительные результаты показали и разработчики офисных пакетов: чистая прибыль ООО «Новые облачные технологии» («МойОфис») составила 3,3 млрд руб. (+295,6% год к году). По данным kartoteka.ru, выручка «Алми Партнер» (AlterOffice, AlterOS) выросла на 165,1% год к году, до 940,3 млн руб.

Такие показатели представители компаний и отраслевые эксперты ожидаемо связывали с ажиотажным спросом на российский софт, который, с одной стороны, подстегивался публичными заявлениями зарубежных компаний об отказе работы с российскими контрагентами, а с другой — постепенно ужесточающимися требованиями правительства в части замещения зарубежного программного обеспечения. Это в том числе программы цифровой трансформации ведомств и госкомпаний, которые предполагают постепенное увеличение доли российского софта на инфраструктуре.

Одно из самых жестких требований власти ввели в марте 2022 года. Тогда президент РФ Владимир Путин подписал указ №166, который предполагает, что субъекты критической информационной инфраструктуры (КИИ; банки, телекомкомпании, ТЭК и др.) должны с 31 марта 2022 года прекратить закупки зарубежного ПО, а с 2023-го — остановить его использование на своей инфраструктуре. Впрочем, реалистичность исполнения этих требований в срок до сих пор вызывает разногласия у регуляторов и бизнеса. Представители топливно-энергетического и финансового комплексов, ссылаясь на трудности замещения системного ПО, просят сдвинуть сроки.

Совокупность этих двух факторов — протекционистских мер правительства и отказа зарубежных вендоров, а также еще досанкционный тренд на увеличение инвестиций государственных и частных предприятий в цифровизацию — позволяет аналитикам прогнозировать продолжение роста выручки российских софтверных предприятий за счет спроса госзаказчиков.

Так, Strategy Partners в своем сентябрьском прогнозе предполагает, что до 2030 года среднегодовой темп роста (CAGR) российского IT-рынка будет составлять 12%. Еще одним фактором его роста в течение ближайших лет может стать замещение частными компаниями, не попадающими под действие большинства протекционистских мер, зарубежных операционных систем и офисных пакетов, в первую очередь от Microsoft, доля которых на инфраструктуре российских компаний все еще велика.

С широко раскрытыми окнами

Судя по официальным заявлениям российских IT-интеграторов и дистрибуторов, среди которых Softline, «Крок» и «Марвел», по итогам первого полугодия продажи цифровых копий Windows в России упали почти на 80%, а складские запасы этого софта, которые были закуплены еще до начала санкций, подходят к концу. Но источники „Ъ“ на IT-рынке говорят, что на деле российские корпоративные потребители продолжают закупки лицензий на ПО от Microsoft через посредников в СНГ. Оценить объемы «обходных» закупок представители IT-компаний и эксперты не берутся, но говорят, что доля софта от Microsoft на инфраструктуре частных российских компаний сейчас доминирует: его доля достигает 80–90%.

Так, архитектор IT-инфраструктуры практики «Стратегия трансформации» «Рексофт Консалтинга» Александр Черный, ссылаясь на исследование J'son & Partners Consulting от 2020 года, говорит, что объем рынка российского офисного ПО оценивался тогда в 38,8 млрд руб., из которых лишь 7% приходилось на российский софт: «На продукты импортного ПО — Microsoft Office, Hancom Office, WPS Office — приходилось 77,5% рынка, на свободное ПО — 15,5%. Вряд ли что-то драматически изменилось на момент объявления Microsoft об уходе».

С этим отчасти соглашается и гендиректор «МойОфис» Павел Калякин: по его словам, в зависимости от сегмента экономики доля клиентов, которые продолжают пользоваться продуктами Microsoft, составляет от 70% до 90%: «„МойОфис“ и другие российские разработчики офисного ПО в совокупности занимают 16% рынка». В компании ITentika, ссылаясь на собственные оценки, говорят, что число клиентского софта Microsoft на инфраструктуре заказчиков сохраняется на уровне 80%. «Если говорить про серверные ОС и виртуализацию, их можно оценить в 35–40%»,— говорит директор московского представительства ITentika Сергей Кузнецов.

В корпоративном сегменте основные пользователи иностранного софта сейчас — заказчики, которые не обязаны законодательно переходить на российское ПО, как госсектор и субъекты критической информационной инфраструктуры, у них есть привычные и оплаченные зарубежные IT-решения, и многие из них все еще надеются переждать санкции, говорит соучредитель Vinteo Дмитрий Серый.

Опрошенные „Ъ“ участники рынка и эксперты считают, что приверженность российских корпоративных и даже государственных потребителей ПО от Microsoft связана с рядом мер, которые корпорация предпринимала для стимулирования внедрения своих продуктов в школах и вузах, которые получали пакеты ПО с большими скидками или вовсе бесплатно. «Например, Teams активно используют образовательные учреждения для дистанционной работы с учениками, студентами, абитуриентами и преподавательским составом. Соответственно, переход на российский аналог, даже если он куда более функциональный, потребует привыкания к новому интерфейсу и обучения работы с решением»,— объясняет Дмитрий Серый.

Помимо этого существуют и другие причины преобладания Microsoft на инфраструктуре заказчиков, в частности высокая совместимость этого ПО с прикладным программным обеспечением, а также тот факт, что сотрудники организаций различных секторов обучались работать именно с этим софтом.

Выход из зоны комфорта

Переход российских корпоративных пользователей на российское ПО сдерживается не нехваткой мер по его стимулированию со стороны государства, а тем, что потребители за годы использования ПО от Microsoft адаптировали собственную инфраструктуру именно под него, переход же на другие решения потребует времени и инвестиций, рассуждают в Vinteo. Когда компания долго работает на каком-либо продукте, она накапливает экспертизу работы с ним. Переход на новое решение требует от сотрудников новых компетенций. В этом случае у персонала возникает сопротивление инновациям, соглашается глава департамента цифровых решений «Полилога» Людмила Богатырева: «Сейчас российским вендорам необходимо завоевывать доверие заказчиков».

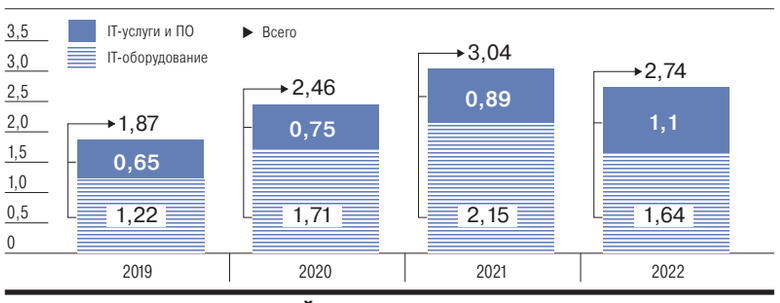
Еще один фактор, который замедляет внедрение российских решений на корпоративной инфраструктуре и у частных заказчиков,— это пиратство софта, популярность которого в России резко подскочила на фоне санкций. В ноябре 2022 года Peer Trace (дистрибутор данных о загрузках контента) подсчитал количество уникальных IP-адресов из РФ, с которых посредством торрентов скачиваются или раздаются пиратские копии Windows и Microsoft Office. Сервис тогда выявил 174 тыс. фактов загрузки и раздачи только в течение 1 ноября. Это на 24,4 тыс. больше, чем в тот же день в 2021-м.

Российские разработчики ОС и офисных пакетов уже предпринимают действия, в результате которых доверие к российскому софту корпоративных и частных потребителей должно вырасти, говорит Александр Черный: «Это наращивание присутствия таких продуктов в потребительском сегменте через торговые сети, выпуск бесплатных версий ПО для домашнего использования и мобильных устройств, ценовую политику, при которой офисные пакеты предлагаются по ценам ниже стоимости продуктов Microsoft, заключение партнерств с вузами».

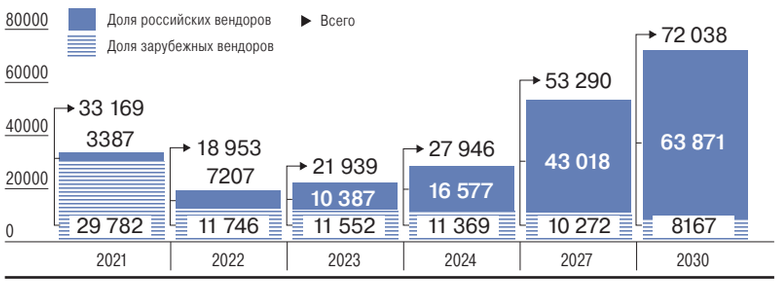
Хотя доля внедрений российских офисных пакетов и операционных систем на корпоративной инфраструктуре, несмотря на недоверие потребителей, а также необходимость доработки решений, будет расти, аналогичного тренда в потребительском сегменте ждать не стоит, считает технический директор CodeInside Владислав Егоров: «Обычные пользователи не готовы платить фактически за дистрибутивы Linux, которые при необходимости можно бесплатно и легально скачать в интернете».

Александр Мамедов

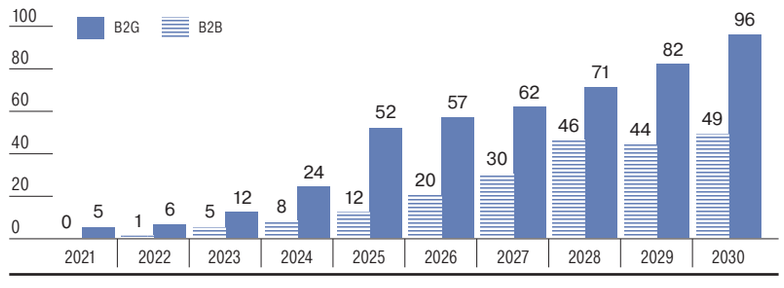
ТЕМПЫ РОСТА РОССИЙСКОГО IT-РЫНКА (ТРЛН РУБ.) ИСТОЧНИК: STRATEGY PARTNERS.



ДИНАМИКА ОБЪЕМА РОССИЙСКОГО РЫНКА ОС ДЛЯ ПК И СЕРВЕРОВ (МЛН РУБ., С ПРОГНОЗОМ) ИСТОЧНИК: STRATEGY PARTNERS.



АНАЛИЗ УРОВНЯ ПРОНИКНОВЕНИЯ РОССИЙСКИХ ОС ДЛЯ ПК И СЕРВЕРОВ ДЛЯ ОСНОВНЫХ СЕГМЕНТОВ ЗАКАЗЧИКОВ В РОССИИ (%, С ПРОГНОЗОМ) ИСТОЧНИК: STRATEGY PARTNERS.



IT-компании рискуют перестраховаться

— регулирование —

В правительстве и IT-отрасли активно обсуждается введение в России механизма обязательного страхования компаний от кибератак, число которых продолжает расти. Летом данную инициативу выдвинул Совфед, в контексте введения оборотных штрафов за утечки персональных данных о ней говорило и Минцифры. Однако пока четких критериев оценки ущерба для компенсации нет, а ЦБ, регулирующий рынок страхования, считает, что для создания единых требований к такой услуге должен быть наработан достаточный опыт в этой сфере.

Публично обсуждать инициативу о создании механизма страхования компаний от кибератак в правительстве начали летом. Член комитета СФ по конституционному законодательству и государственному строительству Артем Шейкин 30 июня сообщил СМИ, что создание рынка страхования от киберугроз в России — «важная инициатива, которая может существенно улучшить кибербезопасность в стране». «Подобно тому как ОСАГО обеспечивает финансовую защиту автомобилистов в случае ДТП, страхование от киберугроз будет обеспечивать защиту компаний в случае кибератак и утечек данных»,— говорил господин Шейкин «РИА Новости». Подробно разрабатывать механизм киберстрахования в парламенте планировали начать осенью нынешнего года.

Как рассказал „Ъ“ Артем Шейкин, на данный момент сенаторы получают обратную связь по вопросу создания обязательного киберстрахования рисков и угроз (сокращенно — ОКРУГ) от профильных министерств, экспертного сообщества, формируя концепцию законопроекта. «Часть тезисов законопроекта будет зависеть от окончательной и одобренной Советом федерации редакции закона об оборотных штрафах, поскольку инициатива по созданию киберстрахования была направлена как раз на борьбу с утечками персональной информации»,— напоминает он. Внести законопроект в Госдуму планируется после создания необходимой нормативной базы.

IT-отрасль встречает инициативу сенаторов с интересом, так как ранее подобного механизма на законодательном уровне не было, и компании по-прежнему рискуют пострадать от кибератак, при этом не получая никакой компенсации. «Когда летом Совет федерации предложил идею киберстрахования, это вызвало активные дискуссии среди экспертов и представителей бизнеса»,— рассказывает гендиректор IT-компании ONLY Кирилл Владимиров. Бизнес уже активно пользуется различными страховыми продуктами, такими как имущественное страхование или страхование ответственности, объясняет он.

с16

Билборд узнает из тысячи

— технологии —

Анализ больших данных сегодня позволяет измерять аудиторию наружных рекламных конструкций, лучше планировать кампании и эффективнее оценивать их результат, отмечают участники рынка. „Ъ“ разбирался, кто сейчас поставляет большие данные операторам наружной рекламы и как они используются.

БОльшая часть затрат рекламодателей на наружную рекламу в России уже приходится именно на цифровые экраны, следует из оценок измерителя Admerix: доля цифровой наружной рекламы в затратах рекламодателей в России, по данным компании, за январь—июль 2023 года составила 54%. За аналогичный период 2022-го показатель составлял 48%, 2021-го — 40%. В оценке учтены продажи наружной рекламы в стандартных форматах (сити-борды, суперсайты, пиллары) в 50 городах РФ, не включена индор-реклама (в ТЦ и пр.) и транзитная реклама (на транспорте, в аэропортах и др.). В крупных городах показатель всегда был выше: как оценивали в группе Russ, доля digital наружной рекламы в Москве выросла за последние два года вдвое и, по данным на сентябрь, равна 67%, в Санкт-Петербурге — 43%.

Операторы наружной рекламы инвестируют в закупку экранов: ими заменяют статические щиты в востребованных местах. Экран позволяет показать намного больше рекламных сообщений, чем традиционные форматы. Кроме того, разместить рекламу на экране намного быстрее, чем печатать и устанавливать билборд. Это позволяет учитывать особенности аудитории в моменте размещения — «считать» ее портрет позволяет Big Data.

Откуда берутся данные

Операторы наружной рекламы в России сейчас ежедневно собирают и обрабатывают более 100 млн записей, оценивает управляющий директор объединенного баинга группы «Игроник» Анастасия Сергеева. Это MAC-адреса пользователей (уникальный идентификатор, назначенный сетевому адаптеру в мобильном устройстве), которые собирают с помощью Wi-Fi снифферов, средств для перехвата и анализа трафика на цифровых билбордах, а также технологии GPS и геозонирования.

«Основные данные, которые собираются (обезличенно),— это социально-демографический портрет (пол, возраст, доход), интересы и предпочтения, покупки и места посещения. Для более точной оценки аудитории и анализа размещения операторы наружной рекламы прибегают к сотрудничеству с другими компаниями, которые также собирают MAC-адреса»,— объясняет Анастасия Сергеева. Операторы связи и банки при сборе больших данных используют также такие идентификаторы, как cookies, email-адреса, номера телефонов и др., добавила она: «Операторы связи могут предоставить данные о местоположении клиентов, а банки — информацию о покупках клиентов в определенных категориях товаров».

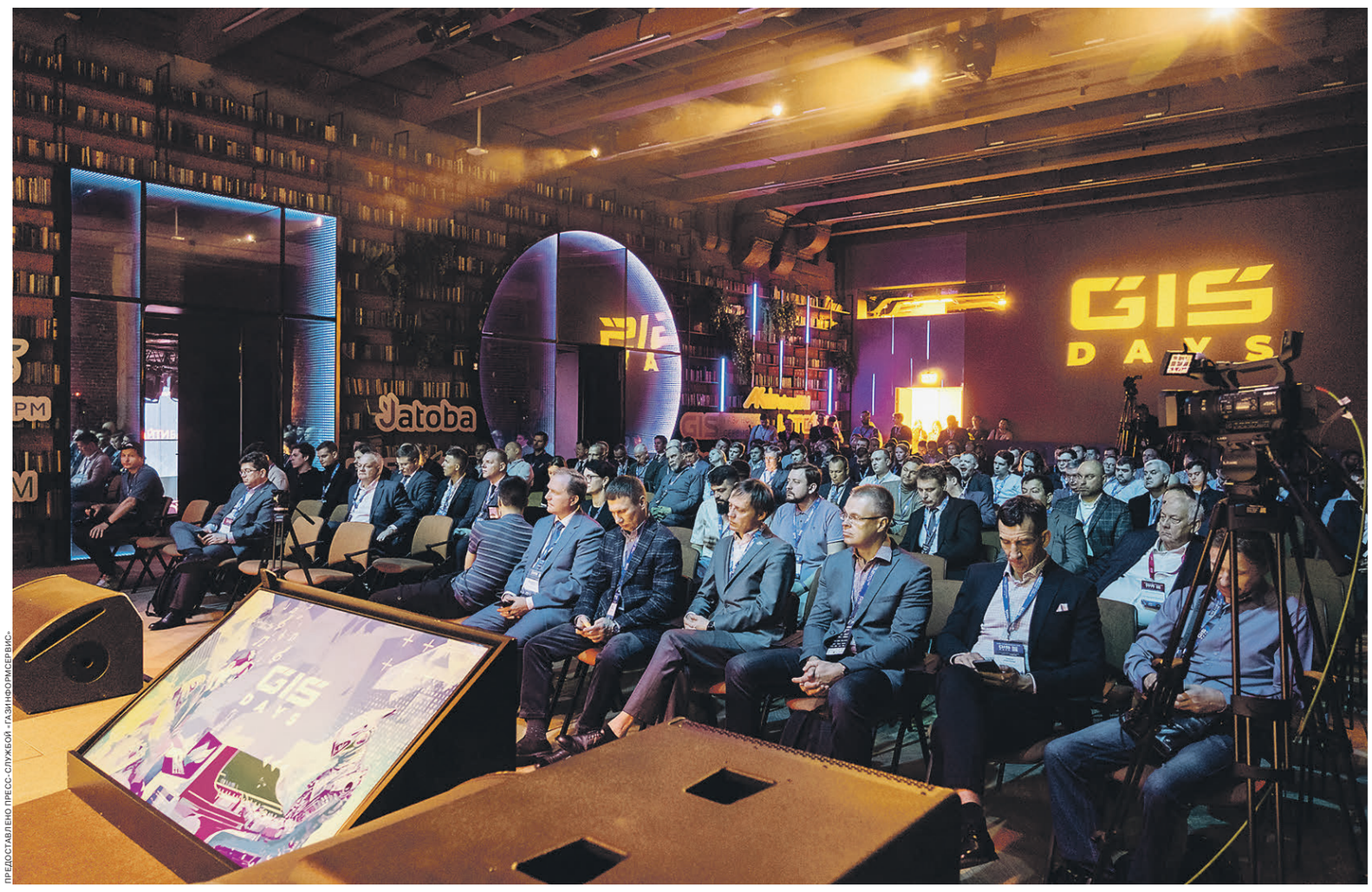
с18

информационные технологии

GIS ГАЗИНФОРМ СЕРВИС

В джазе только ИИ

Осень 2023 года стала крайне насыщенной по проводимым IT-мероприятиям. Сказались накопленный за прошедший год опыт, которым компании сейчас готовы делиться, оживление в бизнес-среде после, как говорят в самой отрасли, шока 2022 года и общее ощущение оптимизма и сплоченности, несмотря на сложные вопросы в области импортозамещения, которые еще предстоит решить. Одним из крупнейших IT-событий года стал форум GIS Days 2023 компании «Газинформсервис», который прошел с 4 по 6 октября сразу в двух городах: Санкт-Петербурге и Москве. „Ъ“ пообщался с участниками форума и убедился: у отрасли не только за год накопился колоссальный опыт, но и появились амбициозные планы.



ПРЕДОСТАВЛЕНО ПРЕСС-СЛУЖБОЙ «ГАЗИНФОРМСЕРВИС»

— дискуссия —

В Санкт-Петербурге и Москве прошел ежегодный форум GIS Days 2023 (Global Information Security Days), который объединил более 170 экспертов в области информационной безопасности, искусственного интеллекта (ИИ) и IT в целом. Организатор форума компания «Газинформсервис» провела GIS Days уже в шестой раз, стилизовав мероприятие под эпоху джаза и выбрав темой события ИИ в кибербезопасности — одну из самых обсуждаемых не только в России, но и во всем мире.

Тема привлекла такое внимание во многом благодаря стремительному росту популярности ChatGPT компании OpenAI, который в силу своей простоты показал, насколько легко обучить нейросети тем или иным задачам. И если для простых пользователей понятный ИИ стал скорее подспорьем, то для мирового сообщества в области кибербезопасности — новой нарастающей угрозой. Хотя в официальных условиях работы того же ChatGPT закреплен запрет на создание вредоносных продуктов, правила были нарушены практически сразу: более опытные пользователи нейросети начали тестировать автоматическое написание вирусных программ и других хакерских инструментов. Это лишь подтвердило опасения специалистов по кибербезопасности как в мире, так и в России.

При этом кибератаки на российскую IT-инфраструктуру за год только возросли: их число увеличилось в два раза относительно прошлого года, а атак хакеров на IT-сектор — в четыре (см. „Ъ“ от 29 августа). Такая повестка сделала GIS Days 2023 особенно актуальным событием.

GIS Days 2023 в Москве открыл учредитель компании «Газинформсервис» Валерий Пустарнаков: «Искусственный интеллект — это не просто хайп, а развивающаяся прикладная технология,— сообщил он,— и наша задача как профессионального сообщества — сделать использование ИИ безопасным, и наш форум поможет в этом».

● *«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, через год ей исполнится 20 лет. Ее решениями пользуются госсектор и бизнес не только в России, но и в Киргизии, Белоруссии и Казахстане. Среди клиентов и партнеров компании — ПАО «Газпром» и его дочерние структуры, ГК «Норникель», а также лидеры российского рынка кибербезопасности.*

На мероприятии эксперты — как со стороны бизнеса, так и регуляторов и научного сообщества — обсуждали, можно ли использовать нейросети в свою пользу, борясь со злоумышленниками и предугадывая их шаги. В первый день форума, который прошел в Санкт-Петербурге, на Клубе IT-директоров доцент факультета безопасности IT ИТМО, научный руководитель по направлению «Безопасность ИИ» Наталия Волошина рассказала, что в современных технологиях решения для кибербезопасности с элементами ИИ можно использовать только в единой инфраструктуре. «В нее должны быть включены функционал уже имеющихся цифровых решений, ресурсы компании, специалисты, постоянно проходящие обучение, и средства безопасности». И уже в эту целостную IT-инфраструктуру безопасно добавлять элементы ИИ, считает эксперт.

Однако использование нейросетей диктует и другие условия компаниям, которые работают над его развитием. Например, умение собирать и обрабатывать большие объемы данных, адаптировать их в единый формат для корректного использования и, конечно, гарантировать их безопасность, добавляет эксперт по цифровой трансформации компании «Аквариус» Александр Дмитриев. Но при правильном использовании данных и IT-решений ИИ позволяет, например, ускорить вычисления, а также обмен данными между пользователями и инфраструктурой, улучшить контроль за качеством информации и даже повысить безопасность их хранения.

При правильном использовании данных и IT-решений ИИ позволяет ускорить вычисления, улучшить контроль за качеством информации и даже повысить безопасность их хранения

Взгляд бизнеса и регулятора: оцениваем риски

Во второй день GIS Days 2023 в Москве, который компания провела в новом пространстве «Кибердом», на пленарной дискуссии «Использование систем искусственного интеллекта: вопросы доверия и информационной безопасности» собрались представители Минцифры, крупного бизнеса и профильных ассоциаций, чтобы обменяться мнениями, где нейросети создают риски и как свести их до минимума.

Заместитель министра цифрового развития, связи и массовых коммуникаций РФ Александр Шойтов сообщил, что замедлять развитие ИИ в России не нужно, важно просто постепенно и осторожно внедрять его в работу. Так как на данный момент Минцифры в первую очередь беспокоят риски неправильного функционирования нейросетей, которые могут быть связаны с некорректными данными или самим алгоритмом. Причем искажены как данные, так и сама технология могут быть намеренно, напоминает Александр Шойтов.

«Критичными ошибки в использовании ИИ становятся, когда люди начинают принимать решения на основании данных, сгенерированных нейросетями»,— напоминает эксперт. Поэтому сейчас наиболее критичными являются сферы высокотехнологичные, например автоматизированный транспорт, медицина, а также критическая информационная инфраструктура (КИИ, телекоммуникации, промышленность и т. д.). Таким образом, риски возрастают во всех сферах, где специалисты уже передали технологии ИИ ряд вопросов, по которым он может принимать решения.

ИИ в помощь замещению

С уходом в 2022 году с российского рынка западных компаний и остановки действия к 2023 году большинства лицензий на зарубежные IT-продукты российская отрасль получила мощный стимул для развития. Через год после GIS Days 2022, где импортозамещение стало главной темой события, а эксперты рынка обсуждали трудности оперативного замещения необходимых продуктов, настроение участников сменилось оптимизмом и осознанием достигнутых результатов.

Как рассказал „Ъ“ Николай Нашивочников, «отрасль преодолела зону турбулентности»: полтора года назад многие компании не знали, на чем конкретно сфокусироваться, и в то же время постоянно подвергались кибератакам. Это заставило сместить акцент в сторону результативного кибербеза, а также начать использовать уже имеющийся в России инструментарий для отражения атак, перечисляет Николай Нашивочников. Он также напомнил, что именно в период турбулентности ИБ-отрасль повела себя сплоченно, объединяя усилия для помощи слабозащищенным компаниям, даже если у клиента не было возможности закупить необходимые решения.

В 2023 году многие процессы стали плановыми, продолжает Николай Нашивочников, вендоры окрепли и накопили опыт. И рынок находится в стадии активного импортозамещения, в случае с кибербезопасностью это процесс одновременный с IT-инфраструктурой в целом. Если раньше компании сначала замещали цифровую инфраструктуру, а затем постепенно переходили на российские системы защиты, то в 2023 году эти процессы синхронизировались, рассказал эксперт. И участники рынка делают ставку на проектирование «изначально безопасной цифровой среды» (Secure by design).

«Критичными ошибки в использовании ИИ становятся, когда люди начинают принимать решения на основании данных, сгенерированных нейросетями»

В первый день форума в Санкт-Петербурге в рамках Клуба IT-директоров заместитель генерального директора «Газинформсервиса» Роман Пустарнаков отметил, что технологии искусственного интеллекта отведено значительное место и в процессе импортозамещения, где он уже применяется для автоматизации важных задач.

Продемонстрировал это ведущий эксперт нефтегазовой отрасли Fplus Дмитрий Сивокоз. Он рассказал, что в российской промышленности ИИ используется для анализа больших данных: от текста до видеоизображений, выявления аномалий и предотвращения аварийных ситуаций. Что крайне востребовано в том числе в нефтегазовой отрасли.

Одним из наиболее ярких импортозамещающих продуктов, созданных к осени 2023 года и обсуждаемых на GIS Days, стало комплексное решение от компании «Газинформсервис» Efros Defence Operations (Efros DefOps). Оно предназначено для защиты сетевых и оконечных устройств, компонентов сред виртуализации, а также прикладного программного обеспечения: SCADA, RPA и СУБД. Руководитель группы продуктов «Газинформсервиса» Сергей Никитин рассказал „Ъ“, что Efros DefOps был создан на основе уже проверенных компанией технологий, которые решали смежные задачи, однако были разрозненными. Новый продукт предназначен для работы в одном пространстве данных, то есть не нужно будет обслуживать несколько разных хранилищ данных под разные элементы ИТ-инфраструктуры.

«С точки зрения клиента это в первую очередь удобно, так как все подсистемы комплекса предоставляют информацию в рамках „одного окна“. В качестве приятного бонуса пользователь получает интеграцию разных продуктов как бы «в подарок». Сергей Никитин подчеркнул, что важно понимать: российские разработчики многое сделали и до 2022 года, в том числе потому, что зарубежные решения не закрывали всех потребностей заказчиков. Но сейчас приоритетом стало создание собственных независимых продуктов, а не интеграции заточенных под Россию решений с западными. Efros Defence Operations — один из результатов усердной работы компании над надежной защитой своих компаний-клиентов. Продукт уже сертифицирован и прошел все необходимые испытания, уточняют в компании, а также включен в единый реестр российских программ для ЭВМ.

На старт: молодые команды на GIS Days 2023

По традиции в родном для «Газинформсервиса» Санкт-Петербурге в рамках GIS Days компания провела студенческий форум и подвела итоги ежегодного конкурса «Биржа IT-стартапов». В текущем году на участие в конкурсе было подано почти 300 заявок из 49 городов России, развивающих собственные проекты в разных цифровых сферах.

На вручении члены жюри отметили: при выборе победителей оценивались проработка технологии искусственного интеллекта, маркетинговая составляющая проекта, его востребованность на рынке, а также цель, к которой идет каждая молодая команда. В финал конкурса вышли пять новых команд, каждую из которых, уверены члены жюри, ждет большое будущее.

Главный приз — 1 млн руб. на развитие IT-проекта — получили разработчики платформы для выявления инсульта на базе искусственного интеллекта Invessel AI из Казани. Технология строится на анализе снимков головного мозга с помощью ИИ и оповещает специалистов об обнаруженных нарушениях кровообращения. С помощью платформы диагностика инсульта сокращается с получаса до пяти минут, и шансы на успешный исход лечения повышаются в разы.

Вторую награду от партнеров «Газинформсервиса» — Школы стартапов «Сколково» — получили создатели проекта VISION, который с использованием ИИ проектирует дизайны для различных областей: промышленности, строительства, машиностроения и т. д. VISION за сутки генерирует готовые решения в виде чертежей, 3D-туров, фото- и видеовизуализации, что снижает временные и финансовые затраты на создание моделей.

Также в финал вышла команда разработчиков финансовой системы ТАФС, выявляющей неправомерные финансовые операции. Алгоритм распознает хищения, мошеннические действия, отмывания средств другую подозрительную деятельность клиентов и сотрудников финансовых организаций. Организаторы отметили, что проект стал особенно актуальным с ростом кибератак на российских пользователей в 2023 году. Внимание заслужил и новый цифровой сервис AIINS для управления корпоративным страховым портфелем. Он автоматизирует процесс страхования организаций, сравнивая ключевые параметры полисов при их выборе, анализирует расходы и контролирует необходимые платежи.

«Все участники готовы заявить о себе на рынке уже сейчас»,— констатируют организаторы конкурса.

GIS Days 2023 в цифрах и участниках

К завершению форума GIS DAYS 2023 его увидело более 860 тыс. человек — столько пользователей подключилось к трансляции в соцсетях, а с докладами выступили более 50 топовых спикеров перед широкой профессиональной аудиторией. При этом в 2022 году аудитория форума была около 170 тыс. человек, и такой стремительный рост интереса к теме кибербезопасности и самому мероприятию свидетельствует о динамичном развитии отрасли.

Среди компаний на форуме присутствовали «Ростелеком», ГК «Солар», Fplus, «Код безопасности», Zecurion, Positive Technologies, Xello, Usergate, «РЕД СОФТ», «АйТи БАСТИОН», «Аладдин Р.Д.», Check Point, «ИнфоТеКС», «Киберпротект» и многие другие. В докладах участников звучали разные точки зрения на искусственный интеллект и кибербезопасность: одни компании видят в технологии ключ к решению сложных вопросов, например дефицита IT-кадров, другие — повышение эффективности уже существующих цифровых решений. Однако ряд экспертов решил выделить именно человеческую составляющую освоения новых технологий.

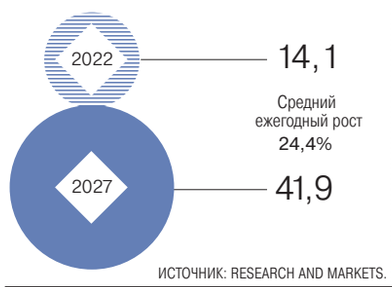
«Если учесть, что для современных информационных систем характерны размытость периметров защиты, новые векторы для кибератак и затруднительность контроля за инфраструктурой, то мы видим, что для автоматизации работы хакеров с использованием ИИ эти особенности систем только на руку»,— говорит операционный директор Check Point (Russia) Василий Широков. И бороться с этим, считает эксперт, нужно с использованием того, что пока непосильно ИИ: автономного мышления с творческой составляющей, то есть постановкой новых задач, что пока свойственно только людям. А значит, специалисты должны сконцентрироваться на стратегии и системности в подходах к своей работе и грамотной постановке новых целей. Творчество во всех аспектах жизни будет тем, что не сможет заменить и превзойти искусственный интеллект, а значит, преимущество всегда будет на стороне людей, заключает Василий Широков.

И участникам GIS DAYS 2023 хочется в это верить. В противном случае, говорит собеседник „Ъ“ на форуме, здесь должны были бы собираться роботы и слушать доклады, сгенерированные искусственным интеллектом. И хорошо, что это пока не так.

Татьяна Исакова

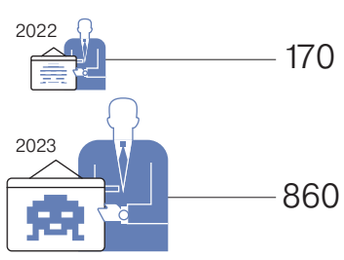
УРОВЕНЬ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ ИИ В РАЗНЫХ ОБЛАСТЯХ (% ОТ ЧИСЛА ОРГАНИЗАЦИЙ, РФ) ИСТОЧНИК: ИСИЭЗ НИУ ВШЭ.

РОСТ РЫНКА ИИ В КИБЕРБЕЗОПАСНОСТИ В МИРЕ ($ МЛРД)



ИСТОЧНИК: RESEARCH AND MARKETS.

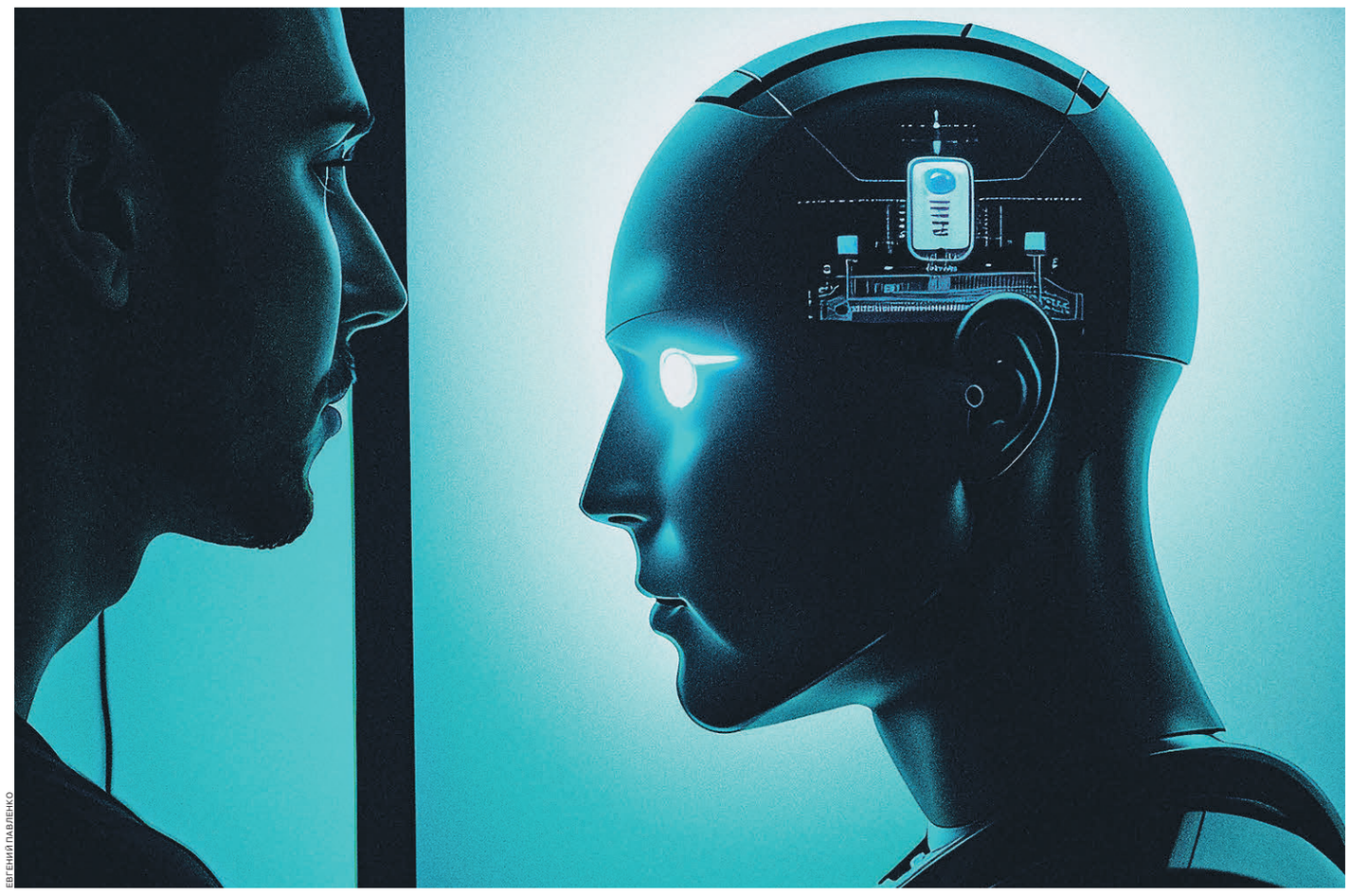
РОСТ АУДИТОРИИ GIS DAYS (ПОСЕЩЕНИЕ ОНЛАЙН И ОФФЛАЙН (ТЫС.)



ИСТОЧНИК: «ГАЗИНФОРМСЕРВИС».

Интеллект на страже информации

Любая новая и перспективная технология всегда сталкивается с тем, что в какой-то момент ее начинают использовать как во благо, так и наоборот. Искусственный интеллект не стал исключением и нашел свое применение и у хакеров. Защищать инфраструктуру от вредоносного программного обеспечения и других атак штатному IT-специалисту будет сложно, поэтому компании все больше задействуют искусственный интеллект для борьбы со злоумышленниками. Эксперты российской группы IT-компаний «Ланит» рассказывают о трендах искусственного интеллекта в кибербезопасности.



ЕВГЕНИЙ ПАВЛЕНКО

— кибербезопасность —

Согласно данным аналитической компании IDC, расходы на искусственный интеллект (ИИ) в 2023 году в Европе достигнут $34,2 млрд, что составляет 20,6% мирового объема инвестиций в эти технологии. Аналитики отмечают, что больше всего средств вкладывается в банковскую сферу (15,7%), сферу услуг (11,2%) и ритейл (10,9%).

В то же время инвестиции в развитие искусственного интеллекта в кибербезопасности также демонстрируют положительную динамику. Так, по данным MarketsandMarkets, сейчас объем мирового рынка ИИ в этой сфере достигает $22,4 млрд, а к 2028 году прогнозируется его увеличение до $60,6 млрд. Аналитики связывают такой финансовый подъем с повышенной уязвимостью сетей Wi-Fi, вызванной огромным количеством мобильных и смарт-устройств. Самый высокий среднегодовой темп роста до 2028 года будет наблюдаться в Азиатско-Тихоокеанском регионе, куда входят Китай, Россия, США и другие страны. В MarketsandMarkets подчеркивают, что в связи с популярностью перехода бизнеса на облачные серверы злоумышленники вынуждены адаптироваться и использовать новые способы кибератак: программы-вымогатели, вредоносное ПО для мошенничества с рекламой, DDoS, ботнеты, трояны и др.

Мошенники уже больше трех лет задействуют ИИ в собственных целях. Так, в конце 2020 года аналитики компании Trend Micro, специализирующейся на кибербезопасности, совместно с Межрегиональным научно-исследовательским институтом ООН по вопросам преступности и правосудия и Европолом подготовили доклад «Злонамеренное использование и злоупотребление искусственным интеллектом». В нем указано, что технологии ИИ чаще всего применяются для создания дипфейков, которые заменяют голос или изображение одного человека на другого. Также искусственный интеллект используют для повышения эффективности вредоносного ПО.

ИИ в центрах управления безопасностью

Искусственный интеллект в центрах управления безопасностью (SOC) применяется во многих направлениях: для автоматизации процессов и отдельных действий, разгрузки аналитиков от ручной работы, а также в принятии некоторых решений, объясняет директор центра мониторинга и противодействия кибератакам IZ:SOC компании «Информзащита» Александр Матвеев. По его словам, применение ИИ может значительно упростить работу SOC, например увеличит скорость обработки инцидентов и уменьшит количество рутинных задач, которые отнимают много времени и зачастую мешают глубже погружаться в суть. «Автоматизация и, как следствие, упрощенный процесс первичной обработки позволят аналитикам больше концентрироваться на самих инцидентах»,— отмечает он.

Господин Матвеев подчеркивает, что ИИ вряд ли полностью заменит человека, однако может стать инструментом для решения задач: «Все упирается в вопрос доверия к ИИ и принятым им решениям, которые могут привести к драматическому исходу». Насколько бы ни была обученной модель ИИ, она рано или поздно столкнется с чем-то, что отсутствовало в данных для обучения, поэтому еще рано говорить о том, что ИИ заменит сотрудников SOC.

По прогнозу Александра Матвеева, вероятность того, что компании целиком перейдут на ИИ в кибербезопасности, крайне мала. «Многие уже частично применяют или планируют использовать функционал ИИ для решения и упрощения конкретных задач, а также для автоматизации отдельных процессов. Это позволяет не только экономить ресурсы, но и предоставляет определенное конкурентное преимущество»,— отмечает он, добавляя, что рано или поздно большинство компаний заместят с помощью ИИ все больше функций, которые сейчас выполняются аналитиками вручную. Среди перспективных направлений для искусственного интеллекта Александр Матвеев называет прогнозирование атак, в том числе тех, о которых достоверно еще неизвестно, планирование реагирования на инциденты, поддержку в восстановлении скомпрометированных систем и т. д.

ИИ в симбиозе с человеком

Искусственный интеллект способен значительно ускорить работу, автоматизируя задачи пентеста (анализ системы на наличие уязвимостей), говорит директор центра информационной безопасности «Ланит-Интеграции» Николай Фокин. По его словам, применение ИИ не только сокращает время тестирования безопасности, генерации сценариев атак, анализа собранных данных, верификации уязвимостей, создания отчетов и т. д., но и позволяет проводить более частые и комплексные проверки в большем масштабе. «Для крупных и динамичных инфраструктур это действительно важно, здесь можно привести в качестве примера генеративные модели ИИ. PentestGPT может выступать ассистентом специалиста при проведении пентеста (метод оценки безопасности IT-систем средствами моделирования атаки.— „Ъ“)»,— отмечает эксперт.

Господин Фокин уверяет, что использование хорошо обученного ИИ позволяет повысить качество пентеста и избежать погрешностей, которые сопряжены с человеческим фактором. Искусственный интеллект, продолжает он, способен дать более высокую точность, снижая ложные срабатывания и выстраивая векторы атак на основе реальных достижений. «Модели, обученные на больших наборах данных, потенциально позволяют распознавать закономерности и выявлять уязвимости, которые могут быть неочевидны для ИБ-специалистов». Он считает, что ИИ со временем сможет адаптировать используемые тактики и техники, обучаясь на прошлых результатах, в зависимости от угроз и окружения инфраструктуры, в котором он находится. «Применение искусственного интеллекта позволит снизить общие затраты на пентест и получить силу тысяч пентестеров в одной автоматизированной системе, а также сократить время на исправление обнаруженных уязвимостей за счет их более качественной приоритизации».

При этом директор центра информационной безопасности «Ланит-Интеграции» отмечает, что использование ИИ при атаках на инфраструктуру сопряжено с некоторыми рисками: в отличие от человека, он не осознает возможных последствий и может не соблюдать ограничения при тестировании, поскольку не способен оценить риск воздействия на бизнес-процессы. «ИБ-специалист обладает творческой силой, интуицией и, возможно, не в 100% случаев, но лучше понимает контекст задачи. Поэтому, на мой взгляд, предпочтительный сценарий — сочетание возможностей ИИ и квалифицированных специалистов»,— дополнил он.

Среди перспектив применения ИИ в пентестах Николай Фокин отмечает несколько направлений: создание систем, способных адаптироваться к ландшафту и контексту, а также совершенствоваться по результатам достижений, автоматизация и симуляция сложных сценариев атак, повышение точности алгоритмов, а также более быстрое развитие инструментария для пентеста благодаря накоплению большого объема данных. ИИ хорошо справляется и с задачей обнаружения уязвимостей нулевого дня — искусственный интеллект может анализировать поведение систем и выявлять аномалии, связанные с возможностью эксплуатации. Отдельно стоит отметить вовлечение все большего числа специалистов по безопасности во взаимодействие с ИИ и его обучение.

ИИ на страже информации

Детекция аномалий (обнаружение уязвимостей) способна выявлять различные типы вредоносных активностей, которые не могут быть определены общепринятыми методами.

Традиционные методы детекции аномалий опираются на заранее известные паттерны вредоносной активности, например на сигнатуры вирусов, говорит руководитель практики анализа данных центра компетенций больших данных и искусственного интеллекта «Ланит» Владислав Балаев. По его словам, шаблоны вредоносного поведения ищутся по уже выявленным ранее типам атак. «Методы детекции аномалий основаны на том, что создается модель типичного поведения системы. Далее происходит анализ действий системы, который позволяет понять, насколько ее поведение отличается от обычного»,— поясняет он, добавляя, что традиционные методы ищут паттерны подозрительной активности в работе системы, а методы детекции аномалий создают картину нормального поведения, где любые признаки отклонения считаются вредоносными.

Среди преимуществ методов детекции аномалий Владислав Балаев отмечает способность выявлять новые, ранее не случившиеся типы вредоносной активности. Среди недостатков — частые сработки на легитимные события, которые отличаются от обычного поведения: перезагрузка системы, обновление ПО, смена пользователей, перепрошивка сетевых устройств.

Искусственный интеллект представляет собой совокупность математических методов, которые используются для выделения аномалий, объясняет Владислав Балаев. По его словам, ИИ вместе с современными MLOps-практиками дает возможность автоматизировать обработку больших объемов данных ИБ. На них обучаются модели машинного обучения, позволяющие выявлять скрытые закономерности между различными показателями работы информационных систем. «Благодаря этому повышается эффективность обработки данных о работе информационных систем, что в конечном счете увеличивает точность и полноту выявляемых атак и вредоносной активности»,— подчеркнул он.

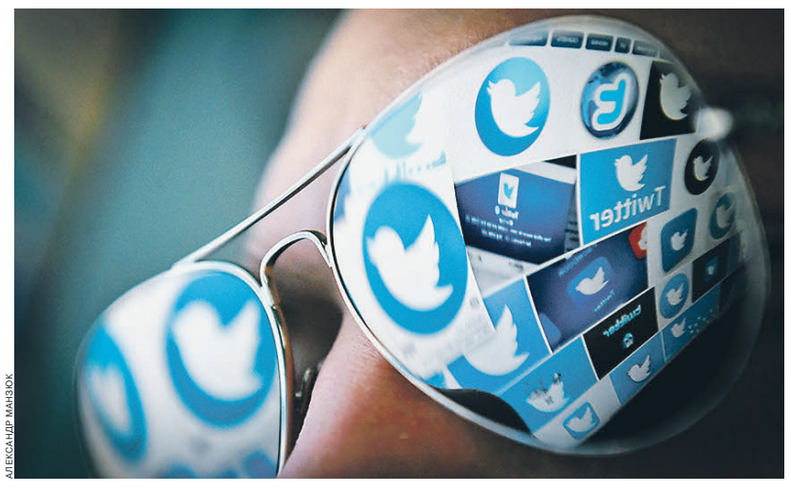
Среди главных перспектив развития технологий детекции аномалий с использованием ИИ эксперт называет следующие тренды: способность выявлять нелинейные сложные зависимости между различными компонентами информационных систем и обнаружение неизвестных ранее типов вредоносной активности. «Эти методы не являются панацеей и обладают рядом недостатков, самым большим из которых является наличие ложных срабатываний, требующих фильтрации результатов и тонкой настройки системы. Однако благодаря своим преимуществам, несмотря на описанные выше нюансы использования, детекция аномалий является необходимым звеном для обеспечения комплексной защиты системами обнаружения вторжений»,— заключил господин Балаев.

Матвей Кислинский

Не тредом единым жив микроблог

— социальные сети —

Сервисы микроблогов, ранее считавшиеся нишевыми или экспериментальными, смогли нарастить известность вследствие продажи Twitter Илону Маску. Mastodon и Bluesky обещают пользователям свободу переноса контента и подписчиков и отсутствие человеческого фактора при верификации. Эксперты признают интерес пользователей к подобным решениям, но уверены, что их недостаточно для создания серьезной угрозы уже привычному сервису.



АЛЕКСАНДР МАНЗЮК

Развитие Twitter (ныне переименован в X) после его покупки Илоном Маском за $44 млрд стало одним из наиболее ярких примеров смены курса управления, предпринятых на рынке социальных платформ в последние годы. Новый владелец ослабил модерацию контента, сократил штат компании и сделал акцент на монетизацию Twitter путем продажи подписок конечным пользователям. В перспективе, которую господин Маск периодически очерчивает в публичных заявлениях, бывший Twitter должен стать «приложением для всего» и объединять функции, пока еще не реализованные на площадке: от видеозвонков до банкинга.

Одним из последствий продажи Twitter стало оживление конкуренции в сфере микроблогов, не наблюдавшейся со времен популяризации соцсетей в 2000-х и 2010-х годах. Компания Meta (ее деятельность по функционированию Facebook и Instagram объявлена в РФ экстремистской и запрещена), которая в последние годы пыталась перестроить свой образ с расчетом на метавселенные и виртуальную реальность, запустила на базе Instagram сервис Threads. Популярность стали набирать и нишевые проекты, как новые, так и ранее существовавшие, призванные воссоздать базовый функционал Twitter.

Вот тебе, блогер, и Юрьев день

Связь между продажей Twitter и сменой его направления развития вызвала всплеск интереса к децентрализированным социальным сетям, которые по своему определению не имеют единого владения или общей политики. Разработчики таких сетей создают не сервис как таковой, а серверное ПО для его работы чаще всего — с открытым исходным кодом. Решение вопросов о правилах каждого отдельного сегмента сети, модерации внутри него и его повседневной работе остаются за администратором каждого из серверов.

Наиболее известным сервисом подобного рода считается Mastodon, разрабатываемый с 2016 года. Пользователь Mastodon может не только выбрать тот сервер, который считает наиболее подходящим, но и переносить свой контент, подписки и подписчиков с одного сервера на другой. По общему правилу использование того или иного сервера Mastodon не ограничивает пользователя в его возможности подписываться на людей с другого сервера и общаться с ними. Администраторы, однако, имеют право ограничивать связь с конкретными серверами — например, если с них поступает спам или если они считают размещаемый контент неприемлемым.

Реализовать переносимость данных обещает и сервис Bluesky, основанный в 2021 году с финансированием от Twitter как экспериментальный проект. Пока что эта сеть существует в виде единственного сервера с регистрацией по приглашениям. Код серверного ПО не является открытым, однако компания публикует код клиентских приложений (тех, с которыми взаимодействует пользователь) и подробности протокола, что должно обеспечивать независимость серверов.

Небольшие соцсети потенциально могут привлечь пользователей, «уже окончательно подсевших на микроблоги», считает гендиректор Epicstars Денис Волков. По его мнению, техническая возможность переноса наработок между площадками поможет последним: «Новым соцсетям будет проще создавать костяк аудитории». Гендиректор КРОС Екатерина Мовсесян, однако, полагает, что массовый пользователь едва ли задумывается о подобных возможностях: «В первую очередь для него важно удобство использования и отсутствие ограничений». Переносимость данных, по ее словам, не избавляет от необходимости придумывать контент, который был бы уникальным для каждой новой площадки: «Поэтому переход в любом случае проявляет необходимость „пересобирать“ список своих подписок и подписчиков».

Сам себя верифицируй

Илон Маск еще в процессе обсуждения покупки Twitter высказывал недовольство непрозрачной, по его мнению, системой верификации значимых людей и организаций на платформе. Это привело к фактическому уничтожению существовавшей системы проверки значимости: «синяя галочка», которая раньше выдавалась только знаменитым людям, стала лишь индикатором того, что пользователь X/Twitter оплачивает ежемесячную подписку. Перемены усугубили проблему имперсонации (выдачи человека за того, кем он не является). В сентябре X объявила, что платящие за «галочку» пользователи могут получить дополнительный индикатор «проверенности» — для этого нужно предоставить соцсети документ, удостоверяющий личность.

Как Mastodon, так и Bluesky используют системы верификации, не зависящие от какого-то одного органа проверки значимости или платежеспособности. Они подразумевают, что у пользователя уже есть внешний ресурс в интернете, который идентифицирует его и находится под его контролем. Чтобы верифицировать себя на Mastodon, пользователь должен разместить на этой странице, например на собственном сайте или на личной странице корпоративного сайта, специально отформатированную ссылку на своей аккаунт. Именно эта система перекрестной проверки интернет-ресурсов стала первым примером взаимодействия между Threads и другими соцсетями: в августе пользователи Mastodon смогли верифицировать ссылки на свой профиль в Threads.

Bluesky для целей проверки подлинности позволяет привязать учетную запись к домену, контролируемому пользователем, по аналогии с веб-хостингом или сервисом электронной почты. Такой подход решает не только проблему верификации, но и вопрос «парковки» красивых или значимых ников в сети. В числе крупных компаний и организаций, которые верифицировали себя таким образом,— Microsoft, Internet Archive, а также крупные американские СМИ: The New York Times, Washington Post, Ars Technica и другие. На Bluesky «припарковалось» и радио NPR — первая крупная организация, которая в апреле покинула Twitter в знак несогласия с обозначением его связи с государством.

Рано ставить крест на X

У X/Twitter, несмотря на растущую популярность небольших соцсетей, все еще остается «устойчивое ядро частных и бизнес-пользователей, на активности которых можно заработать», считает господин Волков: «Едва ли Илон Маск откажется от этой возможности, тем более что на пятки ему наступает Threads». Но парадигма платформы меняется, и в перспективе она может перестать быть одним лишь средством общения пользователей: «В этот переходный период наиболее востребована может быть новостная составляющая X».

«Несколько хаотичный» подход к модерации в Twitter действительно привел к тому, что «некоторая часть прежней ядерной аудитории либо снизила свою активность, либо ушла», признает директор по стратегическим коммуникациям Brand Analytics Василий Черный. Он, однако, отмечает, что на площадку вернулись те, кто раньше разочаровался в сервисе, и оптимистично оценивает будущее X/Twitter: «Если сеть не умерла в первый год под Илоном Маском, то и не умрет в ближайшее время, а будет потихоньку возвращать аудиторию».

Новые проекты, призванные заменить какую бы то ни было соцсеть, несильно поменяют рынок, полагает основатель рекламного агентства Digital Church Марк Хлуднев: «Для того чтобы новая сеть стала популярной, у нее должна быть какая-то интересная фишка. Таких на данный момент нет». Аудитория X, по его мнению, сохранится, «пока в соцсети нет кардинальных изменений и пока со стороны Илона Маска не исходят действия, сигнализирующие, что у нее могут быть проблемы».

Юрий Литвиненко

информационные технологии

Манхьовая пелена

После начала военных действий на Украине Россия начала активно развивать сотрудничество с азиатскими странами. Так, российские издатели после ухода с рынка западных правообладателей комиксов в лице Marvel и DC начали наращивать присутствие в портфеле китайских, корейских и японских наименований. Сейчас азиатские комиксы являются одной из точек развития книжной отрасли, утверждают участники рынка. При этом, напоминают эксперты, в сегменте остро стоит проблема пиратства — на такие продажи приходится около 5% рынка. БОльшая часть контрафактной комиксной продукции изготавливалась на Украине, утверждают собеседники „Ъ“ на издательском рынке — сейчас печатный поток значительно сократился, однако онлайн-копий становится все больше.

— медиаиндустрия —

АНАТОЛИЙ ЖДАНОВ

Новое искусство за миллион

Продажи манги в книжной сети «Читай-город» по итогам первого полугодия сократились на 6% год к году, сообщил „Ъ“ представитель издательского холдинга «Эксмо-АСТ». В компании связывают спад продаж с выходом топовых новинок: «В 2022 году выходило больше тайтлов (наименований.— „Ъ“) — первых серий томов, в 2023-м в новинки попадают продолжения серий, которые покупаются менее активно». При этом, уточнили в компании, с июля продажи в категории начали планомерно расти.

В «Манн, Иванов и Фербер» (МИФ), наоборот, отмечают рост продаж: в первом полугодии показатель вырос на 50%. «Мы увеличили количество азиатских комиксов в портфеле за этот период и продолжим наращивать и в следующем»,— говорит руководитель редакции «Комиксы» Анна Сиваева. Она напомнила, что сейчас главный стимул для книжного рынка — азиатские комиксы, поэтому спрос растет, как и количество новинок в этом сегменте на рынке.

В «Эксмо-АСТ» сообщили, что в первом полугодии самый популярный жанр — это «магическая и боевая» манга. На втором месте — жанр «школа» (главными героями выступают школьники). На третьем — фэнтези, далее — ужасы и комедийная манга. При этом портфель манги в книжной сети «Читай-город» вырос на 21% в первом полугодии по сравнению с прошлым годом, добавил представитель издательского холдинга. В топе продаж сейчас находятся серии «Человек-бензопила», «Sailor Moon», «Истребитель демонов», «Проза бродячих псов», а также «Берсерк» и «Магическая битва».

После начала военных действий на Украине многие зарубежные партнеры заморозили сотрудничество с российскими издательствами. Так, продажу издателям из России лицензии на новые комиксы приостановила Marvel («Фантастическая четверка», «Люди Икс», «Мстители» и др.), при этом компания не отзывала лицензии, купленные до начала военной операции на Украине. Это привело к тому, что интерес аудитории сместился в сторону азиатских комиксов: японской манги, китайской маньхуа и корейской манхва, напоминает собеседник „Ъ“ на книжном рынке: «Издательства, отметив рост интереса к сегменту, начали активно наращивать его долю в портфелях».

В МИФ напомнили, что в прошлом году запустили две серии манхвы — «Магия вернувшегося должна быть особенной» и «Единственный конец злодейки — смерть». Первый тираж «Злодейки» разлетелся буквально за месяц, говорит госпожа Сиваева: «В этом году мы выпустили продолжение серии, в данный момент в продаже три тома, и четвертый совсем скоро выйдет». Она добавила, что компания также выпустила новеллу (первоисточник манхвы), ожидает выхода из печати второго тома. Суммарные тиражи серии, уточняет топ-менеджер, превысили 150 тыс. экземпляров. Кроме того, в издательстве с 2023 года выходят маньхуа и артбуки художников «Студии Мосспака» — команды художников, которые рисуют маньхуа. МИФ выпустил три книги от студии: «Фабрика Зозо», «Волк и найденыш» и артбук (издание, объединяющее изображения, иллюстрации и коллажи) художника Олд Сяня. «Совсем скоро ждем из печати комикс про лучших друзей „Нань Хао и Шан Фэн“»,— добавила госпожа Сиваева.

В издательстве также планируют выпустить в этом году комиксы «История о конфетах», «Тайная любовь» и два артбука от художников «Студии Мосспака». «В октябре в МИФе выйдет маньхуа „Немилая“ от популярного автора Zero. В Китае ее работу читает многомиллионная аудитория»,— добавила Анна Сиваева.

История рынка пиратской манги в России

Однако не только официальные издательства сейчас занимаются развитием азиатских комиксов. Растущий интерес к направлению привлек внимание и пиратских дистрибуторов, напоминают источники „Ъ“ на книжном рынке. На долю серого рынка приходится 5%, считает издатель Федор Еремеев (проект «Фабрика комиксов»): «В аниме-магазинах сейчас в принципе нет пиратской манги, хотя раньше ситуация была другой».

Первый официальный издатель азиатских комиксов, по его словам, появился в 2004 году в Москве. Компания называлась «Сакура-Пресс», сотрудничала с АСТ. Первым проектом издательства стал выпуск лицензированной манги «Ранма 1/2». До этого, в 1990-е годы, японская манга переводилась неофициально на русский и английский языки, после чего диски со сканами и адаптированными надписями в баллонах (графическое средство, используемое для иллюстрации речи либо мыслей персонажа) продавались на «Горбушке», уточняет господин Еремеев: «Азиатские проекты хорошо продавались в Москве, Санкт-Петербурге, Казани».

После появления на рынке «Сакура-Пресс» в Москве стали работать еще два-три пиратских издательства, занимавшихся адаптацией азиатских комиксов. «Они качественно выпускали нелегальную мангу хороших японских авторов, которые печатались в местных издательствах, с которыми трудно договариваться даже сейчас»,— отмечает Федор Еремеев. Упомянутые пиратские издательства выпустили примерно 10–15 наименований, в их числе был популярный проект «Тетрадь смерти», «Гот». В 2010 году к числу издателей азиатских комиксов присоединилась Украина, напоминает бизнесмен: «Местные представители не были знакомы с московскими издательствами, не участвовали в их правилах игры, а просто делали пиратские издания, продавали их в Россию. Несмотря на низкое качество, поток был большой».

Сегодня поклонники азиатских комиксов могут найти в сети новинки, еще не переведенные официальными издательствами. Одни из самых популярных сайтов среди русскоязычных сообществ — MangaLib, ReadManga, ReManga, уточняет собеседник „Ъ“ на книжном рынке: «Между сайтами и издательствами происходит вечная борьба: первые выкладывают тайтл, вторые требуют его удаления, как только появляется лицензия — и так по кругу». Из последних прецедентов: Studio Aiko, одна из команд неофициальных переводчиков, в сообществе во «ВКонтакте» объявила, что проекты «Архимаг, который вернулся» и «Принцесса со свалки» будут перенесены в другую группу «во избежание ненужных проблем». В другом крупном сообществе переводчиков „Ъ“ подтвердили, что команда не покупает права на перевод: «У нас флибустьерская деятельность, но при появлении лицензии мы всегда убираем все, что было сделано от лица нашей команды».

Не отстает и печатный формат: пираты покупают в Азии экземпляры или скачивают интернет-версии комиксов, снабжают их переводом из любительских групп в интернете, печатают в типографиях, а затем продают через маркетплейсы и классифайды, не заключая лицензионных договоров с иностранными правообладателями (см. „Ъ“ от 18 марта). Участники схемы экономят на лицензионных расходах и, как правило, плате за перевод. При этом цены у них доходят до 800–1000 руб. за экземпляр в мягкой обложке. В покупателях недостатка не ощущается, так как они получают либо еще не адаптированные официальными дистрибуторами издания, либо, наоборот, уже распроданные.

Цифровая справедливость

При этом азиатские проекты в цифровом формате можно найти не только на серых площадках. Входящая в МТС платформа «Строки» в августе открыла специальный раздел комиксов, до конца 2024 года планирует разместить там не менее 100 популярных графических произведений (см. „Ъ“ от 24 марта). Сервис «Яндекса» «Букмейт» в апреле также запустил специальный раздел от крупных и нишевых российских издательств, включая каталог Bubble Comics, а также комиксы от «Эксмо-АСТ», No Kidding Press, «Лайвбук», Clever. В «ЛитРесе» уже представлено 1,2 тыс. изданий, включая пособия по истории комиксов и их созданию.

Однако, утверждает собеседник „Ъ“ на издательском рынке, по темпам производства они значительно отстают от пиратов: «Пока издательство будет вести переговоры, русскоязычные команды оцифруют и переведут произведение». Так, по его словам, пиратам также помогают неофициальные англоязычные ресурсы, на которых можно найти сканы многих популярных тайтлов. Впрочем, считает собеседник, выходом могла бы послужить покупка уже вышеперечисленных ресурсов MangaLib, ReadManga, ReManga: «Пришлось бы очищать бОльшую часть их библиотеки, в частности удалять те тайтлы, на которые не приобретена лицензия, однако у платформ уже есть годами наработанная аудитория». Правообладатели, в свою очередь, в этом году начали активнее бороться с пиратскими ресурсами. Государственное южнокорейское агентство креативного контента (KOCCA) совместно с платформой Moi Comics готовят иск к русскоязычной ReManga за нарушение интеллектуальных прав (см. „Ъ“ от 25 сентября).

Юлия Юрасова

IT-компании рискуют перестраховаться

— регулирование —

с13 Но именно киберугрозы, такие как взломы, шифровальщики, фишинг или DDoS-атаки, становятся все более актуальными, рассуждает он.

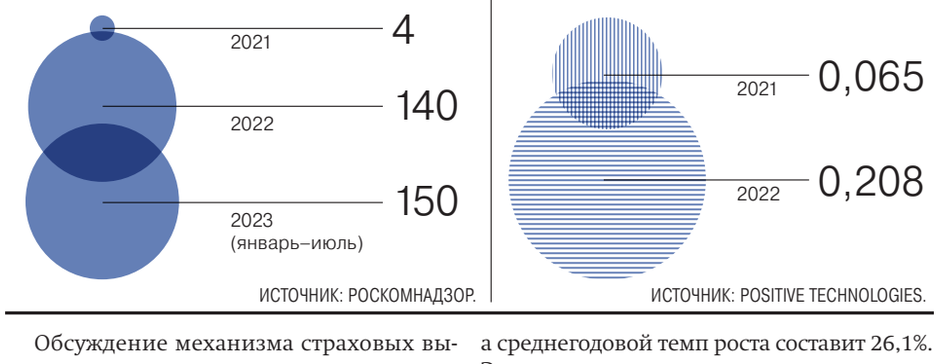
Директор компании Ideco Дмитрий Хомутов считает, что киберстрахование предназначено для компенсации финансовых затрат бизнеса из-за инцидента, связанного с нарушением кибербезопасности: покрытие расходов на юридическую и PR-помощь, компенсация клиентам и контрагентам, восстановление работоспособности информационной системы. Также оно сопровождается экспертной поддержкой — анализ уязвимостей, разработка регламентов противодействия и реагирования киберугрозам.

«Главное преимущество киберстрахования заключается в том, что оно предоставляет финансовую защиту в случае успешной кибератаки. Это особенно важно, если учесть масштабы возможных убытков от таких атак — например, когда из-за действий злоумышленников компания может потерять доступ к критическим данным или, что еще хуже, допустить утечку персональных данных клиентов»,— отмечает Кирилл Владимиров.

Повод задуматься

Интерес к страхованию компаний от угрозы и последствия кибератак бизнес начал проявлять с 2022 года, когда число атак на российскую IT-инфраструктуру резко возросло, а также участились случаи утечек персональных данных. Угроза остается ощутимой: общее число кибератак на российские компании в апреле—июне выросло почти в два раза, до 12,7 тыс. инцидентов, сообщали в МТС RED. Особенно активизировались хакеры в отношении IT-компаний: количество таких атак увеличилось вчетверо, до 4 тыс. По данным Positive Technologies, доля IT-компаний в общем числе атакованных почти утроилась и достигла 17% от всех жертв хакеров. В «Газинформсервисе» отмечали рост атак на IT-компании на 20–25%. При этом именно IT-организации реализуют в России программы импортозамещения и занимаются хранением и обработкой данных своих клиентов (см. „Ъ“ от 29 августа).

ДИНАМИКА УТЕЧЕК ДАННЫХ И КИБЕРАТАК В РОССИИ



Обсуждение механизма страховых выплат компаниям из-за утечек данных и других инцидентов появилось в контексте законопроекта об оборотных штрафах, который разрабатывается Минцифры, чтобы ужесточить работу с персональными данными любых компаний в России. Однако он пока так и не был внесен в Госдуму. В прошлом году в Минцифры сообщали „Ъ“, что рассматривают варианты механизма возмещения вреда субъектам персональных данных вследствие утечек, к которым «относится страхование операторов данных от указанных рисков». Как сообщал РБК, к июлю в правительстве закончили рассмотрение законопроекта, его финальная версия предусматривает максимальный штраф за утечку данных до 3% выручки компании.

По данным «Союз Страхования», спрос на покрытие киберрисков со стороны российских компаний за последние два года вырос более чем на 20%, а в течение следующих трех-пяти лет сегмент может вырасти до 8–10 млрд руб. В «АльфаСтраховании» отмечали, что из-за роста киберрисков спрос на такое страхование со стороны бизнеса стал «более предметным и осознанным».

Зарубежный опыт

По июльской оценке индийской консалтинговой компании MarketDigits, в 2023 году мировой рынок киберстрахования составляет $13,33 млрд, и аналитики прогнозируют, что к 2030-му он достигнет $84,62 млрд, а среднегодовой темп роста составит 26,1%. Эксперты считают, что стимулом роста направления стала пандемия COVID-19, которая ускорила цифровизацию бизнеса и вынудила организации перейти на удаленную работу, что привело к росту уязвимости IT-систем.

Сейчас же на желание компаний «перестраховаться» влияет продолжение роста кибератак и утечек данных. Например, пишут исследователи, в марте 2022 года хакеры украли криптовалюту почти на $540 млн из проекта блокчейна Ronin. Однако в других странах ситуацию видят иначе: согласно результатам недавнего исследования страховой компании QBE Insurance Group в Сингапуре, проводимого при участии малого и среднего бизнеса, 39% респондентов не рассматривают приобретение страховки от кибератак. Объясняют компании это тем, что не видят реальных угроз со стороны хакеров и не думают, что могут быть серьезно атакованы. К тому же 54% респондентов говорят, что не хранят конфиденциальные данные в интернете и, следовательно, не видят необходимости в киберстраховании.

Также среди сдерживающих факторов глобальные аналитические компании видят высокую стоимость страховых пакетов: ставки страховых взносов в целом выросли на 30%, а такие компании, как American International Group Inc., сокращают лимиты страхового покрытия по мере роста затрат, пишут аналитики MarketDigits. Кроме того, пока нигде нет единого стандарта, по которому было бы возможно сформировать страховое предложение. То есть как именно классифицировать те или иные потери компании из-за хакерской атаки, начиная от кражи конфиденциальных данных и заканчивая исками от пользователей сервисов, чьи данные оказались в сети.

Интерес к киберстрахованию за рубежом наступил после введения оборотных штрафов за утечку персональных данных, и не исключено, что с введением аналогичных законодательных мер в России услуги киберстрахования станут востребованными, считает гендиректор Security Vision Руслан Рахметов. Особенно среди компаний, обрабатывающих огромные массивы пользовательских данных, отмечает он: маркетплейсов, интернет-гигантов, банков, страховых и медицинских учреждений и т. д. Кроме того, субъектам критической инфраструктуры (КИИ, телеком, ТЭК и т. д.) также имеет смысл обратить внимание на киберстрахование, особенно с учетом тяжести потенциальных негативных последствий от кибератак на их объекты.

Киберстраховой пакет для российского рынка

По данным консалтинговой компании Kept по итогам 2022 года, рынок страхования в России в целом растет умеренными темпами: в среднем аналитики констатировали его рост на 2% в 2022 году и прогнозировали рост на 1% в 2023-м. Аналитики напоминали, что ухудшение макроэкономической ситуации в начале 2022 года сказалось на страховом рынке: сборы за первое полугодие 2022-го сократились на 3,6% относительно первой половины 2021-го. Но эксперты ожидают, что в 2023 году объем сборов страховых компаний составит 1,8 трлн руб.

Рынок страховых услуг в целом в первую очередь регулирует Банк России. В ЦБ „Ъ“ отметили, что создание нового института страхования киберрисков является одной из задач, определенных стратегическим документом Банка России «Основные направления развития информационной безопасности кредитно-финансовой сферы на 2023–2025 годы».

Однако, по мнению Банка России, для установления единых требований к такому страховому продукту страховщиками должен быть наработан достаточный опыт в этой сфере. Кроме того, до введения обязательного страхования киберрисков следует определить объект страхования, провести всестороннюю экономическую оценку целесообразности этого инструмента защиты интересов потребителей, а также проанализировать предполагаемый объем требований по возмещению вреда и расходов участников страхового рынка.

Артем Шейкин со своей стороны отмечает, что формирование правовых основ для создания ОКРУГа потребует изменений в налоговом законодательстве. Сейчас закон не разделяет ответственность за утечки персональных данных, содержащие, к примеру, ФИО и номер телефона, и утечки биометрических данных. Кроме того, говорит сенатор, предстоит создать институт оценки киберзащищенности с методикой проведения оценки, который позволит привлекать широкую экспертизу для оценки защищенности, но не отдельных уязвимостей, а возможности критических потерь путем кибератак.

Эксперты в области кибербезопасности также видят ряд нерешенных вопросов к инициативе. Киберстрахование — теоретически полезный инструмент, который позволит диверсифицировать риски цифровизации, а потому легче внедрять инновации, отмечает замгендиректора ГК «Гарда» Рустэм Хайретдинов. Но внедрение массового киберстрахования без четких, понятных всем методик оценки ущерба и определения виновных в этом ущербе натолкнется на всплеск страхового мошенничества или заградительных ставок.

Также, предупреждает он, обязательное страхование, не подкрепленное бизнес-смыслом, станет просто очередным налогом. По мнению ГК «Гарда», полезно будет начинать с малого, например страховать только ущерб от простоев или страховать компанию от штрафов, наложенных государственными органами: «Это позволит накопить статистику и наладить независимую оценку ущерба и методики выявления виновников инцидента».

Татьяна Исакова

информационные технологии

ФОНД СОДЕЙСТВИЯ ИННОВАЦИЯМ

Накладная заедет в цифру

С 2024 года транспортная накладная переходит в электронный формат: Минтранс рассматривает вариант, по которому его использование станет обязательным, и оценивает возможность отказа от классических бумажных документов при перевозке грузов. По оценке Strategy Partners, цифровую бизнес-модель сейчас активнее всего используют почтовые и курьерские сервисы (93%), ж/д-службы (92%) и пассажирские авиаперевозчики (81%). А в сфере грузовых автоперевозок — только 15% игроков рынка. Внедрение электронных транспортных накладных (ЭТрН) должно стимулировать процесс цифровизации этого сектора. „Ъ“ разбирался, что в следующем году изменится для логистических компаний и какие IT-решения для ЭТрН они уже могут использовать.

АЛЕКСАНДР КОРЯКОВ

— цифровизация —

Транспортная накладная — документ, который подтверждает факт перевозки груза автомобильным транспортом. Ее оформляют участники логистической цепочки для учета оказанных транспортных услуг и расчетов с перевозчиком. Электронные транспортные накладные — цифровой документ, подписанный усиленными квалифицированными или неквалифицированными электронными подписями всех участников взаимодействия, полный аналог бумажной версии, имеющий такую же юридическую значимость.

С февраля по октябрь 2020 года Минтранс проводил эксперимент по переводу транспортных накладных и путевых листов в цифровой формат. Отправители грузов, перевозчики и грузополучатели оформляли и подписывали документы через операторов электронного документооборота (ЭДО). А ГИБДД и Ространснадзор контролировали процесс через тестовую информационную систему. Эксперимент прошел успешно — новые механизмы взаимодействия участников перевозок друг с другом и с регуляторами оказались эффективными: сопутствующие доставке грузов процессы стали быстрее и дешевле, а также прозрачнее для государственных служб.

С 2021 года возможность использования ЭТрН последовательно закреплялась государством на законодательном уровне, до конца текущего года работа с ней добровольна. Но предполагается, что с 2024 года ЭТрН может стать обязательной — об этом говорил заместитель министра транспорта РФ Дмитрий Баканов, выступая в прошлом ноябре на форуме «Транспорт России». Однако пока нормативные документы, вводящие такое требование, не приняты.

Сейчас правительством утверждена форма электронной транспортной накладной: она должна содержать дату, время, адрес погрузки и выгрузки и другую информацию. Чтобы участники перевозки обменивались данными, а госорганы своевременно получали необходимые сведения, создана Государственная информационная система электронных перевозочных документов (ГИС ЭПД). Ответственным за нее назначен Минтранс. Из этой системы получают данные ГИБДД, Ространснадзор, ФНС и другие федеральные органы исполнительной власти.

Схема работы и потенциальные сложности

Информация по ЭТрН загружается в ГИС ЭПД не напрямую, а через аккредитованных Минтрансом операторов ЭДО, которые обеспечивают ее передачу в ГИС ЭПД (в таком случае может встречаться формулировка «операторы информационных систем электронных перевозочных документов, ИС ЭПД»). Сейчас они организуют роуминговые взаимодействия между собой, чтобы участникам логистической цепочки было удобно обмениваться документами в привычных им системах, не меняя операторов.

Грузоотправитель, перевозчик и грузополучатель должны подключиться к аккредитованным операторам ЭДО — это необходимое условие, поскольку если кто-то из «тройки» этого не сделает, сформировать ЭТрН не получится.

Обмен документами происходит в xml-формате. У сотрудников компаний, задействованных в процессе, должны быть подключенные к интернету устройства (у водителей — планшеты или смартфоны), чтобы подписывать документы простыми электронными подписями. «Если вдруг связь где-то отсутствует, вопрос решается отложенным выполнением действий в системе, то есть операция проводится, когда сигнал восстановится»,— объясняет руководитель отдела аналитики «Цитрос» Надежда Егорова.

При переходе на ЭТрН компания заключает договор с аккредитованным Минтрансом оператором ЭДО. При подключении к нему настраивается интеграция корпоративных информационных систем с сервисами ЭДО для загрузки и выгрузки транспортных накладных. Приобретаются сертификаты электронных подписей для сотрудников, если их нет. Затем заключается соглашение об обмене ЭТрН между контрагентами. Компаниям могут потребоваться доработки собственных информационных систем, чтобы отладить процесс и формировать ЭТрН. Поэтому начинать стоит с простых пилотных сценариев, а затем расширять опции, например учитывать возможную замену транспортных средств или водителей.

«Пока использование ЭТрН не является обязательным, и определенная доля игроков рынка не спешит переходить на электронные накладные. Скорее всего, введение ЭТрН будет поэтапным, например для отдельных видов товаров. Уже известно, что в 2024 году такой формат становится обязательным для алкогольной и спиртосодержащей продукции»,— отмечает Надежда Егорова. По словам эксперта, ЭТрН — один из самых сложных для внедрения форматов электронной документации, поскольку содержит много, как минимум четыре, титулов (составные части электронного документа, которые формируются по окончании какого-либо из этапов). «Каждая из задействованных в транспортировке грузов компания создает свою часть документа, из которых затем формируется ЭТрН, поэтому в процессе возможны организационные сложности»,— объясняют в компании «Цитрос».

Может быть трудно убедить контрагентов в необходимости использовать ЭТрН. Сейчас, объясняет Надежда Егорова, выгода от перехода на цифровые документы очевиднее именно транспортным компаниям, поскольку у них большие объемы таких накладных. «Часть игроков рынка грузоперевозок хотят перейти сразу на отлаженную систему, поэтому ждут, когда закончатся все тестовые периоды и она будет окончательно сформирована»,— добавляет эксперт.

Первопроходцы

Однако успешные кейсы уже есть. В мае текущего года компания X5 Group объявила о начале использования электронных транспортных накладных в ГИС ЭПД. Полностью отказаться от бумажных накладных ритейлер планирует к 2025 году. По собственной оценке X5 Group, внедрение ЭТрН позволит сэкономить более 30 млн руб. в год.

Также в мае мультисервисный оператор логистических услуг ПЭК сообщил, что запускает перевозки с электронными транспортными накладными. До конца года компания планирует перевести на ЭТрН 40% всех рейсов.

Пилотное внедрение ЭТрН в одной из крупных нефтяных компаний прошло с помощью решения «Цитрос ЮЗ ЭДО». «У заказчика работа происходит не в одной корпоративной информационной системе, а в нескольких. Они интегрируются с продуктом „Цитрос ЮЗ ЭДО“, который обеспечивает единую точку входа, что упрощает и унифицирует работу, а также позволяет эффективнее обеспечивать информационную безопасность,— поясняет Надежда Егорова.— При использовании „Цитрос ЮЗ ЭДО“ заметно повысилась скорость обмена и подписания документов: в среднем оформление бумажной транспортной накладной занимает до 10 минут, а в электронном виде — около минуты».

Переход на электронный документооборот на транспорте и подключение к операторам ЭДО — сложный технологический проект, сопряженный с перестройкой бизнес-процессов. Ведущие участники рынка начинают переход уже сейчас, чтобы неспешно отладить все механизмы.

Об этом говорит и начальник управления электронного документооборота ФНС России Федор Новиков: «Электронная транспортная накладная, пожалуй, самый сложный по структуре электронный документ. Тем важнее практика участия будущих потребителей в его разработке. Это дает возможность на самых ранних стадиях понять нюансы и начать готовиться к внедрению».

Преимущества и перспективы

Чем серьезнее у компании объемы документов, тем выше для нее экономический эффект от перехода на ЭДО. В случае с ЭТрН наиболее очевиден он на примере снижения затрат на обработку документов. По данным Минтранса, ежегодно оформляется около 3 млрд транспортных документов, каждая бумажная версия обходится компании-перевозчику примерно в 100 руб. Некоторые участники логистического сектора обозначают ее стоимость в 150–200 руб. Обработка же электронного документа, по оценке Минтранса, будет составлять примерно 5 руб.

«Другие преимущества: повышается скорость обмена документами, и можно отслеживать передвижения груза и статус транспортной накладной в режиме онлайн. Исключается ее потеря и сокращается кассовый разрыв, поэтому перевозчик может получить оплату в короткие сроки»,— добавляет Надежда Егорова. При формировании электронных версий меньше вероятность ошибок из-за человеческого фактора.

Отказ от бумаги в целом несет немало выгод компаниям, в их числе свободный доступ к документам с любого устройства, оперативные взаиморасчеты, сокращение затрат на доставку распечатанной документации, легкий и быстрый поиск нужных файлов в цифровом архиве. Кроме того, после внедрения ЭДО составлять документы будет намного проще — так же, как и редактировать их, передавать и подписывать. На все это потребуется несколько кликов. Переход на цифровой формат документа закроет и вопрос хранения транспортных накладных — ранее, чтобы соблюсти такой пятилетний срок, прописанный в законодательстве, некоторые участники рынка арендовали огромные склады. Теперь ЭТрН будет лежать в электронном архиве, и ее нельзя будет потерять.

Как отмечают сами участники рынка перевозок, переход на электронную транспортную накладную поможет повысить прозрачность отрасли. В государственной информационной системе будут отражены данные о перевозке, включая информацию о транспортном средстве, водителе, стоимости доставки и так далее. Доступ к ней в режиме реального времени появится и у автоинспекторов. Кроме того, с ГИС ЭПД могут работать и контрольно-надзорные органы, например ФНС, то есть перевозчикам не потребуется по запросам ведомства предоставлять документы на бумаге.

Самым эффективным стимулом для внедрения ЭТрН в ближайшее время может стать законодательное регулирование, однако пока норм, прописывающих обязательность ее использования, нет, напоминает Надежда Егорова: «Но сами рыночные условия будут способствовать спросу на решения для работы с ЭТрН, поскольку крупнейшие игроки уже переходят на цифровой формат». По данным «Контур.Логистики», в 2023 году количество запросов, связанных с ЭТрН, выросло вдвое по сравнению с прошлым годом. «Чем больше участников отрасли начинает ее использовать, тем быстрее и активнее идут все отладки и больше новых игроков начинают интересоваться процессом»,— объясняет Надежда Егорова.

Варианты внедрения

Операторы электронного документооборота, которые работают с транспортными перевозочными документами, уже сейчас предлагают интеграции с информационными системами компаний. Однако существуют и отдельные эффективные решения, которые упрощают взаимодействие с ними и обеспечивают одновременный обмен документами через нескольких операторов ЭДО: «Контур.Диадок», СБИС, «Такском» и др. В числе таких продуктов «Цитрос ЮЗ ЭДО» — система юридически значимого электронного документооборота, которая предоставляет заказчикам из коммерческих компаний и государственных организаций инструменты для автоматизации и упрощения процессов по обмену электронными юридически значимыми документами внутри холдинга и с контрагентами.

Коммерциализация продукта «Цитрос ЮЗ ЭДО» выполняется в рамках федерального проекта при поддержке Фонда содействия инновациям (федеральное государственное бюджетное учреждение «Фонд содействия развитию малых форм предприятий в научно-технической сфере»).

К основным преимуществам решения относится организация сквозного процесса юридически значимого ЭДО за счет интеграции с имеющимися информационными системами компании в одной точке, а также стандартизация процессов ЭДО в группах компаний.

Продукт базируется на открытом коде и входит в Единый реестр российского ПО Минцифры. «Цитрос ЮЗ ЭДО» создает доверенную среду обмена электронными документами в рамках компании или холдинга через внутреннего оператора, а с внешними контрагентами — через операторов ЭДО.

«Сейчас по ЭТрН у нас действует интеграция с двумя операторами ЭДО, если в компании настроен роуминг между операторами, то в „Цитрос ЮЗ ЭДО“ он также поддерживается. Если у заказчика большой объем данных, имеет смысл настроить прямой обмен, поскольку роуминг ЭДО пока не всегда обеспечивает стабильность передачи»,— отмечает Надежда Егорова. «Цитрос ЮЗ ЭДО», по ее словам, позволяет нивелировать такие риски.

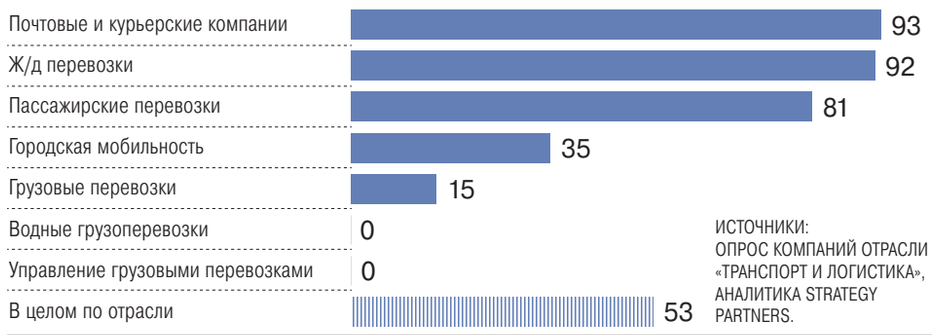
«Если контрагенты используют несколько операторов ЭДО, мы можем настроить автоматическую маршрутизацию. И тогда все документы не будут разбросаны по разным системам, а будут собираться в едином окне»,— добавляет эксперт.

Решение также обеспечивает высокий уровень информационной безопасности: внутренние ИС работают в защищенном внутреннем контуре компании. «Наш продукт разворачивается в инфраструктуре заказчика и обеспечивает единую точку взаимодействия с внешним контуром, и потенциальные риски в данном случае проще отследить»,— уточняет Надежда Егорова.

Компании могут заметно снизить трудозатраты с помощью «Цитрос ЮЗ ЭДО»: автоматизация процессов исключает дублирование операций сотрудниками, нет необходимости создавать и обрабатывать копии документов, нужные данные легко найти. Важный фактор — поддержка функциональности: система учитывает изменения в технологиях операторов ЭДО и законодательстве, оптимизирует затраты на сопровождение и модернизацию ЮЗ ЭДО. По опыту компании «Цитрос», внедрение решения позволяет значимо (до 70%) сократить время, затрачиваемое сотрудниками на обмен документами, а также на 30% снизить расходы, связанные с их обработкой.

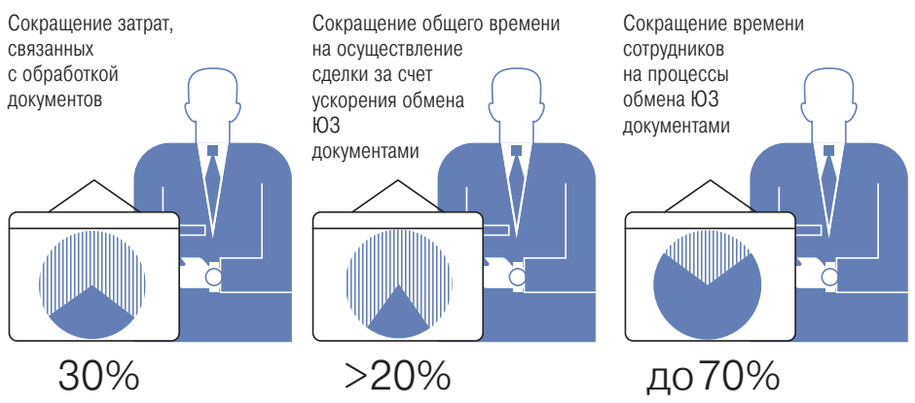
Матвей Соколов

ЭФФЕКТИВНАЯ ДОЛЯ СЕКТОРОВ ОТРАСЛИ ИСПОЛЬЗУЮЩИХ ЦИФРОВУЮ БИЗНЕС-МОДЕЛЬ (% КОМПАНИЙ В ОТРАСЛИ)



ИСТОЧНИКИ: ОПРОС КОМПАНИЙ ОТРАСЛИ «ТРАНСПОРТ И ЛОГИСТИКА», АНАЛИТИКА STRATEGY PARTNERS.

ВЫГОДЫ ОТ ВНЕДРЕНИЯ «ЦИТРОС ЮЗ ЭДО»*



*По опыту внедрения компании «Цитрос».

информационные технологии

Билборд узнает из тысячи

— технологии —

С13

В целом для использования в наружной рекламе подходят любые данные об аудитории с геолокационной составляющей, комментирует директор департамента наружной рекламы АДВ Людмила Сапронова: «MAC-адреса смартфонов, триангуляция местоположения абонента по вышкам сотовых операторов и геоданные из приложений на смартфонах. Эти данные позволяют оценить вероятность контакта с наружной рекламой и сформировать сегменты для сравнения (A/B-теста)».

Дополнительно к этим данным используются любые базы данных, которые можно соединить с этими сегментами и получить распределение по тем или иным действиям аудитории: покупки в приложении, CTA, посещение магазинов и другое, говорит она. Источниками этих данных, по ее словам, также выступают CRM-системы ритейлеров и компаний, СМС-чеки о покупке от мобильных операторов и некоторые ОФД-системы.

В основе исследовательских продуктов измерителя Admetrix, по словам гендиректора компании Ильи Шершукова, лежат данные на основе технологии GPS: «В их числе данные по объемам автомобильного и пешеходного трафика, данные о скоростях автомобильных потоков по дорожно-транспортной сети России». Характеристики аудитории, по его словам, собираются на основе геоданных, профиля потребления интернет-трафика, типов используемых устройств, покупок и т. д., а затем проходят несколько уровней проверки с помощью технологий Big Data.

GETTY IMAGES / ESCHOLLECTION

Wi-Fi аналитика уходит в прошлое

При этом данные о MAC-адресах пользователей, по словам участников рынка, уже не так актуальны, как несколько лет назад. Сильное влияние на потенциал использования WI-FI данных оказывает рандомизация MAC-адресов: автоматическая смена номера устройства при подключении к сети — производители устройств внедряют ее, чтобы защищать пользователей от случайного подключения к нежелательным Wi-Fi сетям. Это существенно тормозит сбор данных Wi-Fi снифферами.

«Инструменты планирования и отчетности на основе Wi-Fi аналитики начали активно развиваться для целей наружной рекламы шесть-семь лет назад. На сегодня данная технология охватывает лишь крайне малую долю рекламного инвентаря, например вообще не используется для классических (нецифровых) рекламных конструкций. И самое главное, Wi-Fi данные не отражают точную картину об объемах и составе аудитории ООН-конструкций»,— говорит Илья Шершуков.

Russ как оператор опирается на данные Admetrix в том, что касается медиаметрии и аудиторных измерений, говорит директор по развитию продуктов компании Павел Суржанский: «Внутри мы продолжаем собирать обезличенные идентификаторы мобильных устройств — MAC-адреса, то есть идентификаторы WI-FI модуля смартфона. WI-FI технологии используются в наружной и indoor-рекламе уже несколько лет и долгое время были успешны. Но сегодня мы видим, что с ростом внимания к защите персональных данных WI-FI технологии в ближайшем будущем потеряют актуальность для измерения аудитории»,— также отмечает он.

«Среди существующих сегодня технологий данные операторов связи представляются самыми перспективными: они непрерывно и стабильно собираются, репрезентируют население, их использование легко масштабировать при росте количества рекламного инвентаря»,— добавляет господин Суржанский.

Как используют анализ Big Data

Павел Суржанский выделяет три направления практического применения больших данных: «Первое — это измерение аудитории. Нам важно понимать средний объем аудитории перед каждым экраном и каждым щитом для каждого часа, а для программатик-закупки — для каждых пяти секунд».

Вторым направлением он называет планирование рекламных кампаний: «Мы используем анализ аудиторных данных для прогнозирования будущих периодов. Например, в сентябре нужно планировать кампанию следующего февраля. Для этого мы анализируем аналогичные прошлые периоды, исключаем аномалии». Данные телеком-операторов, данные крупных банков и ритейлеров, по его словам, также могут использоваться как дополнительный источник информации о местах преобладания целевой аудитория рекламодателя и тем самым позволяют более качественно подбирать адреса размещения рекламы.

Третье направление, по словам Павла Суржанского,— это измерение результата. «Большие данные позволяют сравнивать поведение для группы, которая могла видеть рекламу, и группы, которая рекламу, скорее всего, не видела. Это один из способов выделить вклад конкретного канала продвижения, в частности наружной рекламы»,— говорит он.

Big Data в целом позволяет создавать более эффективные и целевые рекламные кампании, проводить анализ эффективности наружной рекламы и улучшать таргетинг, обобщает Анастасия Сергеева. Демографические и географические данные, по ее словам, позволяют понимать, какие люди проходят мимо наружных рекламных дисплеев, настраивать контент и расписание рекламы для достижения максимального эффекта.

Таргетинг на билборде

Наружная реклама даже может использовать данные в реальном времени, такие как погодные условия, движение на дорогах, и корректировать контент, например продвигать горячие напитки в холодный день рядом с кофейней, отметила Анастасия Сергеева. Большие данные также позволяют создавать персонализированные наружные рекламные кампании, говорит она. Например, цифровой рекламный щит может отображать персонализированные сообщения для отдельных лиц на основе их предпочтений или предыдущих взаимодействий.

Big Data дает рекламодателям возможность выбора локаций, которые в большей степени соответствуют целевой аудитории: тепловые карты, показы в момент, когда концентрация нужной ЦА максимальна, добавила директор по закупкам наружной рекламы NMi Group Ирина Гусева: «Активно используется рекламодателями ретаргетинг в диджитал, за счет чего достигается либо увеличение частоты контактов, либо расширение охвата». «Для оценки эффективности используются инструменты Sales Lift, Brand Lift: они позволяют оценить то, как повлияла именно наружная реклама на покупку того или иного товара или узнаваемость бренда, соответственно оценить доходимость до торговой точки, конверсию в целевые действия»,— отметила она.

Глубокий анализ транспортных потоков по дням недели, по часам, по географическому принципу (по районам, округам, магистралям, группам конструкций) позволяет находить целевые аудитории, увеличивать охват, работать с частотой, говорит Людмила Сапронова. Данные о количественных характеристиках транспортных потоков, по словам Людмилы Сапроновой, позволяют моделировать различные подходы к планированию в pDOOH (программатические закупки): «При одном и том же бюджете pDOOH в сравнении с классическим размещением позволяет увеличивать охват на 14–20%».

Перспективы развития технологий

Компании—владельцы больших данных рассматривают их как ценный актив, но в бизнесе оператора наружной рекламы использование данных не приносит мгновенную дополнительную прибыль, признает Павел Суржанский: «Для оператора использование новых источников — это всегда инвестиция в развитие продуктов».

Сейчас у рынка нет полного понимания, будут ли оправданны вложенные в Big Data инвестиции, говорит Людмила Сапронова: «Мы видим проблематику, связанную с объемом данных и процентом метчинга: не всегда возможно получить статистически значимый результат, иногда сложно получить разнородные сегменты (где процент от тех, кто видел/не видел рекламу, значительно различается) для получения корректного результата при A/B-тестировании (маркетинговое исследование для определения наиболее эффективного продукта.— **„Ъ“**)»,— добавила она.

Сложно стыковать базы данных между собой, поскольку они могут быть созданы с использованием разных форматов данных, подтверждает Анастасия Сергеева: «Это может затруднить использование данных для целевого наружного маркетинга».

В Russ считают, что в перспективе будет расти спрос на измерения эффективности кампаний: «Измерение результата станет де-факто стандартом каждого размещения, каждого флайта. Это позволит превратить размещение рекламы ООН в постоянно действующую модель test and learn: корректировать медиапланирование, выбирать более удачные креативы». Запрос на работу с Big Data есть, в дальнейшем мы ожидаем еще большей доступности этих данных, добавила Людмила Сапронова.

Валерия Лебедева

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