ЖИТЬ ПО УМУ / 2
ЦИФРОВОЙ МАРКЕТИНГ УХОДИТ В МЕТАВСЕЛЕННУЮ / 3
ВКАЛЫВАЮТ РОБОТЫ — ВКАЛЫВАЕТ ЧЕЛОВЕК / 8

Цифровая экономика

Понедельник, 31 марта 2025
Тематическое приложение
к газете «Коммерсантъ» **№6**

Коммерсантъ
ONLINE

Guide



АЛЛА МИХЕЕНКО,
РЕДАКТОР GUIDE
«ЦИФРОВАЯ ЭКОНОМИКА»

КОММУНИКАЦИЯ НАЧИНАЕТСЯ С ИГРЫ

Сегодня повестка практически всех бизнес-конференций базируется на пяти главных тезисах: автоматизация, оптимизация, персонализация, омникальность и искусственный интеллект.

Большое значение бизнес придает коммуникации — как внутренней, ориентированной на мотивацию персонала, так и внешней, направленной на продвижения бренда, увеличение продаж, получение инвестиций. И гонка все больше напоминает игру.

Диджитал-рынок обрастает новыми механиками вовлечения: интегрированных коммуникаций стало больше, они транслируют ключевое послание через разные медиаформаты. Активно используются геймерские метавселенные, позволяющие установить глубокую связь с потребителями. Один из очевидных примеров — онлайн-площадка Roblox, где уже присутствуют игры от киностудий, телеканалов, точек питания, операторов. А геймеры примеряют скины от российских и международных брендов. При этом платформа стала антилидером по числу преступлений с начала 2025 года, по данным МВД РФ. Мошенники выманивают доступ к аккаунтам, совершают манипуляции с кибервалютой. Тем не менее в текущем году эксперты ожидают рост бюджетов на рекламные интеграции, коллаборации во вселенных.

Игрой кажется, когда нейросетка в образе амбассадора — известного героя ведет по «вселенной» компании, обучая персонал и общаясь с клиентами и партнерами.

Во главе бизнес-повестки стала кибербезопасность. Причем угрозы зачастую идут от персонала, который в попытке сгенерировать контент через нейросеть «сливает» секретные данные и разработки компании. Вывод — как бы чрезмерно не увлечься игрой.

↑
КОЛОНКА РЕДАКТОРА

ЖИТЬ ПО УМУ

ТЕХНОЛОГИИ «УМНОГО ДОМА»

ЗА ПОСЛЕДНИЕ НЕСКОЛЬКО ЛЕТ СТАЛИ ОБЯЗАТЕЛЬНЫМ АТРИБУТОМ ДЕВЕЛОПЕРСКИХ ПРОЕКТОВ, НАЙДЯ ПРИМЕНЕНИЕ ВО ВСЕХ СЕГМЕНТАХ И КЛАССАХ ЖИЛЬЯ В КРУПНЫХ РОССИЙСКИХ ГОРОДАХ. СРЕДИ СДЕРЖИВАЮЩИХ ФАКТОРОВ ПОВСЕМЕСТНОГО ВНЕДРЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В ДОМАХ РОССИЯН РАЗРАБОТЧИКИ ОТМЕЧАЮТ ОТСУТСТВИЕ ЕДИНЫХ СТАНДАРТОВ И ЗАВИСИМОСТЬ ОТ ИНОСТРАННЫХ ТЕХНОЛОГИЙ. ВАСИЛИСА МОТОВА

ДО ЧЕГО ТЕХНИКА ДОШЛА На мировом уровне в 2024 году «умные» технологии были внедрены в 27–29% домохозяйств. В России этот показатель составил около 9% с прогнозируемым ростом до 27% в ближайшие годы, рассказал Guide партнер конструкторского бюро «Элементум Лаб» Вадим Тымчик. «Это свидетельствует о растущем интересе к „умным" технологиям среди российских потребителей и застройщиков»,— говорит он.

По словам собственника холдинга SNDGlobal Ольги Квашенкиной, сегодня технологии «умного» дома охватывают широкий спектр решений, включая автоматизацию освещения, климат-контроля, безопасности, управления бытовой техникой, мультимедиа, а также энергосберегающие системы. Эти технологии часто базируются на протоколах связи, таких как Zigbee, Z-Wave, Bluetooth и Wi-Fi. «В более современных реализациях активно используется инфраструктура интернета вещей (IoT), что позволяет интегрировать устройства в единую экосистему, управляемую через централизованное ПО или приложения»,— объясняет эксперт.

Телекоммуникационные компании, такие как МТС и «Ростелеком», активно развивают инфраструктуру IoT, обеспечивая связь для устройств «умного дома». К 2022 году сети NB-IoT МТС охватывали более 90% потенциальных пользователей в 83 регионах России. Решения «Ростелекома» использовались почти в 2, 5 тыс. многоквартирных домов (МКД) России.

УСИЛЕНИЕ СТАНДАРТАМИ Несмотря на положительную динамику, существует ряд трудностей в разработке и внедрении технологий «умного дома». Господин Тымчик отмечает среди них отсутствие единых стандартов и зависимость от иностранных технологий. «До недавнего времени в России не существовало единых стандартов для систем „умного дома", что приводило к несовместимости устройств разных производителей и усложняло их интеграцию. Кроме этого, многие системы „умного дома" в России базировались на зарубежных технологиях и компонентах, что создавало риски в условиях геополитической нестабильности и санкций»,— перечисляет эксперт. Он добавляет, что сложностью в подключении и эксплуатации умных приборов, ограничивающей их массовое внедрение, является также недостаточная осведомленность потребителей.

Госпожа Квашенкина обращает внимание и на юридические риски интеграции «умных» систем в МКД. Внедрение требует согласований с управляющими компаниями и соответствия множеству нормативных документов. По ее мнению, низкие темпы импортозамещения в этой сфере связаны с неоднозначной потребностью на такие решения на рынке. «Многие компоненты, которые нужны для „умного дома" пригодятся и в других сегментах, но именно поэтому эти компоненты сперва идут на удовлетворение спроса электронной промышленности»,— поясняет эксперт.

Господин Тымчик обнадеживает, что сегодня в стране предпринимаются активные шаги для преодоления вышеперечисленных трудностей и продвижения импортозамещения. Так, с 1 февраля 2025 года в России вступили в силу новые ГОСТы, регламентирующие цифровизацию жилищно-коммунального хозяйства и внедрение цифровых технологий в многоквартирных домах. Эти стандарты устанавливают требования к базовому набору устройств и оборудования «умного дома», их совместимости и интеграции. Речь идет про национальный стандарт РФ ГОСТ Р 71199–2023 «Системы киберфизические. Умный дом. Термины и определения».



АЛЕКСАНДР КОРЯКОВ

ДЕВЕЛОПЕРЫ ЗАМЕЧАЮТ, ЧТО В ЖИЛЫХ ПРОЕКТАХ КОМФОРТ- И БИЗНЕС-КЛАССА АКТИВНО ВНЕДРЯЮТСЯ ОТДЕЛЬНЫЕ ФУНКЦИИ «УМНОГО ДОМА», КАСАЮЩИЕСЯ ВАЖНЫХ АСПЕКТОВ ЖИЗНИ: БЕЗОПАСНОСТИ, ПОТРЕБЛЕНИЯ РЕСУРСОВ И УСЛУГ СВЯЗИ

В части государственной поддержки и инвестиций в данную сферу эксперт отмечает прогнозы Минцифры РФ, оценивающего внедрение «умных» домофонов, камер, счетчиков и датчиков в 90 тыс. домов в 350 млрд рублей в течение двух с половиной лет начиная с третьего квартала 2023 года. «Это свидетельствует о серьезных намерениях государства в продвижении технологий „умного дома" и поддержке отечественных разработчиков»,— делает выводы господин Тымчик.

СТОЛИЧНЫЙ УРОВЕНЬ Большая часть проектов «умного дома» приходится на новостройки крупных городов, признают эксперты. В Москве и Санкт-Петербурге доля таких объектов в бизнес- и премиум-классах достигает 80%, что связано с конкуренцией среди застройщиков за потребителя. Однако, по оценке госпожи Квашенкиной, в регионах процесс диджитализации идет медленнее, что обусловлено меньшим числом крупных девелоперов, готовых вкладываться в «умные» технологии; отсутствием повсеместной высокоскоростной инфраструктуры для IoT; более низким спросом со стороны населения. В сегменте ИЖС технологии «умного дома» внедряются чаще, поскольку владельцы частных домов имеют больше свободы в выборе решений. Но уровень внедрения в частном секторе также зависит от доходов семьи и доступности специалистов.

ВЗГЛЯД ДЕВЕЛОПЕРОВ Девелоперы подтверждают, что сейчас в жилых проектах комфорт- и бизнес-классов активно внедряются отдельные функции «умного дома», они касаются обычно самых важных аспектов жизнедеятельности горожан: безопасности, потребления ресурсов и услуг связи. «В наших текущих проектах мы реализуем передовые системы контроля доступа (СКУД), IP-домофонию с распознаванием лиц, телеметрию для автоматического сбора данных о расходе ресурсов (включая отопление),— делится опытом Михаил Гущин, вице-президент по маркетингу и продукту группы RBI.— Это и есть разумная цифровизация: поэтапная минимизация участия человека в рутинных процессах».

По наблюдениям девелопера, массовое внедрение «умного дома» в глазах большинства покупателей пока не является острой необходимостью. Стоимость подобных систем тоже является пока сдерживающим фактором, уточняет господин Гущин.

Директор по продажам компании «Город-спутник Южный» Марина Потепкина согласна, что часто люди отказываются от диджитал-решений в новых квартирах, планируя самостоятельно укомплектовать квартиру. Потребители полагают, что, если взять готовое решение от застройщика, придется переплатить за лишние функции. «В первой очереди нашего проекта мы будем предлагать жителям базовую комплектацию „умного дома", которую можно будет „нарастить" в зависимости от потребностей. Мы недавно провели опрос и теперь понимаем, что именно интересно нашим будущим жителям»,— пояснила подход компании госпожа Потепкина.

По ее данным, сегодня каждый четвертый житель Петербурга хотел бы жить в квартире с системой «умный дом». Наиболее востребованные функции: «умные» счетчики, которые автоматически передают данные тепло- и водоснабжения в управляющую компанию (65% голосов), видеодомофоны (53%), «умные» розетки и система защиты от протечки с блокировкой подачи воды (по 46%). Значительная часть опрошенных также выразила интерес к датчикам движения, для бесконтактного включения света, и датчикам температуры и влажности. При этом многие петербуржцы уже пользуются отдельными «умными» устройствами: «умные» счетчики есть у 64% опрошенных, видеодомофоны — у 50%, а «умные» лампочки — у 40%.

Ян Фельдман, директор по маркетингу ГК «Ленстройтрест», тоже говорит, что в части цифровизации продукта в компании ориентируются на ожидания клиентов. «Границы между классами жилья стираются все больше, и если раньше цифровые опции были прерогативой недвижимости высоких сегментов, то теперь они активно распространяются и на комфорт-класс»,— констатирует эксперт. В целом автоматизация и цифровизация будут все сильнее проникать в проекты застройщиков. «К примеру, технологии ИИ будут активнее применяться для анализа и сбора данных, в частности, это позволит „умным" системам распознавать „своих" жителей для их свободного передвижения в границах жилого квартала: автоматически открывать перед ними двери, доставлять на нужный этаж, определять их предпочтения в повседневной жизни»,— обозначает перспективы господин Фельдман.

Евгений Бескровный, коммерческий директор LAR Development, убежден, что некоторые опции «умного дома» стали неотъемлемыми атрибутами качественной жилой среды и их отсутствие сегодня будет восприниматься как существенный минус даже покупателем в сегменте масс-маркета. ■

ЦИФРОВОЙ МАРКЕТИНГ УХОДИТ В МЕТАВСЕЛЕННУЮ

МАРКЕТИНГОВЫЙ ЛАНДШАФТ В ПОСЛЕДНЕЕ ВРЕМЯ ПРЕТЕРПЕВАЕТ СИЛЬНЫЕ ИЗМЕНЕНИЯ. ЭТОМУ СПОСОБСТВУЕТ ПОЯВЛЕНИЕ НОВЫХ ТЕХНОЛОГИЙ. СЕГОДНЯ НЕЙРОСЕТИ ПО СОЗДАНИЮ РАЗНЫХ ФОРМАТОВ КОНТЕНТА (ОТ ТЕКСТОВОГО ДО ВИДЕОПРЕЗЕНТАЦИЙ), ЧАТ-БОТЫ, ML-ТЕХНОЛОГИИ ЗНАЧИТЕЛЬНО ПОВЫШАЮТ СКОРОСТЬ ПОДГОТОВКИ И КАЧЕСТВО РЕКЛАМНЫХ КАМПАНИЙ. ВНЕДРЯЮТСЯ ЭЛЕМЕНТЫ ГЕЙМИФИКАЦИИ, ПРИМЕНЯЕТСЯ СТРАТЕГИЯ ОМНИКАНАЛЬНОСТИ. СМЕЩАЕТСЯ И САМО ВНИМАНИЕ С ТРАДИЦИОННЫХ РЕКЛАМНЫХ МОДЕЛЕЙ НА БОЛЕЕ ЧЕЛОВЕКОЦЕНТРИЧНЫЕ ПОДХОДЫ. ОДНАКО ПРИ РАБОТЕ С НОВЫМИ ТЕХНОЛОГИЯМИ СЛЕДУЕТ УЧИТЫВАТЬ ОПРЕДЕЛЕННЫЕ НЮАНСЫ, ПРЕДУПРЕЖДАЮТ ОПРОШЕННЫЕ GUIDE ЭКСПЕРТЫ И ИГРОКИ РЫНКА. АЛИСА МАЛЬЦЕВА

Сегодня основной запрос бизнеса при выстраивании маркетинговых стратегий — не только охват и вовлечение новой аудитории, но и ее удержание. Именно поэтому компании активно экспериментируют с новыми площадками и форматами взаимодействия.

«По нашей статистике, 70% пользователей считают удобной коммуникацию с брендами через мессенджеры, а подключение WhatsApp, Telegram и VK позволяет увеличить продажи в среднем на 20% и более. Сегодня в маркетинговые коммуникации встроены мессенджеры. С их помощью можно делать рекламные рассылки, консультировать пользователей, закрывать сделки, оказывать послепродажную поддержку»,— рассказывает бизнес-партнер в IT-компании edna Александр Дубровин. Он привел в пример страховую компания «СогазМед», которая в прошлом году начала использовать сервис VK Notify и через него отправляет информацию по полисному обеспечению. В целом, по словам игроков рынка, это сегодня популярный инструмент.

«Все чаще компании перераспределяют свои бюджеты с „Яндекс.Директа“ и VK Ads на более эффективную рекламу в Telegram, посевы в профильных ТГ-каналах и поисковую оптимизацию сайтов»,— обращает внимание Александр Осипов, директор по маркетингу Arenadata. Спикер добавляет, что в ходу проверенные временем инструменты: email-marketing, SMM, видео, PPC, SEO. «В стандартный список задач по повышению эффективности канала в 2024 году добавились задачи по строгому соответствию законодательству РФ. В частности, нам пришлось почистить базу email-подписчиков, провести ее переподписку. Согласно новым правилам, если компания отправила человеку письмо, но не выполнила все требования по сбору персональных данных, она может получить штраф в размере более 500 тыс. рублей за каждое письмо. Поэтому 2024 год для нас стал годом не новых инструментов, а повышения эффективности текущих со строгим соблюдением законов»,— отмечает господин Осипов.

Артур Саркисян, CEO Calltouch, обращает внимание, что сегодня важно создавать удобную экосистему: «Омниканальность — это не просто „быть везде“, а делать так, чтобы человек чувствовал себя одинаково комфортно на сайте, в соцсетях, в мессенджерах и даже в офлайн-точках».

«За последние пару лет цифровой маркетинг перестал быть просто продвижением в соцсетях и контекстной рекламой. Сегодня мы видим синтез разных каналов — от традиционного SMM до комплексных омниканальных стратегий, где офлайн и онлайн сплетаются воедино. Крупные бренды все активнее инвестируют в технологии ИИ, чтобы персонализировать рекламные сообщения и повышать конверсию. AI-алгоритмы помогают бизнесу прогнозировать, кто именно из покупателей готов сделать покупку, и «подкручивать» предложение в нужный момент»,— комментирует директор по маркетингу «Додо Пицца» Михаил Чернышев.



FREEPIK

ПО ДАННЫМ АКАР, В 2024 ГОДУ НЕЙРОСЕТИ ИСПОЛЬЗОВАЛИ В СВОЕЙ РАБОТЕ 97% РЕКЛАМНЫХ АГЕНТСТВ, ЕЩЕ 55% ПРИМЕНЯЛИ СОБСТВЕННЫЕ РАЗРАБОТКИ НА ОСНОВЕ ИИ

НЕЙРОСЕТЬ И «УМНЫЕ» АЛГОРИТМЫ

На первый план в маркетинге выходят «умные» алгоритмы и автоматизация. Пользователи все больше ждут от брендов персонализированного подхода, хотят больше взаимодействия и вовлеченности. С этой точки зрения бизнес обращает внимание на решения на основе ИИ, интегрированные с CRM-системами. Например, в чат-центре большие языковые модели (LLM) используются для работы чат-ботов.

Ирина Абдураимова, управляющий директор по маркетингу Vesna («дочка» «ЭТП Газпромбанка»), отмечает, что использование нейросетей собственной разработки и других известных разработчиков способствовали повышению производительности на 20%. «Мы используем Perplexity Deep Research и Claude (для анализа рынка и конкурентов, трендвотчинга), Stable Dissusion (для генерации видео и гифок), Flux и Midjourney (для генерации визуалов)»,— поделилась спикер.

Свой кейс привел Артем Чернов, предприниматель, управляющий партнер по цифровизации GloraX: «Клиент из фэшн-ритейла внедрил систему, которая анализирует не только то, что покупал человек, но и на что он смотрел, сколько времени проводил на странице, в какое время суток, с какого устройства. В итоге конверсия выросла на 18% — и это без увеличения рекламного бюджета. При этом многие компании у нас до сих пор не могут нормально настроить A/B-тестирование и думают, что „большие данные“ — это когда у тебя Excel подвисает от количества строк. Разрыв между технологическими лидерами и середняками растет».

«Цифровой маркетинг в 2025 году, сочетая AI, Web3, автоматизацию и гиперперсонализацию, становится невидимым: реклама вшивается в пользовательский опыт. Метавселенные и NFT пока что удел крупных игроков, а малый бизнес, при внедрении ИИ для анализа данных, выигрывает за счет скорости и гибкости в нишевых каналах»,— комментирует Александр Вайс, разработчик и аналитик WEB3Bureau, член комиссии по ЦФА ТПП РФ и РСПП РФ.

ОТ КОНТЕНТА ДО ЦИФРОВЫХ АВАТАРОВ

Как рассказала Мария Мухина, вице-президент по маркетингу компании «Объединенные пивоварни», технологиями на основе ИИ компания пользуется с прошлого года. В частности, InsightChat — платформой для автоматизации Discovery-исследований. «ИИ-ассистент Мария проводит личные интервью в формате чата с респондентами. Опрос быстро формируется на основе простых промптов для ИИ, а на выходе получается отчет с текстовыми выводами, которые дополняет количественная оцифровка данных»,— поясняет алгоритм спикер.

Кроме того, в компании широко используются инструменты для внутренних коммуникаций: цифровые аватары, помогающие в обучении и рассказывающие о продукте; нейросети Midjourney, Sora для создания видео о продукте и его позиционировании.

«Сейчас ИИ начинают применять не для создания вау-эффекта (летающие сумки или гигантские пушистые магазины), а для выполнения конкретных задач. Например, вместо многомиллионных затрат на живые съемки можно генерировать реалистичные изображения и видео, которые практически неотличимы от реальных. Одними из первых этот подход начали применять модные бренды, создавая моделей, которых невозможно было отличить от реальных людей. За ними последовали и другие крупные компании. Наша команда дизайнеров также активно использует ИИ для сайта и других коммуникаций»,— рассказывает Людмила Боголепова, начальник департамента маркетинга подписки «Газпром Бонус».

На метамаркетинг обращает внимание Александр Кадыкеев, представитель агентства Jami Lup.

«Метавселенные в 2025 году — это полноценные медиаэкосистемы, где пользователи взаимодействуют с брендами через игровой процесс, что делает вовлечение гораздо глубже, чем в традиционной рекламе. Например, наш кейс для „Союзмультфильма“: благодаря активации в Roblox мы увеличили лояльность на 131% и вовлеченность на 8%, а просмотры мультсериала „Простоквашино“ выросли на 40%. Roblox стал полноценным бренд-активом — после успешного запуска мира „Простоквашино“ были созданы миры „Ну, погоди!“ и „Петя и Волк“, в которых выходят регулярные обновления. Вся мультвселенная за год привлекла 8,5 млн посещений, став для бренда новым каналом для построения долгосрочных отношений с аудиторией»,— рассказывает спикер.

Еще один кейс был реализован для Sela: была разработана концепция AR-эффектов для детской коллекции футболок, ее интегрировали на платформе Letary, создали игровое пространство в Roblox и разработали визуальные материалы (изображения и ролики), в том числе — с помощью ИИ. Для продвижения диджиталколлекции и мира в Roblox использовались интеграции блогеров. «Так мы реализовали омниканальную стратегию, объединив традиционные (соцсети, инфлюенс-маркетинг) каналы с метавселенными для создания единой точки контакта с пользователем»,— подытожил господин Кадыкеев.

НО ЕСТЬ НЮАНСЫ

Маркетинг окончательно превратится в инженерную дисциплину, замечает Артем Чернов, управляющий партнер по цифровизации GloraX. По его словам, в будущем будут востребованы не креативщики с «огоньком в глазах», а маркетологи-технологи, умеющие выстраивать сложные воронки, анализировать терабайты данных и автоматизировать процессы.

«При этом не стоит забывать про человеческий фактор. В погоне за технологиями многие бренды теряют эмоциональную связь с аудиторией. Технологии должны усиливать эмоциональный эффект, а не заменять его»,— отмечает эксперт.

«Критический анализ и перепроверка информации человеком приобретают гораздо большее значение, чем ранее. Более того, нейросети значительно увеличили объем создаваемой информации, что потенциально может привести к перенасыщению восприятия людей, что, как следствие, может открыть дорогу совершенно новым форматам в маркетинге»,— предупреждает директор по развитию платформы «СберТаргет» ООО «Сбер Бизнес Софт» Андрей Обухов. ■

«ЕСЛИ НАМ ВАЖНЫ ИНФОРМБЕЗОПАСНОСТЬ И ТЕХНОЛОГИЧЕСКОЕ РАЗВИТИЕ В ОБЛАСТИ ТИМ, ТО ОБ ИСПОЛЬЗОВАНИИ ИНОСТРАННЫХ РЕШЕНИЙ НУЖНО ЗАБЫТЬ»

РОССИЙСКАЯ СТРОИТЕЛЬНАЯ ОТРАСЛЬ НАЧАЛА ПЕРЕХОДИТЬ НА ОТЕЧЕСТВЕННЫЕ ТЕХНОЛОГИИ ИНФОРМАЦИОННОГО МОДЕЛИРОВАНИЯ ЗАДОЛГО ДО УХОДА ИЗ СТРАНЫ ЗАРУБЕЖНЫХ ВЕНДОРОВ. ПОЭТОМУ ДАЖЕ ПРИ УСЛОВИИ ИХ ГИПОТЕТИЧЕСКОГО ВОЗВРАЩЕНИЯ РАССТАНОВКА СИЛ НА РЫНКЕ ВРЯД ЛИ ИЗМЕНИТСЯ, СЧИТАЕТ ЗАМЕСТИТЕЛЬ ГЕНДИРЕКТОРА ПО НАУЧНОЙ ДЕЯТЕЛЬНОСТИ АО «СИСОФТ ДЕВЕЛОПМЕНТ», ГЛАВА КОМИТЕТА ПО ИНФОРМАЦИОННОМУ МОДЕЛИРОВАНИЮ АРПП «ОТЕЧЕСТВЕННЫЙ СОФТ» МИХАИЛ БОЧАРОВ. О ТОМ, КАКИЕ ШАГИ НЕОБХОДИМО ПРЕДПРИНЯТЬ ДЛЯ УСКОРЕНИЯ ПРОЦЕССА ИМПОРТОЗАМЕЩЕНИЯ ИНОСТРАННОГО ПО, О ВАЖНОСТИ ИНТЕГРАЦИИ В СТРОИТЕЛЬНУЮ ЦИФРОВУЮ ВЕРТИКАЛЬ И О ПРИОРИТЕТНЫХ НАПРАВЛЕНИЯХ РАЗВИТИЯ КОМПАНИИ ОН РАССКАЗАЛ В ИНТЕРВЬЮ GUIDE. ПАВЕЛ ИЛЬИН



АО «СИСОФТ ДЕВЕЛОПМЕНТ»

GUIDE: Что сегодня является драйвером развития технологий информационного моделирования (ТИМ) в России, а что — сдерживающими факторами?

МИХАИЛ БОЧАРОВ: Основной драйвер — это действующие нормативные-правовые требования, связанные с формированием новых смыслов информационного моделирования и интеграцией отечественных программных решений в государственные информационные системы, в частности в строительную цифровую вертикаль. С этой стороны мы ощущаем заинтересованность и поддержку государства для ускорения темпов импортозамещения зарубежного ПО. Но для более эффективной господдержки в строительной отрасли отечественных технологий информационного моделирования, разумеется, необходимо еще многое сделать. Ведь информационное моделирование применяется сегодня не только крупными предприятиями и девелоперами, работающими с масштабными проектами и госзаказами, но и небольшими компаниями и региональными проектными бюро. Причем ТИМ применяют в различном функциональном наполнении практически во всех субъектах страны. Чтобы это понять, как раз и нужна классификация, ведь информационная модель позволяет сделать управление данными удобным. И, может быть, не везде и не во всем нужно использовать трехмерную графику. Зачем усугублять положение внедрения цифровизации абсурдными требованиями?

Напомню, что с 1 января 2025 года формирование и ведение информационной модели стали обязательными при любом новом строительстве, что, очевидно, окажет на отрасль значительное влияние. Притом что ТИМ во многом очень выгоден с экономической точки зрения, но нужно удержаться от перегибов и излишней зарегулированности процессов, особенно под западные стандарты,— это приведет к срыву цифровизации и откату к устаревшим принципам OpenBIM.

Что касается сдерживающих факторов, то они, как ни парадоксально, также кроются в нормативной базе, а точнее, связаны с хаосом нормативно-технических документов. К сожалению, многие технические стандарты, которые ранее были заложены в отрасли, основаны на западных решениях. И они порой содержат взаимоисключающие понятия и определения, которые противоречат нормативно-правовым актам. Но я рассчитываю, что в ближайшем будущем эти коллизии удастся преодолеть, хотя очень заметно лоббирование интересов (форматов и моделей данных) от западных вендоров через действующие регламенты. Цифровая вертикаль и новые принципы управления данными требуют уже другого, открытого или бесшовного доступа к данным, а нам подменяют понятия, предлагая вместо нормальной открытости данных — «открытый» формат IFC. Страна должна развиваться так, как удобно и выгодно нам, не копируя ошибки западного BIM, а конкуренция должна быть честной.

Мы сейчас не просто замещаем западные решения — мы делаем это лучше. А нас тянут назад форматами и стандартами, да иногда и просто голословными заявлениями, мол, все отечественное — плохое и дорогое.

Помимо нормативно-технической базы, переход на отечественные решения сдерживает и финансовый аспект. Для множества предприятий в нашей стране оперативное импортозамещение сопряжено с высокими — в рамках их экономической модели — затратами. С нашей точки зрения, сегодня в России необходимо разработать механизм так называемого бюджетного кешбэка. Идея такова: российский разработчик ПО ТИМ продает программные продукты компаниям со скидкой, а она впоследствии возмещается

АО «СиСофт Девелопмент» — ведущий российский разработчик программного обеспечения для рынка САПР в области машиностроения, промышленного и гражданского строительства, архитектурного проектирования, землеустройства, электронного документооборота.

государством самому разработчику через налоговые льготы или бюджетные субсидии. Причем размер скидки может варьироваться в зависимости от отраслевой принадлежности покупателя программных решений. Так, если речь идет, например, о муниципальных и районных объектах, которые будет проектировать небольшое региональное бюро, работающее на госзаказе, то скидка может составлять и 90%, почему нет? Так или иначе, это экономия для бюджета. А если ПО приобретают компании из более высокомаржинальных сфер, скажем, представители крупных девелоперов, то скидка может быть меньше, например, 50%. То есть важно дать рынку возможность преодолеть финансовый порог перехода.

G: Над какими программными решениями сегодня работает «СиСофт Девелопмент»? Каковы приоритетные направления для развития?

М. Б.: Наша компания внесла значительный вклад в развитие технологий информационного моделирования в России, и сегодня «СиСофт Девелопмент» занимает на рынке лидирующее место в области бесшовных ТИМ-решений для всего жизненного периода информационной модели. На данный момент мы обладаем самой большой бесшовной линейкой по формированию, а главное, ведению информационной модели: начиная от изысканий и заканчивая архивным хранением. Мы продолжаем укреплять позиции в традиционных для себя нишах, расширяя сферы применения наших программных решений. Они становятся более универсальными и удобными для пользователя. Таким образом, в настоящее время мы являемся лидерами рынка в области проектирования и сейчас активно «заходим» в сферы строительства и эксплуатации.

Надо понимать, что международные BIM-лидеры занимаются общемировыми проблемами BIM. Рынок ТИМ в России идет своим путем, и прошло то время, когда он формировался под западные решения и продукты. Мы уже другие, и требования нашего рынка тоже меняются, поэтому они не будут локализовывать и подстраивать свои продукты под региональные рынки, в частности под российский (который они еще наверняка надеются вернуть под их стандарты и форматы). Западные вендоры сами понимают тупиковость своего подхода и также ищут решения. Поэтому расчет простой: пока разрабатываются новые продукты, держать нас на старых, чтобы исключить уход из-под контроля. Именно поэтому развитие цифровой вертикали и создание бесшовной интероперабельности во всех направлениях — это сегодня задача и для отечественных разработчиков, и для отечественной науки, которой пока нет и которую не заменят разнообразные центры компетенций, действующие каждый по своему разумению.

G: В каком положении оказались отечественные предприятия после ухода зарубежных вендоров?

М. Б.: Сложно сказать однозначно, потому что разные предприятия оказались в разном положении. Те, кто заранее начал процесс перехода — еще до введения санкций,— сегодня чувствуют себя лучше. На них уход зарубежных вендоров оказал меньшее влияние. Те, кто с этим опоздал, находятся в ситуации, когда приходится быстро принимать дорогостоящие и ресурсозатратные решения. А некоторые и вовсе до сих пор ждут возвращения западных вендоров. Это тоже позиция, но, на мой взгляд, не совсем правильная.

G: Как вы полагаете, возвращение в страну западных вендоров положительно отразится на рынке? Как это скажется на вас?

М. Б.: В первую очередь хочется отметить, что компания «СиСофт Девелопмент» была заметным игроком на рынке ТИМ и успешно конкурировала с решениями от Autodesk еще в то время, когда американский вендор работал в России и имел здесь свое представительство. Мы конкурировали и с ним, и с AVEVA, и с Bentley Systems. Поэтому их гипотетическое возвращение на нашем бизнесе никак не скажется. И не только потому, что мы сформировали качественную и понятную пользователям линейку программных решений, но и потому, что ситуация в нашей стране серьезно поменялась. Так, за последние годы был принят ряд документов, главный из которых — указ президента РФ № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». Очевидно, что для множества российских предприятий и компаний использование западного ПО является очень рискованным и токсичным. И речь здесь идет не только о безопасности информации и ее возможной передаче вовне. Кто может гарантировать, что в определенный момент не повторится ситуация, при которой лицензии западных вендоров перестанут работать? А это может сказаться на сотнях и тысячах аффилированных с огромными корпорациями компаниях, деятельность которых влияет на экономику страны. То есть здесь уже налицо отсутствие доверия. Подчеркну, что самое главное сегодня — это понятная, четкая и последовательная политика государства по отношению к зарубежному ПО. Если нам важна информационная безопасность, то об использовании иностранных решений нужно забыть раз и навсегда.

G: Как изменились цены на отечественные решения за последние годы?

М. Б.: Если мы говорим о нашей линейке Model Studio CS, то она состоит из нескольких программных решений, или комплектов ТИМ: для проектирования строительных решений, трубопроводов, водоснабжения и канализации, вентиляции, электрики и так далее. Таким образом, потребитель может собрать свой собственный набор ТИМ под его нужды — и ничего лишнего не будет входить в его цифровую экосистему, например, для конкретных проектных работ. При этом цены на наши продукты из линейки за последние три года хотя и возросли, но они росли ниже уровня инфляции. За других коллег по отрасли говорить не хочу, но в «СиСофт Девелопмент» ситуация такова.

G: Сталкивается ли ваша компания с дефицитом кадров в сфере разработки?

М. Б.: Дефицит присутствует, но не могу сказать, что мы его сильно ощущаем. Конечно же, нам нужны квалифицированные кадры, поэтому мы на постоянной основе пополняем ряды наших разработчиков. Гораздо более важный аспект — дефицит кадров в тех сферах и отраслях, где работают пользователи наших программных решений. Причем здесь речь идет не только о проектировщиках, которые формируют информационную модель, но и о тех, кто ее впоследствии будет «вести». Приведу пример. Есть два глагола: «формировать» и «вести». «Формировать» — это значит создавать саму модель, собирать двухмерную и трехмерную графику, добавлять в модель атрибутивные данные. А «вести» — это когда в атрибутивные данные уже вносятся изменения. Например, проектировщиком предусмотрена стена, которая оштукатуривается и красится. При строительстве в модель важно внести дополнительные данные о том, какой бригадой выложена кирпичная стена, когда и какой кирпич пришел на стройплощадку и с какого завода, кто штукатурил и кто красил (и какой краской). Здесь происходит распределение обязанностей по ведению информационной модели. Точно, что каменщик, штукатур или маляр не будет вносить эти данные, а может сообщить их, например, нормировщику, а он внесет их в модель. Это будет дешевле и серьезно оптимизирует необходимые ТИМ-квалификации по ведению модели на этапе строительства. И дефицит ТИМ-специалистов на рынке будет намного меньше.

G: Как вы оцениваете подготовку студентов в вузах по направлению ТИМ?

М. Б.: Я оцениваю ее как недостаточную. Отечественные разработчики ПО ТИМ проводят огромную работу для внедрения своего ПО в программы обучения в российских вузах. Например, предоставляют бесплатные лицензии, помогают с разработкой учебных программ и курсов. Но проблема в том, что теоретическая часть в вузах устарела, а в ее основе лежат западные решения и стандарты. И наша нормативная база, как я уже говорил ранее, противоречивая и не позволяет создать научную основу информационного моделирования. Практическую часть мы «закрываем», показываем наши решения, учим, как на них работать. Но студент — строитель, инженер, архитектор — должен знать и теоретическую основу. Таким образом, сегодня образование в сфере ТИМ в России — это птица с одним крылом, «практическим», но без второго, «теоретического». Так она далеко не улетит. ■

НОВЫЙ ВИТОК ЩИТА И МЕЧА

ОСНОВНЫМИ УГРОЗАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В 2025 ГОДУ ОСТАЮТСЯ РОСТ ЧИСЛА КИБЕРАТАК, В ТОМ ЧИСЛЕ СВЯЗАННЫХ С ХАКТИВИЗМОМ, ВИРУСЫ-ВЫМОГАТЕЛИ, ФИШИНГОВЫЕ АТАКИ И МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ, АТАКИ НА ЦЕПОЧКИ ПОСТАВОК ЧЕРЕЗ СКОМПРОМЕТИРОВАННЫХ ПОДРЯДЧИКОВ, ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ, УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И АТАКИ НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. ДВОЙСТВЕННОЕ ВЛИЯНИЕ НА КИБЕРБЕЗОПАСНОСТЬ ОКАЗЫВАЕТ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ. АЛИСА МАЛЬЦЕВА

УДАР ПО КИИ Мониторинг RED Security показал, что в прошлом году было совершено 130 тыс. киберинцедентов, что в 2,5 раза больше, чем в 2023 году. Наибольшее количество кибератак приходится на отрасли критической информационной инфраструктуры (КИИ), включая промышленность, финансовый сектор и телекоммуникации.

«Удаленный доступ к системам управления объектами КИИ, террористические кибератаки на производственные цепочки — все это обратная сторона динамичной эволюции цифрового мира. В настоящее время в нашей стране наблюдается переломный этап, когда масштабы киберугроз осознаны на государственном уровне и закрывать на них глаза не представляется возможным. Начинаются тектонические процессы»,— комментирует управляющий директор по ИБ АО «Росатом автоматизированные системы управления» Евгений Дорофеев.

Эксперт прогнозирует дальнейший рост волны кибератак на объекты КИИ, особенно в крупной промышленности и энергетике. При этом «ахиллесовой пятой» в этих отраслях остается проблема импортозамещения. «Импортное ПО несет в себе риски. В условиях санкций утрачивается возможность его обновления и техподдержки. В отсутствие оригинальных ремкомплектов и запчастей для аппаратной составляющей, а также, при использовании „серого“ импорта гарантийное и сервисное обслуживание становятся недоступны. По мере увеличения доли непроверенного ПО и ПАК разных производителей и поколений усложняется IT-ландшафт, растет неоднородность комплексов и систем ИБ. Возрастает уязвимость и существенно снижается эффективность таких систем. Пристальное внимание на комплексное обновление ПО и ПАК — это первый шаг на пути к суверенитету в киберсреде»,— говорит господин Дорофеев.

В ТРЕНДЕ АТАК Представитель «Информзащиты» Александр Матвеев обращает внимание на увеличение числа деструктивных атак, нацеленных на разрушение информационной инфраструктуры без получения финансовой выгоды. И если в первой половине 2024 года такие атаки осуществляли хактивисты (политически мотивированные, но не всегда профессиональные хакеры), то теперь — профессиональные группировки, хактивистские сообщества. На хактивизм обращает внимание и Антон Антропов, технический директор IT Task.

Также господин Матвеев указывает, что в прошлом году сложился тренд на атаки через третьи стороны, которыми чаще всего выступали подрядчики компаний и партнеры, имеющие доступ к информационной системе компании. «Хакеры начали атаковывать организации с более низким уровнем информационной безопасности, чтобы проникнуть в инфраструктуры жертвы через существующие каналы. Таких атак будет еще больше в 2025 году, мы ожидаем рост как минимум на 50–60%. В-третьих, в этом году вырастет число атак с вымогательством. 59% ИБ-руководителей считают именно их главной угрозой для бизнеса в текущем году. Главной причиной роста количества таких атак является распространение RaaS-платформ — сервисов для злоумышленников, где они могут купить лицензию или получить подписку на вредоносное ПО для ransomware-атак. Мы ожидаем, что количество атак через такие платформы увеличится на 15% в 2025 году»,— рассуждает господин Матвеев.

Согласно исследованиям аналитиков компании «Бастион», свыше 60% успешных кибератак заканчивается утечками данных. «Один из главных факторов, позволяющих злоумышленникам вести свою деятельность,— уязвимость приложений. 85% пентестов заканчивается практически полным захватом контроля над сетью компаний»,— подчеркивает Дмитрий Калинин, руководитель департамента по работе с уязвимостями и инцидентами компании.

«Бизнесу необходимо укреплять защиту сетевого периметра, внедрять сертифицированное ПО (особенно компаниям, работающим с критической инфраструктурой), компонентный анализ (SBOM) для обеспечения прозрачности цепочек поставок, интегрировать инструменты безопасности на уровне JDK, серверов приложений и ОС, автоматизировать процессы безопасности и интегрировать их в цикл разработки ПО (DevSecOps), а также применять средства защиты от социальной инженерии, анализирующие подлинность изображений, видео и аудио»,— советует Алексей Рубаков, основатель компании Netrack. ➔ 6



АЛЕКСАНДР МИРИДОНОВ

УВЕЛИЧЕНИЕ УТЕЧЕК БАЗ ДАННЫХ И АТАК ПРОГРАММ-ВЫМОГАТЕЛЕЙ СТАНОВИТСЯ ВСЕ БОЛЕЕ СЕРЬЕЗНОЙ ПРОБЛЕМОЙ ДЛЯ БИЗНЕСА

5 → **В КОНТЕКСТЕ AI** К новым вызовам кибермошенничества опрошенные Guide эксперты относят активное использование AI. «Уже есть новая матрица атак с использованием AI (MITRE Atlas), которую необходимо изучить экспертам в области ИБ для построения проактивных механизмов противодействия угрозам. Решения, основанные на AI для средств защиты, будут использоваться и командами защитников. Возникает новый виток щита и меча»,— акцентирует Дмитрий Узлов, руководитель отдела ИБ «Мобиус Технологии».

Развитие AI-технологий существенно снижает порог входа в «хакерскую сферу»: ее стало гораздо проще организовать, да и обходится она дешевле, говорит бэкенд-разработчик Филипп Щербанич. «Причем речь не только о серьезных взломщиках систем, но и о так называемых скрипт-кидди — людях, которые о взломе знают очень мало, но умеют пользоваться специальными готовыми программами. А AI-решения становятся для них одновременно и учебником, и инструктором по взлому»,— говорит IT-эксперт. Вместе с тем растет и количество инструментов для противостояния атакам. И это тоже происходит благодаря AI: например, уже есть системы, которые анализируют поведение сотрудников, и благодаря им можно предупредить попытку дипфейк-атаки.

Основные AI-угрозы в 2025 году будут по-прежнему связаны с фишингом. «В этом плане AI-инструменты очень полезны хакерам: многие работают удаленно, и их можно относительно легко обмануть, притворившись другим человеком (с помощью подделки аудио или видео). Собеседник уверен, что говорит с родственником, знакомым или начальником, но на „другом конце провода“ — мошенник. Для этого используются технологии дипфейка — с их помощью добываются важные доступы, пароли, секретная информация. Кроме этого, большие языковые модели применяют для имитации сообщений какого-нибудь человека: это тоже может быть очень актуально при фишинговых атаках. Тут злоумышленникам открываются серьезные возможности автоматизации данного процесса»,— рассказывает господин Щербанич.

Руководитель группы защиты инфраструктурных IT-решений «Газинформсервис» Сергей Полунин заострил внимание на доверие к информации: «С помощью ИИ можно изготовить фейковые документ, видео и аудио практический любой сложности. Проблема эта появилась довольно давно, но именно в связи с успехами того же ChatGPT, Gemini, Grok и подобных, она рискует вырасти до очень серьезных размеров».

КОНТУРЫ ЗАЩИТЫ До 2022 года основным источником утечек данных считались действия сотрудников, но затем ситуация изменилась — на первый план вышли внешние угрозы. «Однако в 2024 году вновь произошел рост инцидентов, связанных с внутренними нарушителями, включая умышленные утечки. Поэтому отдавать приоритет защиты внутреннего или внешнего контуров недостаточно, важно разрабатывать комплексную стратегию»,— отмечает генеральный директор «Эвритег» Сергей Тимошенко.

Кроме того, границы между внутренним и внешним контурами защиты размываются из-за облачных сервисов и удаленной работы. «Защита требуется на всех уровнях: от личных устройств до серверов. Приоритетом становится контроль внутреннего контура, так как ему традиционно доверяют больше, а угрозы изнутри (например, вредоносное ПО на устройствах сотрудников) могут быть более опасными. Основным трендом становится внедрение систем классов Endpoint Protection, DLP, возможно с элементами ИИ»,— отмечает Андрей Малов, директор по продукту «ТТК.Облако».

В целом перспективным подходом в контексте защиты по внутреннему контуру становится модель Zero Trust, предполагающая, что любая попытка доступа к данным проверяется вне зависимости от доверенного статуса пользователя, то есть даже если запрос исходит от администратора.

КОГДА УГРОЗА — СОТРУДНИК Человеческий фактор остается самой большой проблемой. «Почти 90% кибератак происходят из-за невнимательности или незнания сотрудников. Без регулярного обучения люди продолжают кликать по фишинговым ссылкам, использовать слабые пароли и передавать данные третьим лицам. Поэтому обучение должно быть не формальностью, а обязательным элементом безопасности»,— предупреждает генеральный директор компании «Фрикейк» Виталий Панов.

«По незнанию люди могут спросить у того же ChatGPT, насколько хороша та или иная идея, запросить оценку ее потенциала, генерацию новых идей на основе уже разработанных. Так может произойти утечка и раскрытие данных. Также известны случаи, когда работники компаний „скармливали“ для быстрой аналитики ИИ ряд секретных документов. В сеть спокойно просачивались те данные, которые должны были оставаться конфиденциальыми. Поэтому вопрос именно цифровой грамотности и безопасности сегодня ключевой»,— подчеркивает основатель холдинга The Business Pill Игорь Малинин.

Причем, даже если человек понял и принял все рекомендации, в стрессовой ситуации он будет действовать на эмоциях. «Именно на этом строится большинство атак. Фишинговые письма всегда провоцируют эмоциональный отклик, подавляя логическое мышление. Сочетание грамотного объяснения, мотивации и постоянной практики позволяет превратить сотрудников из главной уязвимости в надежный элемент системы защиты»,— подытожил специалист ГК Softline Николай Постнов. ■

В ПОЛЕ ЗАЩИТЫ ОТ КИБЕРРИСКОВ

КИБЕРСТРАХОВАНИЕ В РОССИИ ПОКА ОСТАЕТСЯ СЛАБО РАСПРОСТРАНЕННЫМ, КОНСТАТИРУЮТ ОПРОШЕННЫЕ GUIDE АНАЛИТИКИ И ИГРОКИ РЫНКА. СРЕДИ ОПАСЕНИЙ ОТНОСИТЕЛЬНО ДАННОГО ПРОДУКТА БИЗНЕС НАЗЫВАЕТ ВЫСОКУЮ СТОИМОСТЬ ПОЛИСОВ, НЕПРОЗРАЧНЫЕ УСЛОВИЯ ДОГОВОРОВ, ТРУДНОСТИ В ДОКАЗЫВАНИИ ИНЦИДЕНТА И ПОЛУЧЕНИИ СТРАХОВЫХ ПРЕМИЙ. ОДНАКО С РОСТОМ ЧИСЛА УГРОЗ ИНТЕРЕС К СЕГМЕНТУ БУДЕТ РАСТИ, УВЕРЕНЫ ЭКСПЕРТЫ. ТАКЖЕ В БЛИЖАЙШИЕ ГОДЫ СТРАХОВЩИКИ НАЧНУТ ПРЕДЛАГАТЬ БОЛЕЕ ГИБКИЕ И ДОСТУПНЫЕ РЕШЕНИЯ, АДАПТИРОВАННЫЕ ПОД БИЗНЕС РАЗНОГО УРОВНЯ. АЛЛА МИХЕЕНКО



ОЛЕГ ХАРСЕЕВ

РОСТ ЧИСЛА АТАК И УСИЛЕНИЕ РЕГУЛЯТОРНЫХ НОРМ ПОДТОЛКНУТ БОЛЬШЕ КОМПАНИЙ К ИСПОЛЬЗОВАНИЮ ИБ-СТРАХОВАНИЯ КАК ЧАСТИ СТРАТЕГИИ ЗАЩИТЫ

По данным страхового брокера Mainsgroup, представившего исследование рынка страхования киберрисков в начале марта 2025 года, данный сегмент еще недостаточно развит: всего 8 из 15 страховщиков России предоставляют услугу по киберстрахованию, а количество договоров насчитывает около полутора тысяч — от мелких «коробочных» решений до стандартных полисов с полноценным покрытием.

Согласно открытым данным, услуги по страхованию киберрисков предоставляют АО «Альфастрахование», СПАО «Ингосстрах», АО «Согаз», «СберСтрахование», «Зетта Страхование» и др. Опрос Mainsgroup показал низкую активность бизнеса в таком гаранте безопасности. Всего 12,5% опрошенных (в исследовании участвовало 37 представителей страховых компаний, страховых брокеров и страхователей) застраховали киберриски.

«Это услуга не сильно популярна в России,— констатирует руководитель группы защиты инфраструктурных IT-решений компании «Газинформсервис» Сергей Полунин.— Да, первые предложения появились уже в 2017 году на волне атак шифровальщиков WannaCry и Petya, но с тех пор спрос на эту услугу если и рос, то крайне слабо. В основном отношение организаций не то чтобы было скептическим, но бюджет на это точно мало у кого был предусмотрен».

По словам эксперта, сейчас эта услуга востребована в IT и финансовом секторе, остальные все же полагаются на технические способы защиты и не пытаются переносить риски таким способом.

«В России 13–14% компаний имеют киберстраховку»,— приводит свою статистику директор Центра мониторинга и противодействия кибератакам IZ:SOC компании «Информзащита» Александр Матвеев. Одним из факторов низкой популярности, по мнению спикера, является страх компаний сообщать о случившемся инциденте ИБ из-за репутационных потерь. «Другой фактор состоит в том, что страховка не может защитить от инцидента, не всегда покрывает потери, не позволяет решить задачу минимизации последствий. Поэтому популярность услуги остается низкой»,— рассуждает он.

Эксперты отмечают, что с учетом роста кибератак логично, что запрос на данную услугу будет увеличиваться. Вопрос только в том, насколько сильно.

В «СберСтраховании» посчитали, что за три квартала прошлого года услугу по страхованию киберрисков оформили более 100 юрлиц, что в два раза больше в сравнении год к году. А сумма вложений компаний составила 4 млрд рублей, что в три раза больше, чем за аналогичный период прошлого года. Всего за семь лет «СберСтрахование» обеспечило страховую защиту от киберрисков более чем 9 тыс. компаний. Программы киберстрахования помогают бизнесу справиться с последствиями действий злоумышленников в киберпространстве, уверены в «СберСтраховании». Предприятиям МСБ достаточно страховой суммы от 10 до 50 млн рублей, чтобы защититься от основных рисков. А для холдингов и крупного бизнеса составляются индивидуальные андеррайтинги.

ДОПОЛНИТЕЛЬНЫЙ СТИМУЛ К 2025 году ожидается, что главным трендом в киберстраховании станет интеграция с ожесточающимися нормативными требованиями, обращает внимание директор Ideco Дмитрий Хомутов. «Рост числа атак и усиление регуляторных норм подтолкнут больше компаний к использованию ИБ-страхования как части стратегии защиты»,— думает эксперт.

Данную тенденцию выделяет и Дмитрий Калинин, руководитель департамента по работе с уязвимостями и инцидентами ИБ компании «Бастион». «С увеличением числа и сложности кибератак растет и интерес к киберстрахованию. На этом фоне страховые компании расширяют спектр услуг, в том числе завлекая потенциальных клиентов применением AI-технологий в своих решениях. Все больше руководителей задумываются об информационной безопасности, изучают инструменты управления киберрисками, среди которых встречают киберстрахование. Кроме того, усиление регуляторного контроля и введение новых требований к защите данных стимулируют компании обращаться к страховщикам»,— делится эксперт.

УГРОЗЫ БУДУТ РАСТИ По прогнозам экспертов, 2025 год станет годом эскалации киберугроз: количество атак продолжит расти, а хакерские группировки расширят свою деятельность, выбирая в качестве целей не только госструктуры, но и частный бизнес. Согласно аналитическому отчету о реагировании на инциденты в 2024 году от команды «Лаборатории Касперского» (GERT, отчет опубликован 20 марта 2025 года), в минувшем году большинство запросов поступило от промпредприятий, тогда как госучреждения подвергались атакам реже, чем в 2023-м. «Мы также зафиксировали рост числа инцидентов, связанных с транспортной отраслью: количество запросов на услуги реагирования удвоилось по сравнению с 2023 годом»,— отмечают в «Лаборатории Касперского».

Среди популярных киберинцидентов 2024 года там называют атаки с использованием шифровальщиков (их число за 2024 год увеличилось на 8,3 п. п. по сравнению с 2023 годом и составило 41,6% от общего числа инцидентов). По оценкам экспертов, тренд сохранится и в следующем году шифровальщики останутся главной угрозой для организаций по всему миру. Также сохраняется тенденция утечек данных, являющейся второй по частоте причиной запросов на реагирование на инциденты, составляя 16,9% от всех случаев.

«Киберстрахование становится необходимым инструментом для компаний всех отраслей в условиях растущего числа кибератак»,— считает господин Хомутов. Он напомнил, что в 2023 году общий объем страховых премий в сфере киберстрахования в России увеличился на 20%, достигнув примерно 900 млн рублей. В целом, по мнению эксперта, страховки помогают минимизировать финансовые потери, сохранить репутацию, обеспечить соответствие нормативным требованиям и восстановить бизнес с минимальными затратами.

ОПАСЕНИЯ БИЗНЕСА Среди основных причин неиспользования услуг по киберстрахованию игроки рынка отмечают высокую стоимость полисов. «Основная проблема тут в том, что подобное страхование стоит немалых денег: компании-страховщики сами перестраховываются и завышают цены на услуги, так как оценить все риски очень и очень сложно, особенно когда появляется столько решений, позволяющим злоумышленникам взламывать системы быстрее и дешевле. Кроме того, есть и сложности с возмещением потерь, так как требуется сначала проводить дорогостоящие расследования»,— говорит бэкенд-разработчик Филипп Щербанич.

Компании также сомневаются в страховом покрытии и недостаточно информированы о политике и практике поставщиков таких услуг. «Условия страхования не всегда прозрачны»,— обращает внимание гендиректор компании «Фрикейк» Виталий Панов.

«Я считаю, что проблема заключается в том, что источник ущерба трудно доказать. А посчитать выплату еще труднее. Высока вероятность отказа, так что понятнее пустить страховую премию на реальные защитные меры»,— указывает технический директор IT Task Антон Антропов.

Заместитель генерального директора ГК «Гарда» Рустэм Хайретдинов поясняет: «До сих пор нет независимого арбитража и практики экспертизы при расследовании инцидентов. Непонятно, как доказывать вину (страховая компания заинтересована обвинить клиента в нарушении правил страховки и не платить при первой возможности) и потери (потерявший считает застрахованные потери огромными, страховая старается их занизить). Также нужны инструменты сбора данных, аналог авиационного „черного ящика“, к которому никто не имеет доступа и который вскрывается во время расследования инцидента,— и таким инструментам должны доверять все стороны и суд. Пока данных не будет накоплено достаточно и пока нет понятных инструментов и институтов принятия решения, никто не будет страховать ущерб, а лишь, как сегодня, стоимость средств защиты».

Валентин Поляков, владелец продукта «Антивирус» в компании PRO32, рассказал, что несколько лет назад компания пробовала запустить этот продукт, но инициатива не увенчалась успехом. «Даже если все условия соблюдены, есть вероятность, что страховая выплата может не покрыть тот ущерб, который был нанесен бизнесу в случае утери критически важных данных. Так бывает, например, если организация пострадала от нацеленной атаки при помощи вируса-шифратора»,— рассказывает господин Поляков.

При этом многие игроки рынка все же считают, что необходимо применять страховку наравне с другими мерами киберзащиты. «2025 год принесет новые вызовы в сфере кибербезопасности. Компании должны внедрять комплексные меры защиты, повышать осведомленность сотрудников и учитывать риски, связанные с новыми технологиями. Только так можно эффективно противостоять современным киберугрозам»,— агитирует бизнес-партнер компании «Компьютерные технологии» Павел Карасев. ■

ВКАЛЫВАЮТ РОБОТЫ — ВКАЛЫВАЕТ ЧЕЛОВЕК

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В МЕДИЦИНЕ — НЕ ФУТУРОЛОГИЯ, А РЕАЛЬНЫЙ ИНСТРУМЕНТ, КОТОРЫЙ ПОМОГАЕТ КАК МЕДРАБОТНИКАМ ПЕРВИЧНОГО ЗВЕНА, ТАК И ВРАЧАМ, ОКАЗЫВАЮЩИМ ВЫСОКОТЕХНОЛОГИЧНУЮ ПОМОЧЬ. ТЕХНОЛОГИИ УЖЕ ИСПОЛЬЗУЮТСЯ ПРИ ПРОВЕДЕНИИ ОПЕРАЦИЙ, СНИЖАЯ РИСКИ ХИРУРГИЧЕСКИХ ОШИБОК, МИНИМИЗИРУЯ ТРАВМАТИЧНОСТЬ И СОКРАЩАЯ ВРЕМЯ НА ВОССТАНОВЛЕНИЕ ПАЦИЕНТОВ НА 20–30%. В ПРОШЛОМ ГОДУ БОЛЬШАЯ ЯЗЫКОВАЯ МОДЕЛЬ УСПЕШНО СДАЛА ЭКЗАМЕН НА ВРАЧА ОБЩЕЙ ПРАКТИКИ. СТАНУТ ЛИ ПОМОЩНИКИ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ В ПЕРСПЕКТИВЕ ПОЛНОЦЕННЫМИ ВРАЧАМИ, РАЗБИРАЛСЯ GUIDE. КСЕНИЯ АХМЕТЖАНОВА

НЕЙРОСЕТЬ ПОШЛА УЧИТЬСЯ Год назад важный шаг в развитии помощников с искусственным интеллектом в Петербурге сделала большая языковая модель «Сбера» GigaChat. Одной из первых в мире она сдала экзамен высшего медучреждения по направлению подготовки «Лечебное дело», получив за него «четверку». Экзамен принимала комиссия из профессоров Института медицинского образования НМИЦ им. Алмазова, специалисты этого же учреждения занимаются обучением робота. Как заметили члены комиссии, если бы все студенты обладали такой базой знаний, удовлетворенность системой здравоохранения в нашей стране была бы выше.

К этому же проекту присоединился Первый мед (ПСПбГМУ им. Павлова). В рамках ПМЭФ-2024 вуз подписал соглашение со «Сбером» о сотрудничестве по обучению GigaChat.

Сейчас обучением большой языковой модели занимаются как минимум триста специалистов. Как рассказали Guide в НМИЦ им. Алмазова, нейросеть сдала экзамен на врача общей практики и получает постдипломное образование. Кроме того, ее готовят по отдельным медицинским сценариям и по решению узкоспециализированных вопросов.

«В идеале эта модель должна стать полноценным членом врачебной команды, помощником врачей, пациентов и организаторов здравоохранения,— прокомментировал заместитель гендиректора по информационным технологиям и проектному управлению НМИЦ им. Алмазова Дмитрий Курапеев.— У нас расписан план работ по созданию прикладных решений до конца 2026 года».

Задача ИИ, как отмечают эксперты, не вытеснять человека с его рабочего места, а быть помощником. Нейросети можно передать обработку больших объемов данных, применять ее для точности диагностики и полноты всей клинической картины.

ЭФФЕКТИВНЫЕ МАНИПУЛЯЦИИ Цифровые технологии давно помогают в операционных. Так, в клинической больнице Святителя Луки в Петербурге оборудовали шесть современных интегрированных операционных. Они оснащены медицинской системой визуализации, благодаря чему врачи могут следить за ходом операции в прямом эфире, консультировать и давать советы коллегам.

Уже несколько лет в петербургских операционных помогает робот Da Vinci. Он выводит изображение операционного поля на мониторы в формате 3D, а также фиксирует хирургические материалы, которые используют врачи. Это исключает риск забытой салфетки или иглы в теле пациента.

Осенью 2023 года с помощью Da Vinci провели операцию на сердце в Центре им. Алмазова. Там удалили доброкачественную опухоль сердца крупных размеров у 29-летнего петербуржца. Тогда врачи смогли обойтись без стернотомии (рассечения грудины). Операцию провели через небольшие разрезы, которые обеспечивали доступ роботических портов и инструментов ассистента.

В конечном итоге применение роботических технологий в хирургии позволяет минимизировать травмирование мягких тканей и скелета пациента. «Такие системы снижают риски хирургических ошибок, минимизируют травматичность и сокращают время на восстановление пациентов на 20–30%»,— добавляет директор по развитию «Тегратек» Артем Ищук.



ЕВГЕНИЙ ПАВЛЕНКО

НЕЙРОСЕТИ МОЖНО ПЕРЕДАТЬ ОБРАБОТКУ БОЛЬШИХ ОБЪЕМОВ ДАННЫХ, ПРИМЕНЯТЬ ЕЕ ДЛЯ ТОЧНОСТИ ДИАГНОСТИКИ И ПОЛНОТЫ ВСЕЙ КЛИНИЧЕСКОЙ КАРТИНЫ

А ПОГОВОРИТЬ? Как полагает директор департамента голосовых цифровых технологий компании BSS Александр Крушинский, генеративные нейросети, большие языковые модели (LLM), технология RAG в обслуживании клиентов в медицинских центрах приобретут более массовый характер в горизонте двух-трех лет. Пока же многие опрошенные Guide медцентры либо не прибегают к помощи нейросетей, либо нагружают их рутинными задачами.

Так, в «СМ-Клинике» с 2019 года на звонки клиентов «на первой линии» отвечает голосовой помощник Надежда. Работает она по типу Виктории из городской службы 122: напоминает пациентам о скором приеме в клинике, предоставляет контактную информацию и консультирует по услугам, задает уточняющие вопросы, а затем перенаправляет человека на «профильный» сегмент контакт-центра, который занимается записью по конкретным направлениям и к специалистам.

«Надежду разработали специально под наши задачи. Важное техническое преимущество системы — адаптивность и большой выбор настроек. Мы можем самостоятельно прописывать для робота сценарии работы, менять скрипты, добавлять новые функции,— рассказывает медицинский директор «СМ-Клиники» в Санкт-Петербурге Сергей Пониделко.— Решение удобное и серьезно экономит ресурсы клиники. Пациентопоток у нас ежегодно растет в среднем на 20%, а вместе с ним увеличивается и нагрузка на контакт-центр. При текущем уровне загрузки только на „первую линию“ нам бы потребовалось не менее 20 диспетчеров за смену, то есть всего 40 сотрудников. Сегодня их всех заменяет голосовой помощник».

Только с прошлого года клиника стала интегрировать ИИ непосредственно во врачебную практику. Сейчас робот в формате пилотного проекта анализирует данные КТ-диагностики. Так, за время проведения проекта с помощью системы удалось обработать около 1,5 млн КТ-исследований.

«Технология распознает даже незначительные изменения в костной ткани, органах дыхания, сердце, сосудах и других системах организма. После завершения проверки врач получает отдельный протокол с клиническими рекомендациями, которые специалисты также могут использовать в подготовке медицинского заключения»,— добавил господин Пониделко.

ВЫСОКАЯ ТОЧНОСТЬ Важным преимуществом ИИ эксперты называют его способность проводить диагностику. Так, например, системы компьютерного зрения в радиологии анализируют рентгеновские снимки и КТ с точностью до 97%, что помогает обнаруживать онкологические и сердечно-сосудистые заболевания задолго до появления выраженных симптомов.

«ИИ анализирует данные о пациенте: генетические особенности, образ жизни, историю болезней — и на их основе создает индивидуальные схемы лечения. В онкологии, например, такие подходы уже помогли повысить эффективность терапии на 35%. Мы движемся к тому, что лечение станет не универсальным, а подстроенным под конкретного человека»,— говорит господин Ищук.

Для скорости и точности диагностики нейросети используют и в Ленинградской областной клинической больнице. Тут ИИ выступает в роли помощника врачей-рентгенологов. К примеру, после маммографического исследования снимок передается в онлайн-архив, а искусственный интеллект анализирует его, выявляя подозрительные области и оценивая их в соответствии с современной классификацией BI-RADS. Это позволяет сопоставлять результаты и получать дополнительную информацию для постановки диагноза. ИИ также может делать разметку на маммограмме, выделяя доброкачественные или злокачественные новообразования.

«Важно понимать, что ИИ — это инструмент, а не замена специалиста. Как и любой помощник, он может допускать ошибки, поэтому врачи-рентгенологи всегда принимают окончательное решение на основе комплексного анализа»,— подчеркивает заместитель главного врача по диагностике, главный внештатный специалист по лучевой и инструментальной диагностике Ленобласти Петр Калинин.

В современной стоматологии ИИ применяют для анализа рентгеновских снимков и прогнозирования результатов лечения. Как отмечают в системе клиник «Меди», в перспективе ожидается более широкое использование ИИ в диагностике при планировании ортодонтического лечения и хирургических операций, в том числе имплантации.

«Мы внедрили программу Diagnocat, которая анализирует рентгеновские снимки, помогая выявлять патологии зубов и окружающих тканей. Хотя программа еще совершенствуется и не заменяет опытного врача, она служит дополнительным мнением в диагностическом процессе,— рассказывает заведующая отделением стоматологии системы клиник «Меди» Елизавета Лопатина.— Кроме того, мы приобрели передовой дентальный томограф Axeos, являющийся одной из самых современных систем визуализации. Он позволяет делать сверхчеткие широкоформатные снимки, 3D-цефалометрию, расчеты КЛКТ (конусно-лучевой компьютерной томографии)».

С ЭТИМ НАДО ПОРАБОТАТЬ Как рассказала Guide ретинолог клиники «Счастливый взгляд» Владислава Фомичева, для офтальмологов разработано несколько полезных зарубежных онлайн-инструментов, а также отечественная платформа (Retina.ai). Эти сервисы позволяют анализировать диагностические данные при помощи ИИ.

«В облачные сервисы загружаются снимки структур глаза, полученные оптическим когерентным томографом. Далее ИИ анализирует их, помогая врачу выявить, например, признаки диабетической ретинопатии и диабетического макулярного отека. Сейчас платформы актуальны больше для врачей-ординаторов и имеют ограничения в использовании, но, вероятно, в ближайшем будущем станут незаменимым инструментом в анализе диагностических исследований»,— добавляет госпожа Фомичева.

В клинике хотели внедрить чат-бот для общения с клиентами, но опыт показал, что «человек с этой работой справляется пока лучше».

«Если раньше речь шла про роботизацию как ноухау, то сейчас производители говорят про автоматизацию на основе ИИ. Но пока ИИ не может заменить хирурга или медсестру, их мануальные навыки. Поэтому говорить, что ИИ как-то повлияет на кадровый вопрос, весьма преждевременно. К тому же правовой статус ИИ в медицине — тоже открытый вопрос, требующий серьезной проработки»,— полагает главврач клиники «Счастливый взгляд» Ирина Шикалович. ■

Тематическое приложение к газете «Коммерсантъ» (онлайн-выпуск Санкт-Петербург, Guide «Цифровая экономика»)

Роман Уманский — генеральный директор АО «Коммерсантъ»
Михаил Лукин — главный редактор
Анатолий Гусев — автор дизайн-макета
Андрей Ершов — главный редактор СПб страниц
Александр Коряков — бильд-редактор
Алла Михеенко — выпускающий редактор
Марина Шевченко — корректор
Мария Громова — верстка
Мария Кузнецова — отдел спецпроектов
Марина Победенная — рекламная служба

Адрес редакции и издателя: 123112, г. Москва, Пресненская наб, д.10 этаж 35. Тел. (495) 797-6970. Адрес редакции в Санкт-Петербурге: 191024, Харьковская ул., д. 8А, лит А. Тел. (812) 324-6949

Учредитель: АО «Коммерсантъ».
Тематическое приложение к газете «Коммерсантъ», зарегистрировано Роскомнадзором, регистрационный номер и дата принятия решения о регистрации ПИ №ФС77-76923 от 11.10.2019 года

В печатном виде номер не выходит.
Распространяется бесплатно.
16+

Фото на обложке: Freepik