«ХОЧЕШЬ УСКОРИТЬ ХАОС — АВТОМАТИЗИРУЙ ЕГО» / 4
ТРЕНДЫ КИБЕРБЕЗОПАСНОСТИ / 5
ОСТОРОЖНАЯ МИГРАЦИЯ НА ОБЛАКО / 8

Цифровая экономика

Понедельник, 19 мая 2025
Тематическое приложение к газете «Коммерсантъ» **№15**

Коммерсантъ
ONLINE

Guide



АЛЛА МИХЕЕНКО,
РЕДАКТОР GUIDE
«ЦИФРОВАЯ ЭКОНОМИКА»

НОВАЯ ОБЯЗАТЕЛЬНАЯ ГРАМОТНОСТЬ

Еще пять лет назад владение Excel считалось продвинутым навыком для офисного работника. Сегодня даже бухгалтеры используют ChatGPT для анализа документов, а менеджеры по продажам самостоятельно настраивают бизнес-процессы в no-code-системах. IT перестает быть уделом избранных — теперь это обязательная грамотность для всех. На первый план выходят user-friendly сервисы, которые может освоить даже нетехнический специалист.

По данным HeadHunter, за последние два года спрос на «гибридные» профессии (где нужно и разбираться в предметной области, и уметь работать с цифровыми инструментами) вырос на 40%. Теперь даже в вакансиях юристов или маркетологов часто встречаются требования вроде «опыт работы с ChatGPT для анализа документов» или «навыки Power BI для визуализации данных».

Компании все чаще внедряют low-code/no-code-платформы, позволяющие сотрудникам без программирования создавать landing-страницы, базы данных и даже автоматизированные workflows.

Исследование Mail.ru Group показывает, что 83% компаний используют хотя бы один цифровой инструмент для автоматизации рутинных задач, 61% сотрудников регулярно применяет AI-решения в работе. При этом лишь 27% организаций проводят системное обучение новым технологиям.

Парадокс современного рынка труда: технологии становятся проще, а требования к сотрудникам — жестче. Главная проблема — растущий разрыв между «цифровыми» и «аналоговыми» сотрудниками. По данным НИУ ВШЭ, 45% работников старше 45 лет испытывают трудности с освоением новых технологий, 30% компаний сталкиваются с саботажем цифровых инициатив со стороны персонала, только 15% организаций имеют продуманную систему мотивации для внедрения инноваций.

Компании, которые не обучат сотрудников работать с этими технологиями, рискуют потерять в эффективности. С другой стороны, сами работники, осваивающие новые цифровые навыки, получают серьезное конкурентное преимущество — даже если они не разработчики.

КОД ДЕФИЦИТА: ВУЗЫ И БИЗНЕС РЕШАЮТ КАДРОВЫЙ ВОПРОС В IT

IT-ОТРАСЛЬ РАЗВИВАЕТСЯ СТРЕМИТЕЛЬНО, А ПОДГОТОВКА НОВЫХ СПЕЦИАЛИСТОВ НУЖНОГО УРОВНЯ ЗАНИМАЕТ НЕСКОЛЬКО ЛЕТ. СЕГОДНЯ НА РЫНКЕ ТРУДА НАИБОЛЕЕ ВОСТРЕБОВАНЫ ПРОФЕССИОНАЛЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, МАШИННОГО ОБУЧЕНИЯ, ИНЖЕНЕРЫ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ. В СВЯЗИ С ЗАПРОСОМ ПРАВИТЕЛЬСТВО УВЕЛИЧИВАЕТ ЧИСЛО БЮДЖЕТНЫХ МЕСТ ПО IT-НАПРАВЛЕНИЯМ В ВУЗАХ, А УНИВЕРСИТЕТЫ ТРАНСФОРМИРУЮТ ПРОГРАММЫ И В КОЛЛАБОРАЦИИ С ТОПОВЫМИ КОМПАНИЯМИ РАЗВИВАЮТ НОВЫЕ НАПРАВЛЕНИЯ. УЧАСТНИКИ РЫНКА ПОЛАГАЮТ, ЧТО В БЛИЖАЙШИЕ ГОДЫ ВЫСОКИЙ СПРОС НА ЭТИХ СПЕЦИАЛИСТОВ СОХРАНИТСЯ. НАДЕЖДА ЯРМУЛА

Число сотрудников IT-компаний в России за последние пять лет выросло на 70% и приблизилось к 1 млн человек, заявил в конце января руководитель аппарата правительства РФ Дмитрия Григоренко. Однако в условиях ухода иностранных компаний, постоянной цифровизации и вынужденного импортозамещения даже такой стремительной рост и интерес к информационной сфере не решает проблему дефицита кадров. По данным Министерства цифрового развития, связи и массовых коммуникаций РФ, нехватка специалистов в 2024 году составила 500–700 тыс. человек, а бизнес-сообщество оценивает дефицит до 1 млн человек.

Решение проблемы правительство видит, в том числе, в увеличении количества бюджетных мест на IT-специальности в вузах. В декабре 2024 года во время совещания правительства с президентом РФ Владимиром Путиным глава Минцифры Максут Шадаев заявлял, что за четыре года количество мест увеличили в два раза. «У нас в этом году 125 тыс. человек зачислено в вузы на бюджетные места, еще 70 тыс. — на внебюджетные места. 500 вузов сейчас осуществляют подготовку IT-специалистов. Примерно 600 тыс. человек учится в вузах»,— отчитался министр.

Количество желающих поступить на IT-направления ежегодно растет. В 2024 году ЕГЭ по информатике сдавали 122 тыс. выпускников российских школ. В Петербурге в 2025 году информатику выбрали 8 тыс. человек — 21,2% от числа всех сдающих (всего на ЕГЭ зарегистрировано 37,8 тыс. петербуржцев). В прошлом году этот показатель был немного ниже: 18,67%, или 6,2 тыс. человек из 37,4 тыс. сдающих.

ОБНОВЛЕНИЕ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ На фоне развития IT-сферы и повышенного интереса со стороны абитуриентов вузы видоизменяют учебные программы и вместе с бигтехами открывают новые направления и школы. В этом году ВШЭ в Петербурге совместно с VK трансформирует факультет физики, математики и компьютерных наук в Школу информатики, физики и технологий (ШИФТ).

«С трансформацией факультета физико-математических и компьютерных наук в Школу произошло существенное расширение образовательных возможностей. Сейчас мы предлагаем пять программ на бакалавриате и пять — в магистратуре: по четыре в IT-направлении и одну по физике»,— рассказывает декан факультета ШИФТ НИУ ВШЭ — Санкт-Петербург Михаил Мухин. В предстоящем учебном году в ШИФТ дополнительно выделят бюджетные (25 штук) и коммерческие места (80 штук) по направлению «Программная инженерия», отмечают в «Вышке». Кроме того, в университете в следующем учебном году предусмотрена новая образовательная программа «Программирование и инжиниринг компьютерных игр».

«ШИФТ принципиально отличается от классического факультета тем, что выстраивается по модели IT-компании. Обучение будет проходить в условиях, максимально приближенных к работе в бигтехе. Плюс для работодателей в такой совместной работе с вузом заключается в возможности участвовать в формировании образовательных программ, предоставлять реальные кейсы для обучения, привлекать студентов к решению актуальных бизнес-задач и в итоге получать специали-



ЕВГЕНИЙ ЛАВЛЕНКО

В ПЕТЕРБУРГЕ РАСТЕТ ЧИСЛО ЖЕЛАЮЩИХ ПОЙТИ В IT-СФЕРУ. ЭТО МОЖНО ПРОСЛЕДИТЬ ПО РОСТУ ЧИСЛА ЖЕЛАЮЩИХ СДАТЬ ЕГЭ ПО ИНФОРМАТИКЕ. В 2025 ГОДУ ДАННЫЙ ЭКЗАМЕН ВЫБРАЛИ 8 ТЫС. ЧЕЛОВЕК, А В 2024 ГОДУ — 6,2 ТЫС. ЧЕЛОВЕК

стов с релевантными навыками и знаниями, адаптированных к работе в корпоративной среде»,— говорит господин Мухин.

Количество платных мест увеличится в Санкт-Петербургском государственном электротехническом университете «ЛЭТИ». «На платную форму обучения количество мест увеличилось почти на 200. В основном увеличение мест было на IT-направления: информационные системы и технологии, программная инженерия, компьютерная безопасность. Бюджета в этом году на данные направления также было выделено больше на 44 места по сравнению с прошлым годом. Это связано с тем, что спрос на IT-специалистов на рынке труда растет, и мы в приемной комиссии замечаем тенденцию роста по количеству поданных заявлений на IT-направлении»,— рассказывают в центре «Абитуриент» вуза.

В конце апреля Санкт-Петербургский государственный университет присоединится к первому в России ИИ-бакалавриату AI360 для будущих архитекторов и исследователей искусственного интеллекта. Программу в сентябре 2024-го запустили «Яндекс» и «Сбер». В новом учебном году набор на программу в пяти вузах-партнерах — ИТМО, НИУ ВШЭ, МФТИ, Университете «Иннополис» и СПбГУ — увеличится в полтора раза, рассказали в пресс-службе «Яндекс Образования».

НА ВОЛНЕ ИИ На рынке труда продолжает расти интерес к специалистам, владеющим навыками использования технологий искусственного интеллекта. По данным совместного исследования компании Tecno и hh.ru, за 2024 год количество вакансий с упоминанием AI превысило 4,2 тыс., что на 4% больше по сравнению с 2023 годом. Основная часть вакансий (более 1,7 тыс.) приходится на IT-отрасль. На финансовый сектор — около 1 тыс. объявлений, на сферу образования — более 300.

«Интерес к ИИ в России продолжает расти: с 2021 по 2024 год доля компаний, применяющих такие технологии, увеличилась с 20 до 43%. Все больше решений внедряется в реальные отрасли: ритейл, логистику, финансы, промышленность. Это отражается и на рынке труда, сегодня все чаще появляются вакансии, где требуются навыки работы с ИИ и понимание его практического применения. Компании ищут специалистов, способных не только разработать, но и адаптировать технологии под конкретные бизнес-задачи»,— комментирует менеджер по продуктовому маркетингу Tecno Евгений Рыбкин.

Интерес к ИИ отмечают и петербургские вузы. «Сейчас самые „хайповые“ направления завязаны на ИИ. Для нас это абсолютно ожидаемо, тем более что ИИ-разработками ИТМО занимается давно, причем вместе с индустриальными партнерами»,— говорит начальник отдела организации приема ИТМО Алексей Итин.

Заместитель генерального директора по работе с персоналом Selectel Надежда Курлат отмечает: «Спрос на специалистов в сфере информационной безопасности и ИИ продолжает расти, однако мы видим потребность не только в разработчиках и инженерах данных, но и в специалистах, обеспечивающих работу IT-инфраструктуры под такие задачи. ИБ и ИИ-проекты требуют особых условий размещения и поддержки: это и высокая плотность потребления энергии, и специфические требования к отказоустойчивости. Поэтому на рынке особенно востребованы технические специалисты, способные обеспечивать бесперебойную работу такой инфраструктуры, настраивать оборудование под нестандартные задачи и взаимодействовать с инженерными командами со стороны заказчиков».

НАСТОЯЩЕЕ В компаниях, впрочем, заявляют: найти высококвалифицированного специалисты в любом направлении остается сложной задачей. «Дефицит кадров на IT-рынке — перманентная ситуация, требующая комплексного подхода. Сильные IT-специалисты всегда будут востребованы. Важно, чтобы их подготовка осуществлялась в тесном сотрудничестве вузов и бизнеса и учитывала актуальные потребности работодателей»,— указывает заместитель вице-президента по образовательным проектам VK Анна Степанова.

За первые четыре месяца 2025 года петербургские компании разместили на HeadHunter 23 тыс. вакансии в разделе «Информационные технологии». По сравнению с аналогичным периодом 2024 года спрос на айтишников немного просел (–3% размещенных вакансий), приводит данные руководитель пресс-службы hh.ru в Центре и на Северо-Западе Мария Бузунова. Чаще других компании искали программистов: на них приходится 25%, или почти 6 тыс. вакансий от всего объема в отрасли. Также востребованы IT-художники (10%, или 2,4 тыс. вакансий) и руководители IT-проектов (10%, или 2,2 тыс. вакансий).

«Найти высококвалифицированного эксперта в любое направление IT по-прежнему остается сложной задачей для бизнеса. Появляются новые ИИ-инструменты, легкие для изучения и использования языки программирования, которые упрощают вход в IT и ускоряют работу, но они не всегда подходят для решения сложных задач, пул которых растет в данной сфере. И зачастую вопрос дефицита кадров кроется в дисбалансе между объемом сложных задач и специалистов, у которых есть необходимые навыки для их решения»,— объясняет госпожа Курлат. По ее словам, на рынке также увеличивается спрос на инженеров центров обработки данных. Такой интерес связан с ростом потребности бизнеса в мощностях дата-центров.

«Это специалисты на стыке IT и технической специальности, умеющие работать с современной аппаратной инфраструктурой дата-центров. По данным iKS-Consulting, темпы роста облачного рынка в ближайшие годы сохранятся на уровне 30%. Спрос на облачные сервисы и услуги ЦОД будет расти, соответственно, потребуются квалифицированные кадры не только для поддержания работы дата-центров, но и для развития новых продуктовых решений»,— продолжает госпожа Курлат.

На рынке труда, по словам директора по управлению персоналом компании «Т1 Интеграция» Екатерины Мелентьевой, также востребованы специалисты в области машинного обучения, backend- и frontend-разработчики с опытом в высоконагруженных системах.

БУДУЩЕЕ Говорить о будущем IT-отрасли, учитывая скорость ее развития, довольно трудно. «По прогнозам экспертов, две трети представителей поколения „Альфа“ будут работать по специальностям, которых пока не существует, например, инженеры дополненной реальности, специалисты по ИИ-этике или проектировщики нейроинтерфейсов. Будут востребованы специалисты, способные управлять ИИ и развивать нейросети»,— заявляет госпожа Степанова.

В ЛЭТИ полагают, что в ближайшие 5–10 лет будет сохраняться высокий спрос на специалистов в сфере ИИ, машинного обучения, кибербезопасности, аналитики данных и автоматизации процессов.

«На рынке IT, даже при условии повсеместного внедрения AI-инструментов для разработки ПО, всегда будут востребованы исследователи и инженеры в области ML, а также системные архитекторы. ML-инженер будет развивать, поддерживать и обслуживать AI, а системный архитектор ставить ему задачи»,— заявляет господин Мухин.

По мнению господина Итина, в будущем будут востребованы люди, которые смогут решать сложные задачи, писать алгоритмы, быть архитекторами информационных систем. «Таких на рынке и сейчас мало, а в будущем они будут нужны еще больше»,— подчеркивает эксперт.

В ближайшие 5–10 лет, по мнению госпожи Мелентьевой, будут востребованы люди, умеющие работать с данными: собирать, анализировать и интерпретировать информацию для принятия обоснованных решений в IT-проектах. «На первый план постепенно выходят не столько профессиональные компетенции (hard skills), сколько ключевые „мягкие“ навыки (soft skills) — критическое мышление, умение адаптироваться к изменениям, способность к непрерывному обучению»,— подчеркивает она.

При этом, по мнению Екатерины Мелентьевой, говорить о возникновении качественно новых профессий пока не стоит. «Речь идет скорее о расширении или трансформации компетенций уже существующих ролей. Специалистам по кибербезопасности теперь важно разбираться в основах ИИ и машинного обучения, а ML-инженерам — в нюансах DevOps-подхода. Некоторые ИИ-разработчики становятся тренерами моделей и промпт-инженерами»,— заключает эксперт. ■

«НАША ЗАДАЧА — СДЕЛАТЬ РЕВОЛЮЦИЮ В ОБУЧЕНИИ NO-CODE-СПЕЦИАЛИСТОВ»

СФЕРА РАЗРАБОТКИ САЙТОВ ПЕРЕЖИВАЕТ ТРАНСФОРМАЦИЮ: NO-CODE-ПЛАТФОРМЫ ПОЗВОЛЯЮТ СОЗДАВАТЬ ДИДЖИТАЛ-ПРОДУКТЫ БЕЗ ГЛУБОКИХ ТЕХНИЧЕСКИХ ЗНАНИЙ. О НОВЫХ ИНСТРУМЕНТАХ И ИХ РАБОТЕ GUIDE РАССКАЗАЛ ИГОРЬ ЛИТВИНЦЕВ, РУКОВОДИТЕЛЬ ПЛАТФОРМЫ «ТАПТОП» (TAPTOP.PRO ОТ «МЕГАГРУПП.РУ»). АЛЛА МИХЕЕНКО

GUIDE: Как вы оцениваете спрос на no-code-решения?

ИГОРЬ ЛИТВИНЦЕВ: No-code активно проникает во многие сферы. По прогнозам консалтинговой компании Gartner, к 2027 году 80% всего софта будет сделано на no-code, а оставшиеся 20% — разработка верхнего уровня. Это подход, позволяющий нетехническим пользователям создавать сайты, приложения и автоматизированные процессы с помощью визуальных инструментов. Без привлечения разработчика можно запустить продукт. Этим пользуются малый и средний бизнес, а также холдинги. Крупные компании (ритейл, финсектор) заботятся о безопасности — поэтому выбирают решения, которые можно развернуть внутри своей инфраструктуры. Наш продукт тоже можно внедрить в контуре заказчика, мы адаптируем его под нужды клиента.

G: Насколько конкурентен рынок веб-разработки?

И. Л.: В России ежегодно появляется около миллиона новых доменов. Сегодня сайт — обязательный атрибут бизнеса. Простейшие сайты на 1–5 страниц предприниматели создают сами на конструкторах. Но если нужен сложный сайт с уникальным дизайном, анимацией и масштабируемостью до тысячи страниц, простые решения не подходят. Наша платформа предназначена именно для таких задач. Она предлагает широкие возможности кастомизации внешнего вида сайта и позволяет создавать неограниченное число страниц: о компании, истории, статьи, доски объявлений.

Раньше единственным мощным визуальным редактором кода был WebFlow, но с 2022 года появились ограничения: нельзя оплатить с российской карты, нет интеграции с локальными сервисами, не соответствует закону 152-ФЗ. Наш сервис решает эти проблемы. У нас функционал WebFlow + Figma, но адаптированный под российский рынок: поддержка платежей российских банков, интеграции с «Яндексом», 1С, «Битриксом».

G: А что насчет других платформ, таких как Tilda, Wix?

И. Л.: Tilda и Wix были популярны, так как других вариантов не было. Но с сентября 2024 года Wix больше не обслуживает резидентов России. Что касается Tilda, то платформа была изначально создана не для верстки, а для визуального размещения блоков. Дизайнер располагает элементы на экране, а Tilda компилирует за него код. В итоге он получается громоздким, что замедляет загрузку сайта и усложняет продвижение в поисковых системах. Taptop генерирует легкий, чистый код, и почти все задачи решаются средствами самой платформы, без сторонних скриптов. Платформа подходит как для казуальных, простых сайтов, одностраничников, так и для крупных масштабируемых проектов. Он может расти вместе с бизнесом — от лендинга до полноценного корпоративного сайта. Кроме того, в Taptop дизайнер сам управляет кодом в визуальном интерфейсе, без посредников. Это ускоряет процесс в три-четыре раза, снижает стоимость и устраняет искажения между макетом и реализацией.



TAPTOP

G: Какое у вас ключевое преимущество с точки зрения бизнес-модели?

И. Л.: Мы практикуем не просто открытую коммуникацию, а доступность на личном уровне. Мы общаемся с каждым пользователем «на ты»: вся команда — от разработчиков до CEO — присутствует в соцсетях и открыта к диалогу. У нас есть публичный roadmap с анонсами релизов. Люди голосуют за идеи, предлагают свои. Мы аккумулируем предложения, обрабатываем их с помощью нейросетей, сегментируем, и если идея действительно нужна рынку, внедряем ее. Такая модель — редкость среди российских диджитал-сервисов.

G: Расскажите про обучение дизайнеров.

И. Л.: Поскольку это профессиональный инструмент, то входной порог выше, чем у блочных конструкторов. Мы выстроили систему обучения, охватывающую все уровни подготовки.

Есть бесплатная академия — уровень junior, которую за полгода уже прошли более 500 дизайнеров. Есть и платная. Она создана совместно и по методологии Uprock. Это крупнейшая авторская школа UX/UI-дизайна, которая обучила более 12 тыс. студентов. Это курс уровня middle и выше. Он построен как имитация работы в реальных условиях: с дедлайнами, обратной связью, презентацией проектов. Обучение длится два месяца, а во время прохождения студенты окупают его, получая первые заказы.

Мы формируем карьерную цепочку: бесплатный курс → платный курс → выход на рынок как no-code-специалист. На Западе дизайнер все чаще становится одновременно и разработчиком. За такую универсальность клиент готов платить в два-три раза больше, чем за обычную работу на конструкторах. Taptop поддерживает этот тренд: у нас дизайнер делает полноценные сложные проекты — и получает соответствующую оплату. ■

«ХОЧЕШЬ УСКОРИТЬ ХАОС — АВТОМАТИЗИРУЙ ЕГО»

В УСЛОВИЯХ РАСТУЩЕЙ КОНКУРЕНЦИИ И ЭКОНОМИЧЕСКОЙ НЕСТАБИЛЬНОСТИ КОМПАНИИ ВСЕ ЧАЩЕ ОБРАЩАЮТСЯ К ЦИФРОВЫМ РЕШЕНИЯМ ДЛЯ ОПТИМИЗАЦИИ ОПЕРАЦИОННОЙ ДЕЯТЕЛЬНОСТИ. РОБОТИЗАЦИЯ РУТИННЫХ ЗАДАЧ, ВНЕДРЕНИЕ AI-АНАЛИТИКИ И ПЕРЕХОД НА ОБЛАЧНЫЕ ПЛАТФОРМЫ ПОЗВОЛЯЮТ БИЗНЕСУ СОКРАЩАТЬ ЗАТРАТЫ НА 20–30%, МИНИМИЗИРОВАТЬ ЧЕЛОВЕЧЕСКИЙ ФАКТОР И УСКОРЯТЬ КЛЮЧЕВЫЕ ПРОЦЕССЫ — ОТ ЛОГИСТИКИ ДО КЛИЕНТСКОГО СЕРВИСА. ОДНАКО ЭКСПЕРТЫ ЗАЯВЛЯЮТ, ЧТО БОЛЬШАЯ ЧАСТЬ ИНИЦИАТИВ В ЭТОЙ СФЕРЕ ТЕРПЯТ НЕУДАЧУ ИЗ-ЗА НЕПРАВИЛЬНОГО ВЫБОРА ИНСТРУМЕНТОВ ИЛИ СОПРОТИВЛЕНИЯ СОТРУДНИКОВ. GUIDE РАЗБИРАЛСЯ, КАКИЕ ТЕХНОЛОГИИ ПРИНОСЯТ КОМПАНИЯМ РЕАЛЬНУЮ ВЫГОДУ И КАК ИЗБЕЖАТЬ ТИПИЧНЫХ ОШИБОК ПРИ ИХ ВНЕДРЕНИИ. АЛЛА МИХЕЕНКО

По статистике, которую приводит Кирилл Федулов, сооснователь и директор по развитию Okdesk, в РФ более 74% компании активно занимаются автоматизацией бизнес-процессов, но при этом лишь 50% МСБ охвачены автоматизацией в той или иной степени. При этом сам уровень автоматизации в организациях сильно разнится. «Где-то это „как-то работает, но как — непонятно“, а у других, согласно ответам участников отраслевого исследования: „все автоматизировано как часы“. И это при том, что для кого-то автоматизация — это использование мессенджеров и корпоративных чатов, а для кого-то — работа в условных EPR-системах. Зачастую низкий уровень автоматизации связан с тем, что проекты внедрения новых решений оказываются неуспешными, неэффективными или вовсе не завершаются»,— рассуждает господин Федулов.

Наиболее активно бизнес-процессы автоматизируют в рознице, логистике, банковском секторе и телекоммуникациях. Так, X5 Group внедряет AI-алгоритмы для управления товарными запасами, «Сбер» роботизировал до 80% back-office операций, а «Почта России» тестирует компьютерное зрение для сортировки посылок. В промышленности лидеры, такие как «Росатом» и «Северсталь», автоматизируют контроль качества и логистику, сокращая простои на 15–20%. Между тем малый бизнес чаще всего внедряет CRM-системы и чат-ботов.

Игорь Гуняшов, сооснователь стартапа Plevako.ai, по внедрению ИИ в адвокатуре отмечает, что интересна ситуация по автоматизации складывается в консервативных сферах, где традиционно преобладал ручной интеллектуальный труд. «Мы видим, как, например, трансформируется юридическая отрасль. По данным Thomson Reuters, 84% юрфирм планируют увеличить вложения в ИИ-технологии. Наш опыт показывает, что автоматизация особенно эффективна в четырех направлениях. Во-первых, анализ данных. Во-вторых, поддержка принятия решений. В-третьих, автоматизация документооборота с учетом всех формальных требований. И наконец, улучшение клиентского сервиса через личные кабинеты доверителей и умные автоответчики. Эти подходы применимы, конечно, не только в юриспруденции. Но есть и риски. В США был случай, когда адвокат получил штраф в $5000 за использование ложных данных от ИИ. Поэтому важно сохранять критическое мышление и не допускать чрезмерной зависимости от технологий»,— комментирует бизнесмен.

Если говорить о крупных производственных холдингах, то внедрение инновационных решений требует значительных инвестиций, предупреждает коммерческий директор IT-компании BIA Technologies Александр Воловик. «Это не только затраты на оборудование, но и необходимость формирования штата специалистов по техподдержке. Например, на производстве, где выпускается всего десять товарных номенклатур в стандартных упаковках, может оказаться более целесообразным заменить конвейерную линию на труд двух сотрудников. В этом случае достигается аналогичная эффективность при значительно меньших затратах. Когда речь идет о больших объемах обработки товаров, оптимизация процессов становится сложной задачей, требующей предварительного моделирования. Без тщательного анализа всех этапов невозможно достичь максимальной эффективности»,— указывает господин Воловик. Он предлагает использовать цифровых двойников, чтобы учесть все детали оптимизации.



АЛЕКСАНДР КОРЖОВ

ПО ДАННЫМ НАФИ ЗА 2023 ГОД, 67% РОССИЙСКИХ КОМПАНИЙ ИСПОЛЬЗУЮТ ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ, ПРИЧЕМ 42% — НА ПОСТОЯННОЙ ОСНОВЕ

С ЧЕГО НАЧАТЬ?

Эксперты отмечают, что есть несколько подходов во внедрении цифровых инструментов и отстройке инфраструктуры. Можно начать автоматизацию с нуля. «Этот путь хорош, если процессы еще не зафиксированы или вы готовы к трансформации. Минус — сложнее на старте, потому что нужно сначала описать процессы, собрать требования, протестировать гипотезы. Но зато выстраивается система, которая не тянет за собой старые ошибки. Мы не раз видели, как именно с чистого листа удается выстроить реально эффективную и удобную систему»,— делится Олеся Шаркова, директор IT-интегратора «Экспресс Лаб».

Второй вариант — перенос на новую систему. Подходит, если есть наработанная инфраструктура, но текущие инструменты уже не справляются. «Самое сложное здесь — оценка объема работ. Кажется, что „вот тут просто выгрузим и зальем“, но на деле: нет единого формата данных, пропущены поля или логика связей, старая база „грязная“ и требует очистки, пользователи не понимают, что с этим делать. А еще бизнес-процессы часто существуют только „в головах“ сотрудников, и при попытке их переноса наружу возникает огромное количество несостыковок и вопросов»,— говорит госпожа Шаркова.

«Часто хочется сказать: давайте не тащить с собой все ошибки, баги и костыли, которые вы собирали пять лет. Когда компания хочет навести порядок, но в процессах уже каша — проще нарисовать идеальную картину и внедрять с чистого листа. Автоматизация не начинается с системы. Она начинается с честного взгляда на бардак. Это про зрелость команды. Прежде чем настраивать IT, нужно навести порядок в голове и в процессах. А технология — это уже инструмент, а не волшебная палочка»,— отмечает Анастасия Иванова, CEO Salesmates.

«Сегодня стандартом для эффективного переноса процессов на новые IT-системы является внедрение интеграционной шины (ESB), изначально предназначенной, с одной стороны, для быстрой замены компонентов информационной системы без риска обрушить существующие процессы, а с другой — внедрение новых бизнес-процессов, используя возможности существующей ИС. Другими словами, ESB позволяет абстрагировать (отвязать) бизнес-процессы от конкретной IT-системы, которая его реализует. А автоматизация „с нуля“ является, как минимум, неоправданным расходом средств. „Лоскутная“ автоматизация, как давно известно, не решает ни одну из производственных и бизнес-задач»,— считает Дмитрий Грязнов, генеральный директор компании «Инполюс».

ОТ БАРДАКА — К ПЕРЕОСМЫСЛЕНИЮ

Без детального понимания того, как устроены текущие рабочие процессы, невозможно определить, что именно требует оптимизации, поэтому любой проект нужно начинать с аудита, составления карт процессов и выявления узких мест. Такое мнение высказывает основатель ГК «Юнисофт» Алексей Оносов. «Это занимает до 15% времени всего проекта, но экономит ресурсы и предотвращает множество ошибок на последующих этапах. Оптимальный выбор зависит от текущего состояния IT-инфраструктуры. Полная замена систем обходится дороже и занимает больше времени, но иногда это единственный способ добиться качественного скачка в эффективности. При этом хорошо работающие компоненты имеет смысл интегрировать в новую систему, а не выбрасывать. Приведу пример: в нашей компании мы сохранили работающую систему учета заказов, построив вокруг нее новую экосистему взамен устаревших решений. Это позволило сэкономить около 30% бюджета и избежать сложностей с переобучением персонала»,— говорит господин Оносов.

Автоматизация бизнес-процессов начинается с аудита, уверена коммерческий директор «Теле2Мед» Юлия Классен. В частности, должно быть понимание, какие

данные уже обрабатываются, какие этапы критичны, а какие устарели. Есть и нюансы. «Например, в логистике это сбор данных о работе транспорта. Двадцать лет назад целью было сокращение издержек: на машины ставили датчики пробега и топлива, а данные сверялись вручную с путевыми листами. Потом автоматизировали выдачу путевых листов, затем их таксировку — все это ради бизнеса. В 2023 году разрешили электронные путевые листы: водитель выезжает с QR-кодом. Бумажная волокита исчезла, но заказчиком стал уже не бизнес, а государство — а значит, в путевом листе остались только те данные, которые нужны регуляторам»,— приводит пример госпожа Классен.

Другая распространенная ошибка — оцифровка хаоса. «Например, если раньше сотрудник бегал за подписью по этажам, теперь он просто гоняет документы в ЭДО. Но нужна ли подпись вообще? Поэтому первый шаг — не автоматизация как есть, а переосмысление процесса под задачи заказчика»,— добавляет эксперт.

НЕДООЦЕНЕННЫЕ НЮАНСЫ Эксперты отмечают, что недооценка сроков внедрения — самая распространенная ошибка. Особенно часто недооценивается время на интеграцию между системами. «По нашему опыту, на интеграционные работы следует закладывать от 20 до 30% общего времени проекта. Именно на этом этапе возникают непредвиденные сложности: несовместимость форматов данных, отсутствие API у старых систем и другие технические препятствия. Еще один важный аспект — не автоматизировать нестабильные процессы. Если бизнес-процесс часто меняется или нет его четкого описания, сначала нужно его стабилизировать и формализовать, и только потом приступать к автоматизации»,— говорит господин Оносов.

Выбор технологической платформы должен определяться потребностями и масштабами бизнеса, а не модой или рекламой. Для малого бизнеса часто достаточно существующих коробочных решений или облачных сервисов с минимальной кастомизацией. Средним компаниям подходят отраслевые решения с возможностью доработки. Крупным организациям может потребоваться создание собственных систем или глубокая настройка корпоративных платформ.

По словам руководителя IT-агентства WebSiberia Арега Варданяна, при автоматизации компании совершают типичные ошибки. Одна из них — автоматизировать все сразу. «Есть такая шутка: хочешь ускорить хаос — автоматизируй его. Как ни печально, в ней много правды. Пытаться внедрить сразу десяток новых систем в компании — гиблая затея. Видел, как организация одновременно запустила CRM, ERP и электронный документооборот. Итог: команда захлебнулась, часть систем бросили на полпути, сотрудники вернулись к прежним методам. Не пытайтесь охватить необъятное»,— предупреждает эксперт.

Кроме того, есть еще одна ошибка — поставить новый софт и ждать, что персонал сам к нему привыкнет. «Если людей не обучить и не вовлечь, они либо саботируют изменения, либо игнорируют новую систему. Например, одна организация внедрила портал без объяснений — сотрудники продолжили по-старому, и новое ПО простаивало»,— комментирует господин Варданян.

«Ключевой фактор успеха — вовлечение сотрудников,— подтверждает Юрий Востриков, генеральный директор BPMSoft (входит в IT-холдинг Lansoft).— Без участия бизнес-пользователей автоматизация либо не работает, либо превращается в цифровую копию прежней бюрократии».

Автоматизация — это не разовый проект, а непрерывный процесс совершенствования бизнеса. Эксперты говорят, что, выбирая конкретные технологии и подходы, стоит ориентироваться на реальные потребности, а не на модные тренды. Внедрение лучше начинать с тех вертикалей, где эффект будет максимальным, постепенно расширяя охват. Автоматизация должна решать конкретные бизнес-задачи, а не быть самоцелью. Сегодня даже небольшие компании могут получить значительные преимущества от внедрения современных IT-решений, главное — грамотно спланировать процесс и избежать типичных ошибок. Успех определяется не столько технологиями, сколько подходом к внедрению и готовностью компании к изменениям. ■

ДОМА «УМНЕЮТ» ФУНКЦИЯМИ

СИСТЕМЫ «УМНОГО ДОМА» ПРОДОЛЖАЮТ НАБИРАТЬ ПОПУЛЯРНОСТЬ. ЕЩЕ ТРИ ГОДА НАЗАД РАЗЛИЧНЫЕ ЭЛЕМЕНТЫ ЭТОЙ ТЕХНОЛОГИИ ИСПОЛЬЗОВАЛИСЬ НЕ БОЛЕЕ ЧЕМ В 2–3% ЖИЛОГО ФОНДА В СТРАНЕ, СЕЙЧАС ЖЕ ЭТОТ ПОКАЗАТЕЛЬ, ПО РАЗНЫМ ПОДСЧЕТАМ, УВЕЛИЧИЛСЯ ДО 9%. ЭКСПЕРТЫ ГОВОРЯТ, ЧТО ОТДЕЛЬНЫЕ ФУНКЦИИ «УМНОГО ДОМА» УЖЕ НЕ ЯВЛЯЮТСЯ ЧЕМ-ТО ФУТУРИСТИЧЕСКИМ, А НАПРОТИВ, СТАЛИ ЧАСТЬЮ РАЗУМНОЙ ЦИФРОВИЗАЦИИ, КОГДА ТЕХНОЛОГИИ ИЗБАВЛЯЮТ ЧЕЛОВЕКА ОТ РУТИНЫ. ОДНАКО К УСТАНОВКЕ ПОЛНОЦЕННЫХ СИСТЕМ ПОКА ГОТОВ НЕ КАЖДЫЙ. ВИКТОР ИРИСОВ

Чаще всего комплексную систему «умный дом» можно встретить в премиальных жилых проектах, но отдельные ее функции, которые касаются самых важных аспектов жизни (безопасности, потребления ресурсов и услуг связи), девелоперы активно внедряют в домах комфорт- и бизнес-классов. Чаще всего это IP-домофоны и мобильные приложения для автоматической передачи показаний счетчиков.

ИСХОДЯ ИЗ ЗАПРОСОВ Спрос на системы «умного дома» продолжает расти, но все еще остается в пределах определенных сегментов аудитории, говорит вице-президент по маркетингу и продукту группы RBI Михаил Гущин. По его словам, наибольшую отдачу дают не абстрактные технологические платформы, а конкретные функции, решающие повседневные задачи жителей, особенно в сферах безопасности, энергоэффективности и удобства взаимодействия с домом.

В проектах комфорт- и бизнес-класса девелоперы внедряют IP-домофонию с распознаванием лиц и телеметрию, позволяющую автоматически передавать показания счетчиков, а также современные системы контроля доступа, которые, по мнению господина Гущина, уже не являются чем-то футуристическим, а напротив, стали частью разумной цифровизации, когда технологии избавляют человека от рутины, не перегружая его лишним функционалом.

По словам директора департамента элитной недвижимости NF Group в Санкт-Петербурге Алии Ханбековой, возможности внедрения полноценных «умных» систем внутри квартир на этапе строительства ограничены, поскольку жилье, как правило, сдается с черновой отделкой, поэтому дополнительные функции жильцы устанавливают уже на стадии ремонта.

Михаил Гущин подтверждает, что в проектах, как правило, используются гибридные модели: базовая инфраструктура закладывается застройщиком, а дальше уже сам житель может развивать ее по своему усмотрению.

«Массовый покупатель пока воспринимает „умный дом“ скорее как приятный бонус, нежели ключевой фактор выбора квартиры. Цена таких решений также остается барьером, особенно если речь идет о полноценной системе автоматизации внутри квартиры, при этом максимальный интерес к полноценным конфигурациям „умного дома“ демонстрируют, как правило, технологически подкованные покупатели, чаще молодые и активные. Но и в более зрелых сегментах аудитории спрос постепенно формируется, в основном на решения, повышающие уровень комфорта без необходимости глубоко вникать в настройки»,— поясняет эксперт.

РЫНОК И БЕЗОПАСНОСТЬ Если цена на полноценные системы «умного дома» все еще высока для рядового потребителя, то стоимость отдельных компонентов год от года становится ниже и, соответственно, доступнее. Это в первую очередь связано с увеличением предложения на рынке.

Помимо крупнейших игроков рынка — «Яндекса» и «Сбера», которые предлагают широкий ассортимент устройств «умного дома», ряд телеком-компаний, таких как МТС и «Ростелеком», активно развивают инфраструктуру IoT, обеспечивая связь для этих устройств. К 2022 году сети NB-IoT МТС охватывали более 90% потенциальных пользователей в 83 регионах РФ, а решения «Ростелекома» применялись почти в 2,5 тыс. многоквартирных домов России.

И все же отдельным вопросом для пользователей «умных» систем остается их цифровая безопасность. В СМИ неоднократно появлялись новости о злоумышленниках, получивших доступ к «умным» устройствам жильцов квартир. Хакеры могут использовать гаджеты «умного» дома для разных целей, поясняет советник гендиректора компании RooX, которая специализируется на аутентификации, авторизации и разработке веб-платформ для корпоративного сектора, Наталия Леднева.

Взломав камеру видеонаблюдения, они получают доступ к видеопотокам и могут следить за владельцами, а через колонки и ассистенты — подслушивать, что происходит дома, и собирать личную информацию. Через телевизор можно добраться до файлов, которые хранятся на подключенных к нему устройствах, а взломанный фитнес-трекер расскажет о местоположении и личной физической активности владельца.

Для защиты от взлома «умного дома» эксперт рекомендует регулярно обновлять прошивки и программное обеспечение гаджетов, так как в обновлениях производители закрывают уязвимости, тем самым повышая безопасность устройств.

«Также после покупки нужно сразу менять дефолтные пароли, которые были установлены производителями техники и Wi-Fi-роутеров. Базовые рекомендации по паролям: они должны быть разные и длинные. Кроме того, рекомендуем сегментировать сеть, разделив ее по профилю использования, например, для жителей дома, для гостей и для устройств»,— уточняет госпожа Леднева. ■



ЕВГЕНИЙ ПАВЛЕНКО

ИСПОЛЬЗУЯ «УМНЫЕ» РЕШЕНИЯ ДЛЯ ДОМА, СЛЕДУЕТ ПОМНИТЬ О БЕЗОПАСНОСТИ, СОВЕТУЮТ ЭКСПЕРТЫ

ВЫРАБОТАТЬ КОЛЛЕКТИВНЫЙ КИБЕРИММУНИТЕТ

МИРОВОЙ УЩЕРБ ОТ КИБЕРПРЕСТУПЛЕНИЙ ОЦЕНИВАЕТСЯ В $200 МЛРД — $1 ТРЛН В ГОД, И ЭТА ЦИФРА ПРОДОЛЖАЕТ РАСТИ. В РОССИИ, ПО ОЦЕНКАМ МИНЦИФРЫ, ПРЯМОЙ УЩЕРБ ОТ ДЕЙСТВИЙ КИБЕРПРЕСТУПНИКОВ В 2024 ГОДУ СОСТАВИЛ 160 МЛРД РУБЛЕЙ. В ЗОНЕ ПОВЫШЕННОГО РИСКА — ГОССТРУКТУРЫ, ФИНАНСОВАЯ СФЕРА, ПРОМЫШЛЕННОСТЬ И ЭНЕРГЕТИКА, ГДЕ АТАКИ МОГУТ ПРИВЕСТИ К СЕРЬЕЗНЫМ ЭКОНОМИЧЕСКИМ И ОПЕРАЦИОННЫМ ПОТЕРЯМ. ПО МНЕНИЮ ЭКСПЕРТОВ, ДЛЯ ЗАЩИТЫ БИЗНЕСА НЕОБХОДИМО ПЕРЕХОДИТЬ ОТ РЕАГИРОВАНИЯ К ПРОАКТИВНОЙ СТРАТЕГИИ. ИНВЕСТИЦИИ В КИБЕРУСТОЙЧИВОСТЬ СЕГОДНЯ СТАНОВЯТСЯ НЕ ПРОСТО НЕОБХОДИМОСТЬЮ, А КРИТИЧЕСКИМ ФАКТОРОМ КОНКУРЕНТОСПОСОБНОСТИ. ИРИНА КОВАЛЕВА

Эпоха первых масштабных кибератак началась с вируса LoveLetter, который в 2000 году причинил ущерб на $10 млрд. «Этот инцидент продемонстрировал, как быстро злоумышленники адаптируются к новым технологиям, особенно с появлением интернет-платежей»,— сказал CEO «Лаборатории Касперского» Евгений Касперский, выступая на прошедшей в апреле этого года конференции Kaspersky Future. Кроме того, знаковым моментом стала история с шифровальщиком GPCode в 2006 году. «Первоначально специалистам удалось взломать его криптографическую защиту, но авторы вируса быстро выпустили обновленную версию с 660-битным ключом. Однако и эта защита оказалась уязвимой из-за ошибки в алгоритме генерации ключей»,— уточнил господин Касперский.

Следующее десятилетие ознаменовалось появлением высокопрофессиональных киберпреступных группировок. Так, группа Carbanak установила новый стандарт, похитив около миллиарда долларов через атаки на банковские системы. Особенностью их методов было удаленное управление банкоматами без физического доступа. «Отдельной главой в истории кибербезопасности стала атака Stuxnet на иранские ядерные объекты в 2010 году. Этот сложный вредонос скрытно изменял работу центрифуг, одновременно фальсифицируя данные телеметрии, что привело к их физическому разрушению»,— отметил Евгений Касперский.

По словам эксперта, в настоящее время ежегодный ущерб от киберпреступлений оценивается в $200 млрд — $1 трлн в год, причем эта цифра продолжает расти. В России, в свою очередь, по оценкам Минцифры, прямой ущерб от киберпреступлений в 2024 году достиг 160 млрд рублей, а их количество выросло почти на треть по сравнению с 2023 годом.



ЕВГЕНИЙ ПАВЛЕНКО

ЭКСПЕРТЫ ОТМЕЧАЮТ, ЧТО В НАСТОЯЩЕЕ ВРЕМЯ НАБЛЮДАЕТСЯ УСИЛЕНИЕ УГРОЗ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИИ

НОВЫЙ УРОВЕНЬ УГРОЗ

Собеседники Guide отмечают, что рынок информационной безопасности будет продолжать адаптироваться под задачи, связанные с противодействием усложняющимся киберугрозам. Среди наиболее явных — рост атак на критически важную инфраструктуру, в том числе с применением APT-группировок, поддерживаемых различными государствами. По словам Елены Скалозубовой, ведущего архитектора по информационной безопасности MONS (ГК «КОРУС Консалтинг»), геополитическая нестабильность остается значимым фактором риска. «Это уже не просто инциденты информационной безопасности, а новый вид оружия, и в развитие инструментов для кибератак вкладываются значительные ресурсы»,— утверждает Евгений Дорофеев, управляющий директор по направлениям «ИБ и Доверенные цифровые решения» АО «Росатом Автоматизированные системы управления». В 2025 году он прогнозирует 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 недекларированных возможностей, присутствия заложенного скрытого вредоносного функционала»,— считает он.

УВЕЛИЧЕНИЕ ЧИСЛА КИБЕРАТАК, ВКЛЮЧАЯ DDOS И ЦЕЛЕВЫЕ ВЗЛОМЫ, ЗАСТАВЛЯЕТ КОМПАНИИ ИСКАТЬ БОЛЕЕ НАДЕЖНЫЕ СПОСОБЫ ЗАЩИТЫ ДАННЫХ И ПЕРЕСМАТРИВАТЬ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

Госпожа Скалозубова подтверждает, что в 2024–2025 годах чаще других подвергались атакам государственные органы и объекты КИИ (в связи с геополитикой и высокой ценностью данных), финансовый сектор (из-за прямого доступа к денежным ресурсам и системам переводов), промышленность и энергетика (в этих отраслях распространены уязвимые SCADA-системы, а также слабая сегментация и высокая стоимость простоев). «Кроме того, часто атаковались организации здравоохранения (дефицит специалистов по ИБ, наличие персональных и медицинских данных, уязвимое ПО). Слабые стороны этих отраслей — недостаточное обновление систем, человеческий фактор, старое ПО и низкий уровень кибергигиены»,— указывает она.

Также в настоящее время наблюдается усиление угроз, связанных с использованием ИИ, вследствие чего возникает необходимость защищать сами ИИ-модели от потенциальных атак. «Кроме того, ИИ может применяться для анализа угроз и управления инцидентами безопасности, но с другой стороны — этими же технологиями могут пользоваться и злоумышленники»,— отмечает Антон Ведерников, руководитель направления продуктовой безопасности Selectel.

Среди наиболее распространенных методов атак 2024–2025 годов эксперты выделяют фишинг и социальную инженерию (особенно это касается мессенджеров и голосовых дипфейков), взлом VPN, RDP и других удаленных доступов (зачастую из-за слабых паролей или утечек), эксплуатацию уязвимостей в ПО — Log4Shell, ProxyShell, уязвимости в Outlook, Microsoft Exchange, Fortinet, атаки на цепочку поставок (через подрядчиков, облачные сервисы или библиотеки ПО), а также шифровальщики (Ransomware) — особенно в атакующих кампаниях на промышленные и муниципальные сети. При этом наиболее опасные уязвимости последних лет — это нулевые дни в VPN-решениях (например, FortiGate, Ivanti), уязвимости в веб-интерфейсах (CVE–2023–34362 в MOVEit), ошибки конфигурации облаков, а также уязвимости в Outlook/Exchange, позволяющие выполнение кода без взаимодействия с пользователем.

«Степень проработанности отдельных атак показывает высокий уровень квалификации, технических возможностей и слаженности организации хакерской группировки. Удаленный доступ к системам управления объектами КИИ, террористические кибератаки на производственные цепочки — все это обратная сторона динамичной эволюции цифрового мира»,— подчеркивает господин Дорофеев.

СТРАТЕГИИ КИБЕРЗАЩИТЫ

Увеличение числа кибератак, включая DDoS и целевые взломы, заставляет компании искать более надежные способы защиты данных и пересматривать подходы к обеспечению безопасности. По мнению Елены Скалозубовой, в условиях стремительных изменений в ИТ-инфраструктуре предприятиям необходимо переходить от «реакционной» модели защиты (когда компания реагирует на уже случившуюся атаку) к проактивной. «На первый план выходят подходы security by design (проектирование киберсистем, в которых меры безопасности интегрированы в архитектуру и программный код и являются его частью), включая безопасную разработку, а также обеспечение „наблюдаемости“ (observability) инфраструктуры для служб эксплуатации и безопасности для своевременного обнаружения атак»,— объясняет господин Ведерников.

Среди других методов госпожа Скалозубова выделяет подход Zero Trust (архитектура, не доверяющая по умолчанию ни одному пользователю или устройству), Threat Intelligence (постоянный анализ данных об угрозах, мониторинг даркнета, выявление признаков атак на ранних стадиях), сегментацию сети и контроль доступа для локализации инцидентов и ограничения распространения вредоносного кода, а также киберучения и симуляции атак (Red Teaming) для проверки готовность персонала и систем к вторжению. «Также ключевое значение приобретают инвестиции в устойчивость ИТ-инфраструктуры (резервное копирование, план реагирования, командные процедуры), поскольку важно не только предотвращение атак, но и минимизация их последствий»,— говорит она.

При этом не менее важным является обучение сотрудников — повышение их осведомленности о фишинге и социальных инженерных атаках помогает снизить риск успешных проникновений, заключает Артур Кондаков, руководитель направления разработки и внедрения систем ИБ в пакет приложений «МойОфис». ■

КОГДА МАЛЫЙ БИЗНЕС СТАНОВИТСЯ БОЛЬШОЙ МИШЕНЬЮ

Киберпреступность давно вышла за рамки «большой игры». Сегодня в фокусе злоумышленников — малый и средний бизнес. Ресурсов там меньше, а вот данные не менее ценные: от клиентских баз до доступа к сервисам. Одна атака способна надолго выбить компанию из колеи, повлечь убытки, проверки и репутационные потери. В таких условиях информационная безопасность — уже не роскошь, а реальная необходимость. Но как защититься, если нет своей ИБ-службы, многомиллионного бюджета и времени на сложные внедрения? Об этом рассказал Константин Родин, заместитель директора по развитию бизнеса компании «АйТи Бастион».

— Насколько актуальна сегодня тема информационной безопасности для малого и среднего бизнеса?

— Актуальность этой проблемы сложно переоценить. Так было всегда, но если раньше основными мишенями киберпреступников были крупные корпорации, то сегодня малый и средний бизнес как никогда «под прицелом». Причина — в ограниченных ресурсах и отсутствии выстроенной ИБ-инфраструктуры. Компании часто вынуждены выбирать между затратами на развитие бизнеса и инвестициями в безопасность. В результате растет риск инцидентов: от утечек персональных данных до компрометации корпоративных систем. При этом последствия именно для небольших компаний могут быть критичными: от штрафов до потери клиентов и репутации.

— Почему МСБ нередко не уделяет достаточного внимания информационной безопасности?

— Причин несколько. Во-первых, ограниченные бюджеты. Во-вторых, нехватка ИТ-экспертизы внутри команды. Нередко ИБ-вопросами занимаются один-два специалиста, а иногда вообще никто — это делегируется на внешний аутсорс. А злоумышленники очень хорошо натренировались на крупных корпорациях, да и технологии на месте не стоят. Стоимость атаки неуклонно снижается. В-третьих, отсутствует понимание, что угрозы реальны. Пока не произойдет инцидент, вопрос безопасности, увы, воспринимается как «второстепенный». Мы стремимся изменить этот подход, предлагая решения, которые учитывают возможности и специфику малого бизнеса.

— Что вы имеете в виду под «спецификой»? В чем отличия защиты ИТ-инфраструктуры малого бизнеса от крупного?

— Очевидно, что основное отличие — в масштабе и гибкости. У МСБ нет собственных ЦОД и распределенных команд ИБ, как у корпораций. Инфраструктура, как правило, размещается на аутсорсинге или в облаке, доступ к системам получают подрядчики, а администрирование нередко совмещается с другими функциями. Поэтому ключевыми становятся простота внедрения, низкий порог входа и высокая эффективность даже при минимальных ресурсах. Именно под такие запросы и был разработан наш новый продукт — СКДПУ НТ Старт, выход которого мы на днях анонсировали.

— Расскажите, что представляет собой это решение и чем оно отличается от флагманского?

— СКДПУ НТ Старт — это легкий вариант нашей основной PAM-платформы СКДПУ НТ, адаптированный под возможности и потребности малого и среднего бизнеса. Он предоставляет базовый, но достаточный набор функций: контроль привилегированного доступа, запись сессий, гибкое разграничение прав через ролевую модель, автоматический анализ активности пользователей, автоматические блокировки нежелательных действий. В отличие от «большого» СКДПУ НТ, который рассчитан на крупные компании с комплексной инфраструктурой (в том числе и на объекты КИИ), Старт не требует длительного внедрения и может быть полностью развернут в срок до четырех часов. Образно говоря, это своего рода «входной билет» в мир PAM-решений — зрелый, но доступный и практичный.



— Каковы основные риски, с которыми сталкивается МСБ при работе с подрядчиками и удаленными администраторами?

— Не секрет, что один из главных рисков — отсутствие контроля. Подрядчику или временно привлеченному специалисту часто выдаются максимальные привилегии, и даже после завершения проекта этот доступ остается (удивительно, но факт!). Нет логирования действий, не видно, кто, когда и зачем подключался. В результате этот специалист (не обязательно, конечно, злоумышленник) может вернуться спустя какое-то время и использовать «открытые двери» для каких-то своих целей. СКДПУ НТ Старт устраняет эту проблему: все действия фиксируются, доступ управляется централизованно, можно ограничить время, IP, команды — все прозрачно и управляемо. И даже если спустя месяц вы решили проверить, не оставил ли он вам «подарок», это легко можно сделать, просмотрев журналы событий и видео его работы на компьютере.

— Система фиксирует действия пользователей. Насколько глубоко это реализовано?

— В СКДПУ НТ Старт реализована полноценная система записи сессий: видеопоток и текстовая команда. Это значит, что можно не только просматривать действия в интерфейсе, но и проанализировать, какие именно команды были выполнены. Дополнительно встроены механизмы анализа сетевых команд: если пользователь вводит потенциально опасную команду или запускает несанкционированное приложение — система может немедленно заблокировать его действия или оповестить администратора. Мы реализовали механизмы, которые позволяют видеть даже запущенные или остановленные процессы на целевой системе. Какие будут ваши действия, если бы вы увидели, что процесс вашего антивируса был завершен пользователем? Я бы немедленно отреагировал.

— Как происходит внедрение системы и сколько времени оно занимает?

— Ключевая идея — это простота. Интеграция, как я уже сказал, занимает от одного до четырех часов. Не требуется глубоких технических знаний или вмешательства в ИТ-инфраструктуру. Мы предусмотрели типовые сценарии, которые позволяют быстро развернуть систему даже без штатного ИБ-специалиста. Это особенно важно для компаний, у которых нет возможности выделить команду на длительный проект.

— Какие задачи автоматизирует СКДПУ НТ Старт?

— Они разные. Во-первых, это автоматическое предоставление и отзыв доступа — из работы исключается «человеческий фактор». Во-вторых, система сама выявляет нежелательную активность и может инициировать блокировку или уведомление. Это особенно полезно в условиях высокой текучести кадров — новички или уволенные сотрудники не смогут использовать старые учетные данные. Кроме того, ведется непрерывный аудит действий, который упрощает внутренние проверки и подготовку отчетности в дальнейшем.

— Есть ли у СКДПУ НТ Старт сертификат ФСТЭК, чтобы его можно было использовать в компаниях?

— Сертификат ФСТЭК на СКДПУ НТ Старт мы не предоставляем. У него другое назначение — обеспечить защиту «здесь и сейчас». Считаю это важным преимуществом именно для малого и среднего бизнеса. Благодаря этому Старт можно быстро внедрять без лишней бюрократии, согласований и затрат. Сертифицированные решения — это, безусловно, важно для госсектора и объектов КИИ, но для МСБ зачастую именно это становится барьером: долго, сложно, дорого. Наш продукт создан именно как легкое, практичное решение. Но при этом оно полностью отвечает требованиям здравого смысла и базовым мерам по ИБ. А если бизнес вырастет и появится необходимость в сертифицированной версии, то у нас есть основное решение СКДПУ НТ, на которое можно потом перейти на максимально выгодных условиях.

— А насколько Старт устойчив к внутренним угрозам?

— Действительно, очень часто киберугрозы исходят не извне, а изнутри: недобросовестный сотрудник, случайная ошибка, незакрытый доступ. СКДПУ НТ Старт позволяет свести такие риски к минимуму. Благодаря блокировке опасных команд и приложений, контролю действий в реальном времени и записи всех сессий поведение каждого пользователя можно отследить и проанализировать. Это не только превентивная защита, но и мощный инструмент реагирования.

— С какими типичными ошибками в безопасности чаще всего сталкиваются компании из сегмента МСБ?

— Прежде всего — это отсутствие учета и контроля доступа. Люди работают под одним логином, доступы не пересматриваются годами, логов нет. Также часто используются устаревшие средства: пароли в Excel единым списком, удаленный доступ через неконтролируемые ПО. Все это создает иллюзию безопасности и эффективности. Наша задача — дать бизнесу простой инструмент, который поможет закрыть эти уязвимости без излишней сложности.

— Планируется ли расширение функциональности СКДПУ НТ Старт в будущем?

— Конечно. Мы активно собираем обратную связь от наших партнеров и заказчиков. Уже сейчас в планах — интеграция с другими решениями по ИБ, расширение взаимодействия по API с корпоративными системами и расширенные отчеты. Но важный принцип остается: система должна оставаться простой и доступной для небольших команд. И иметь, разумеется, потенциал роста.

— Что бы вы посоветовали компаниям, которые только задумываются о защите IT-инфраструктуры?

— Мой совет прост: не надо откладывать. Информационная безопасность — это не роскошь, а базовая необходимость. Даже один инцидент может обернуться катастрофой для бизнеса. Лучше сделать первый шаг, чем бесконечно откладывать путь из-за его кажущейся сложности. Мы предлагаем начать с самого важного — с контроля критически важных для бизнеса систем. А именно — с управления привилегированным доступом, ведь именно здесь сосредоточены наибольшие риски. Дальше — постепенно выстраивать систему безопасности по мере роста бизнеса и требований. Со своей стороны, мы готовы предложить решения, которые соответствуют реальным возможностям компаний и при этом надежно защищают их данные.

РЕКЛАМА, 12+

ОСТОРОЖНАЯ МИГРАЦИЯ НА ОБЛАКО

ПРОВАЙДЕРЫ И АНАЛИТИКИ ПРОГНОЗИРУЮТ СТРЕМИТЕЛЬНЫЙ РОСТ СПРОСА НА ОБЛАЧНЫЕ РЕШЕНИЯ: ЕЖЕГОДНЫЙ ПРИРОСТ МОЖЕТ СОСТАВИТЬ ПОЧТИ ТРЕТЬ В ПРОЦЕНТНОМ СООТНОШЕНИИ. ПРИ ЭТОМ НЕКОТОРЫЕ ИГРОКИ РЫНКА СКЕПТИЧЕСКИ ОТНОСЯТСЯ К ТАКИМ ЗАЯВЛЕНИЯМ, ЗАМЕЧАЯ, ЧТО РЕАЛЬНЫЙ УРОВЕНЬ КОММЕРЧЕСКОГО ИСПОЛЬЗОВАНИЯ ОБЛАКОВ ПОКА НЕВЫСОК. ПРОБЛЕМА В ВОПРОСАХ БЕЗОПАСНОСТИ И ДАЖЕ В РОССИЙСКОМ МЕНТАЛИТЕТЕ. ЭКСПЕРТЫ СХОДЯТСЯ ВО МНЕНИИ, ЧТО ДРАЙВЕРОМ ЭТОГО РЫНКА СТАНЕТ МАЛЫЙ И СРЕДНИЙ БИЗНЕС. В ТЕНДЕНЦИЯХ ПЕРЕХОДА НА ОБЛАЧНУЮ ИНФРАСТРУКТУРУ, МОДЕЛЯХ ОБСЛУЖИВАНИЯ, РИСКАХ И ВОЗМОЖНОСТЯХ РАЗБИРАЛСЯ КОРРЕСПОНДЕНТ GUIDE. АЛИСА МАЛЬЦЕВА

Рынок облачных услуг за 2024 год в процентном соотношении увеличился на 36,3%, а в денежном — на 165,6 млрд рублей (по статистике «DataPy Облако»). В перспективе темпы прироста не сильно уступят и составят 30% до 2028 года (усредненная оценка, так как IDC и Gartner указывают 28–34%) за счет ухода иностранных игроков, а по оценке компании «МойОфис» — 21%.

Прогнозируемый стремительный рост рынка облачных технологий в России до 2028 года во многом объясняется эффектом низкой базы, рассуждает Руслан Заединов, директор департамента «Облака и данные» компании «Рексофт». «Несмотря на активный PR со стороны провайдеров, реальный уровень коммерческого использования облаков пока невысок. Так сложилось в нашей психологии: мы предпочитаем иметь свое, а не арендовать, у нас нет глубокой традиции бизнес-партнерства. Крупные компании, которые могли бы стать драйверами развития облачных вычислений как потребители, предпочитают строить собственные решения вместо использования рыночных»,— объясняет эксперт.

Среди ключевых препятствий он называет устойчивые позиции внутренних IT-подразделений крупных компаний, обслуживающих своих корпоративных клиентов. Фактически динамика рынка будет определяться развитием малого и среднего бизнеса, так как именно сегмент МСБ может стать основным драйвером роста облачных сервисов. Однако если экономика останется ориентированной на крупные корпорации (включая государственные), то реальный рост публичных облаков окажется под вопросом.

По мнению IT-директора DataSpace Константина Симонова, драйвером роста использования облаков может стать в целом экономическая ситуация. Так, на фоне санкционного давления и денежно-кредитной политики компании сокращают свои расходы, так как не могут нести крупные капитальные затраты на покупку и модернизацию собственной IT-инфраструктуры. Кроме того, очевиден дефицит IT-специалистов.

«Мы уже не первый год видим, как бизнес массово переходит от собственных серверных комнат к облачным сервисам. Это происходит по нескольким причинам. Глобальная нестабильность заставила компании задуматься о гибкости и „отказоустойчивости“ IT-инфраструктуры. Пандемия и последующие события наглядно показали, что бизнесу нужна возможность быстро менять стратегию и легко масштабироваться. Если у тебя собственное „железо“, перестроиться быстро и безболезненно практически невозможно. Облако же позволяет это делать буквально за пару кликов: нужно больше ресурсов — пожалуйста, в сезонный спад можно без проблем уменьшить нагрузку и не переплачивать»,— комментирует Максим Захаренко, CEO «Облакотека».

Однако, по словам господина Захаренко, главный вопрос в безопасности данных. По большей части, все зависит от подхода и выбранного провайдера. Хорошо, если облачный провайдер на старте предложит инструменты защиты данных, резервного копирования, аварийного восстановления.

«В 2009 году начался тренд по уходу в публичные облака части решений для бизнеса с SaaS/PaaS моделями сбыта. Но до сих пор крупные компании зачастую наотрез отказываются от публичных облаков, связано это с рисками утечки данных и колоссальными штрафами»,— добавляет Виталий Янко, основатель сообщества IT-экспортеров ExportNow, консалтинга по росту технологических бизнесов SoftwareLead и инвестбутика SPb Founders.



ЕВГЕНИЙ ПАВЛЕНКО

ТРЕНД ПО УХОДУ В ПУБЛИЧНЫЕ ОБЛАКА НАЧАЛСЯ В 2009 ГОДУ, ОТМЕЧАЮТ ЭКСПЕРТЫ

Он отмечает, что касательно аспекта безопасности существуют компании (в Петербурге, например, CloudAdvisor), которые могут аудировать настройку публичных облачных сервисов в контуре компании и подсвечивает угрозы ИБ. В целом же, по мнению спикера, сейчас только микробизнес и малый бизнес без сомнений выбирают публичные облака, в то время как средний бизнес очень долго, чаще дольше чем крупный, задумывается о переходе к бизнес-приложениям.

«С правильными инструментами рисков становится меньше. Из того, что сейчас выбирают чаще всего, трендом стала комбинация публичного облака и гибридной инфраструктуры. Компании хотят одновременно получить доступ к быстрым и масштабируемым мощностям, но и сохранить часть критичных данных под собственным контролем»,— отмечает господин Захаренко.

Роман Блонов, CEO Proptech Solutions, тенденцией называет переход к многооблачной стратегии: «Это позволяет избежать зависимости от одного поставщика и обеспечивает повышенный уровень информационной безопасности».

«При выборе облачного провайдера важно учитывать несколько факторов. Во-первых, соответствие требованиям регуляторов: оператор должен гарантировать локализацию и защиту данных по российскому законодательству. Во-вторых, надежность и независимость: сбои у провайдера или проблемы с каналами связи могут приводить к простоям, а зависимость от зарубежной инфраструктуры — к внезапной потере доступа из-за санкций. Поэтому многие компании распределяют нагрузки между несколькими площадками (мультиоблачность) для обеспечения непрерывности работы. Все больше облачных провайдеров предлагают решения, построенные на отечественных производителей аппаратных мощностей, а также OpenStac-решения для виртуализации и управления контейнеризацией, это позволяет им сохранять стоимость услуг за счет внутренней экспертизы и предлагать автоматизацию развертывания инфраструктуры по принципу „Инфраструктура как код“»,— говорит Илья Глейкин, ведущий бизнес-консультант компании «Арбайт».

МОДЕЛИ ОБСЛУЖИВАНИЯ

На протяжении ряда лет наиболее востребованным остается базовое решение типа IaaS, представляющее собой аренду вычислительных ресурсов, позволяющую быстро масштабировать корпоративную IT-инфраструктуру, рассказывает Валентин Соколов, IT-директор облачной платформы RCloud by 3data. Он добавляет, что среди прочих популярных сервисов — виртуальные рабочие места с поддержкой GPU, частные выделенные облака, услуги резервного копирования данных. «Следует подчеркнуть, что большинство заказчиков наряду с традиционными услугами IaaS приобретают дополнительно защиту от кибератак Anti-DDoS. Ранее проблемы информационной безопасности зачастую занимали второстепенное место среди приоритетов бизнеса, однако сегодня значительно увеличилось число организаций, серьезно оценивающих надежность облачной инфраструктуры перед миграцией критически важных приложений и данных. Компании проводят тщательную оценку существующих угроз и риск-факторов, обращают особое внимание на наличие у поставщиков соответствующих международных стандартов и сертификатов (ISO 27001, PCI DSS и другие)»,— говорит эксперт.

Если IaaS больше используется холдингами, то средний и малый бизнес выбирает решения SaaS (Software as a Service): например, «1С: Облако», Microsoft 365, Google Workspace, отмечает Алексей Дмитриев, руководитель отдела корпоративного развития компании «МойОфис». Они популярны из-за простоты внедрения. А вот PaaS (Platform as a Service), например T1 Cloud или MTS Cloud, упрощают разработку, избавляя от необходимости управлять серверами. Также в ходу гибридные и мультиоблачные стратегии: бизнес комбинирует публичные и приватные облака, чтобы соблюдать регуляторные требования (например, 152-ФЗ) и снижать риски вендор-локинга.

«Один из трендов сегмента — появление новых cloud-native СУБД, которые позволяют анализировать большие объемы данных еще быстрее и эффективнее, используя ресурсы облака и хранилища S3 Storage (S3 Storage — объектное хранилище, которое позволяет хранить огромные объемы данных в исходном формате без иерархии и разбивки на отдельные каталоги и без ограничений по масштабированию)»,— акцентирует Антон Близгарев, директор по развитию облачного бизнеса Arenadata.

«Бизнес стал чаще выбирать российские облачные сервисы — они более гибкие, стоимость подписки сильно ниже, чем у западных аналогов, нет проблем с оплатой. Кроме того, российские сервисы точно никуда не уйдут, и на них можно строить долгосрочную IT-стратегию»,— добавляет Евгений Перов, директор по продукту в корпоративном мессенджере Compass.

ВАЖНОСТЬ ДЕТАЛЕЙ

Помимо организации информационной безопасности, существуют еще нюансы в использовании облаков. «Прежде всего нужно понимать, что расходы в облаке — это операционные затраты, или OPEX. Если заказчику необходимо растить капитальные затраты, облако этого не даст. Также не все готовы платить ежемесячно, или если бюджет на IT непостоянный, это может приводить к неудобству оплаты за облачные сервисы,— комментирует господин Близгарев.

Алексей Гришин, технический директор BPMSoft (входит в IT-холдинг Lansoft), обращает внимание, что необходимо выстроить ИБ-архитектуру. «На прикладном уровне особое внимание уделяется защите данных и каналов их передачи. Обязательна сегментация сети, особенно в случае сложной распределенной инфраструктуры, где важно ограничить возможное горизонтальное перемещение в случае инцидента. Отдельный фокус — защита API. Наконец, ключевое значение имеют процессы мониторинга и реагирования»,— указывает эксперт.

Также для некоторых организаций, особенно в удаленных или промышленных зонах, доступ к высокоскоростному интернету может быть ограничен, что затрудняет использование облачных решений. ■

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
Василиса Сатирская — 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: Евгений Павленко