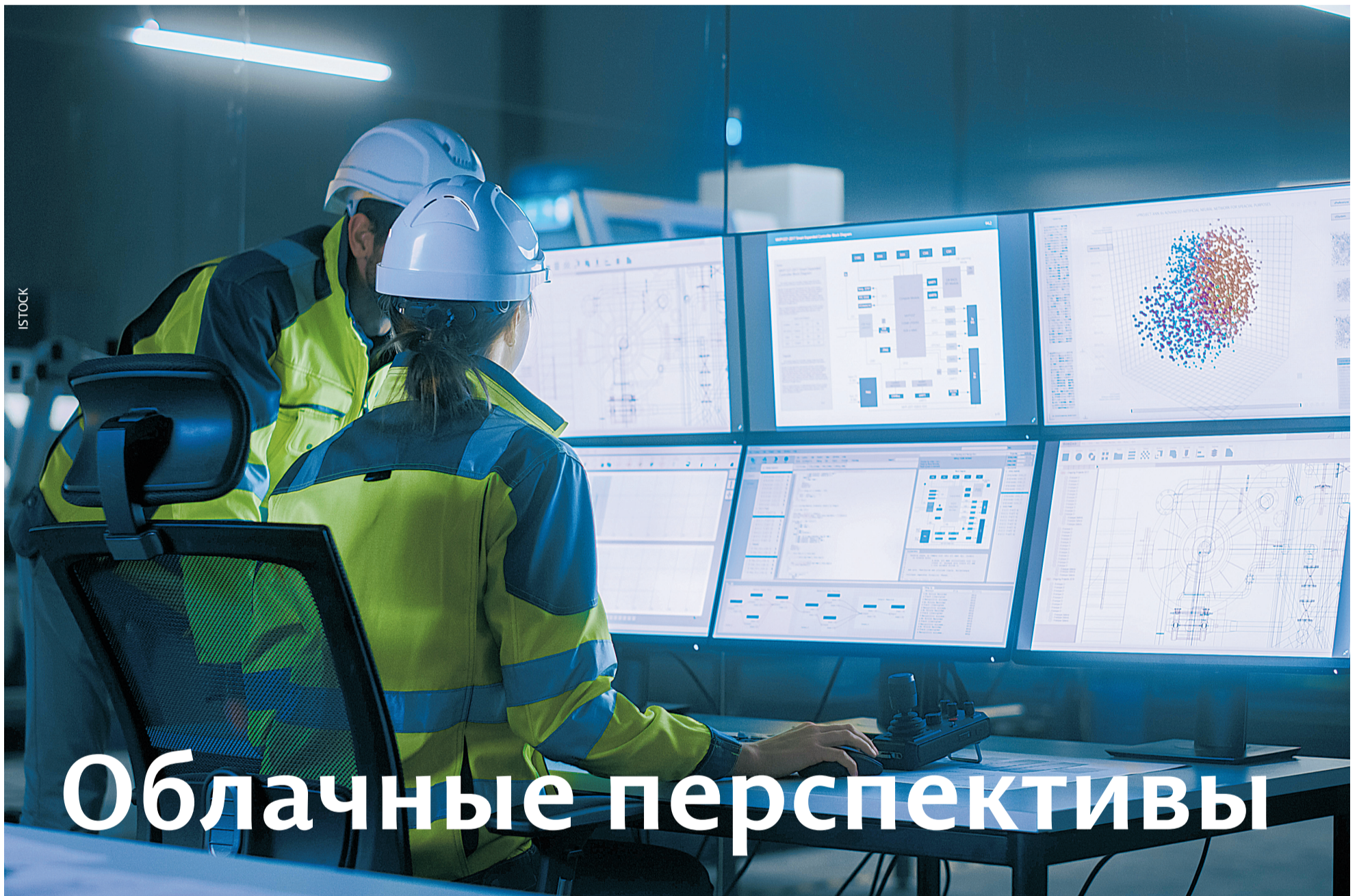


Промышленность 4.0: облачные технологии

партнер выпуска: **Yandex Cloud**



Облачные перспективы

Почему предприятия используют облака для развития бизнеса

Егор Сонин

В 2024 г. 35% российских промышленных компаний увеличат инвестиции в цифровое и технологическое развитие. Такую оценку приводят аналитики Института статистических исследований Высшей школы экономики, которые проанализировали работу более 1000 предприятий. Ключевое направление инвестиций – исследование и разработка новых технологий (НИР). 52% респондентов считают, что НИР станет драйвером для развития производства в 2024 г. «Ведомости&» опросили промышленников и выяснили, какие технологии востребованы для решения их задач.

Облака как способ ускорить производство

По оценке Gartner, более 50% предприятий в мире будут использовать облачные платформы для ускорения бизнес-инициатив уже в 2028 г. Россия тоже в тренде: компаниям нужны гибкие инструменты для автоматизации заказов, анализа данных, ускорения разработки нового программного обеспечения и других задач. По данным исследования облачной платформы Yandex Cloud и «УльтимаТека», 40% крупных предприятий уже внедрили в процессы публич-

ные облака, но только 14% планируют расширить сферу их применения. Отчасти из-за того, что в 2019–2021 гг. российские промышленные компании потратили до 500 млрд руб. на оборудование для цифровизации и быстро отказались от уже вложенных инвестиций в свою инфраструктуру пока проблематично. Однако крупные предприятия все равно рассматривают облака как инструменты для ускорения цифровизации.

Так, в компании «Алроса» облачные решения обеспечивают гибкость, масштабируемость и удобство доступа к необходимым ресурсам, что делает их популярным выбором для ориентированных на внешних пользователей и разработчиков проектов, говорит Игорь Лабудев, руководитель центра компетенций Центра разработки и тестирования ООО «Алроса ИТ».

Отраслевой фокус

«Многие сценарии работы в облаке универсальны для всех крупных компаний, но в промышленности есть и индустриальная специфика, – рассказывает Павел Приедитис, директор по работе с промышленными компаниями Yandex Cloud. – Во-первых, это необходимость ра-

ботать с бизнес-приложениями и учетными системами типа SAP, которые требуют большого количества вычислительных ресурсов. Во-вторых, это необходимость анализировать большие массивы данных, в том числе производственных с датчиков интернета вещей. В-третьих, предприятия часто территориально распределены и работа в облаке упрощает взаимодействие, обмен информацией».

В облаке можно создать закрытую среду, которая позволяет организовать единый контур и взаимодействие, получать и обрабатывать данные оборудования, датчиков, производственных процессов и т. п., говорит Юрий Швыдченко, директор технологической практики компании «Технологии доверия».

Российские промышленные компании чаще всего используют облачные сервисы для быстрого старта проектов – размещают в облаке корпоративные порталы, e-com магазины. Например, на облачной платформе работает портал «Платферрум» от «Северстали». Это маркетплейс для покупки и продажи металлопроката, он построен на облачных сервисах, рассказывает Приедитис

Безопасное производство

Как промышленники соблюдают баланс между инновациями и безопасностью данных

Егор Сонин

Число кибергруппировок, атакующих Россию, в апреле 2024 г. выросло более чем на 20%, отмечают эксперты по информационной безопасности (ИБ) BI.ZONE. По итогам 2023 г. количество инцидентов в сфере ИБ увеличилось более чем на 60%, причем большая их часть пришлась на промышленность, подсчитала «Лаборатория Касперского». Как в условиях роста угроз сохранять безопасность IT-инфраструктуры, но при этом не снижать темпы разработки новых технологий? «Ведомости&» поговорили об этом с директорами по ИБ крупных промышленных предприятий.

Больше безопасности

В России, по оценке «Лаборатории Касперского», в прошлом году больше всего кибератак пришлось на сферу производства (24%). Это одна из причин, по которой промышленный сектор активно увеличивает инвестиции в ИБ – как в инфраструктуру, так и в обучение специалистов. Так, по данным совместного исследования Yandex Cloud и компании «Деловые решения и технологии» (ДРТ), в 2023 г. у большинства из 300 опрошенных российских промышленных компаний затраты на ИБ-проекты по сравнению с прошлым годом выросли в среднем на 20%. Эти цифры подтверждаются и ростом спроса на ИБ-продукты вендоров. По итогам 2023 г. группа сервисов безопасности Yandex Cloud стала лидером по росту темпов потребления среди других сервисов – этот показатель вырос в 2,5 раза, отмечают в компании.

Опрос ДРТ и Yandex Cloud среди руководителей отделов ИБ показал, что большинство промышленных компаний вкладывают средства в продление лицензий на ПО, масштабирование средств защиты, а также замену устаревшего оборудования и систем. Представители ряда компаний с 2023 г. сосредоточились на внедрении конкретных решений, например центра управления безопасностью (SOC, Security Operation Center). Другие статьи расходов – проведение искусственных фишинговых атак. Некоторые российские компании начали создавать собственные университеты и крупные платформы для обучения своих специалистов ИБ.

«Цель нашей команды не изменилась – это обеспечение кибербезопасности бизнеса, но сейчас специалистам требуется больше технических компетенций, чтобы детально понимать суть всего стека применяемых технологий и обеспечивать эффективную защиту».



Антон Кокин
директор по инфраструктуре и кибербезопасности Трубной металлургической компании

В частности, по его словам, это технологии виртуализации и контейнеризации (создание программных пакетов, способных работать на всех типах устройств и операционных систем. – «Ведомости&»), нейронные сети, машинное зрение. «К примеру, чтобы грамотно и эффективно обеспечить безопасную среду контейнеризации, специалист по ИБ должен хорошо ориентироваться в принципах работы специализированных программ Docker и Kubernetes», – пояснил эксперт.

Расходы на безопасность увеличили не только промышленные компании, но и разработчики технологий, с ко-

торыми они работают. Так, облачный провайдер Yandex Cloud инвестировал в 2023 г. в развитие ИБ более 820 млн руб. Это затраты на разработку собственных сервисов и рекомендаций в области защиты данных, проведение аудитов, повышение уровней соответствия ключевым стандартам индустрии и др., поясняют в компании. «Мы выстраиваем работу так, чтобы помогать компаниям-клиентам обеспечивать защиту на всех уровнях работы в облаке: самой облачной платформы, инфраструктуры пользователей и приложений и систем клиентов. Ресурсы располагаются в собственных дата-центрах, доступ к которым и работа в которых строго регламентированы. Наша задача – постоянно расширять перечень средств защиты и делать их наиболее доступными, чтобы они не требовали дополнительного администрирования, интеграций», – говорит Евгений Сидоров, директор по ИБ Yandex Cloud. Так, в 2023 г. компания запустила новые сервисы для хранения секретов, сканер уязвимости и собственное решение для защиты веб-приложений от DDoS-атак.

Ландшафт киберугроз

Число атак программ-вымогателей на IT-инфраструктуру промышленных предприятий за 2023 г. выросло на 50–70%, подсчитала компания Infowatch. Значительно увеличилась доля случаев, когда внедрение вредоносного ПО и DDoS-атаки проводились по заказу: злоумышленники предоставляли программы-вымогатели или сервис по организации DDoS-атак как услугу. Автоматизированных нападений на промышленные предприятия стало меньше, зато количество атак программ-вымогателей, управляемых человеком, выросло более чем в 3 раза, отметили в Infowatch.

«Количество атак на промышленные предприятия начало расти с 2022 г. – это были преимущественно DDoS, фишинг и атаки на Web. В нашем случае рост был более чем в 2 раза, но со временем ситуация стабилизировалась. Типы угроз ИБ за последние несколько лет мало изменились – это по-прежнему DDoS и различные попытки найти уязвимости в инфраструктуре компании. При этом специалистам по безопасности приходится быстрее адаптироваться к меняющимся условиям».



Андрей Нуйкин
начальник отдела обеспечения безопасности информационных систем из блока вице-президента по IT «Евраз»

В ТМК также заметили увеличение количества кибератак. Кокин отмечает, что это закономерный процесс, особенно с учетом масштабов цифровизации промышленных компаний и скорости развития информационных технологий. «Важным становится оперативно получать актуаль-

ную информацию как о самих угрозах, так и о мерах защиты от них», – подчеркивает эксперт.

Так или иначе сейчас кибербезопасность важна всем компаниям, которые заинтересованы в непрерывности бизнес-процессов, считает Кокин. С ним соглашается Нуйкин: «Наблюдая за инцидентами по всему миру, мы видим, что пренебрежение ИБ может дорого обойтись компании. Остановка производства влечет и финансовые, и репутационные риски».

Скорость решает все

Перед крупными промышленными компаниями стоит масштабная цель – разработать принципиально новые цифровые продукты, решающие специализированные задачи горнодобывающей и металлургической промышленности. Для этого при поддержке государства появились индустриальные центры компетенций (ИЦК). Реализация проектов ИЦК началась в 2023 г., когда правительство утвердило 143 особо значимых проекта, из которых 32 получили грантовую поддержку из бюджета – почти 20 млрд руб. Большинство этих решений должны быть представлены и внедрены в производство не позднее конца 2025 г., писал портал TAdviser со ссылкой на материалы круглого стола, прошедшего в Совете Федерации 16 апреля 2024 г.

Один из способов ускорить выпуск новых продуктов – применение облачных платформ для запуска инновационных проектов, отмечает Павел Приедитис, директор по работе с промышленным сектором Yandex Cloud. По данным исследования компании «УльтимаТек», 73% российских промышленных компаний реализовали хотя бы один проект в облаке. Облачные сервисы используют команды разработки промышленных компаний, для которых важны такие показатели, как скорость выпуска новых цифровых продуктов на рынок – time-to-market. Значимый критерий при переходе в публичный облако и выборе провайдера – это обеспечение безопасности, говорится в исследовании.

Важной задачей для ИБ в промышленных компаниях остается соблюдение баланса между безопасностью и функциональностью бизнеса, считает Нуйкин. Это касается ряда технологий, в частности работы с публичными облачными платформами.

«Облачную инфраструктуру мы считаем частью нашей географически распределенной IT-инфраструктуры, и, соответственно, к ней предъявляются все требования наших политик и стандартов в области ИБ», – отмечает Кокин. При этом в первую очередь необходимо точно понимать, каким образом провайдер обеспечивает безопасность облака и по каким границам проходит зона разделения ответственности. По словам эксперта, при решении задач в облаке необходимо использовать комплекс ИБ-инструментов, в который входит антивирусная защита и контроль доступа из внешних информационных систем. «Отдельно стоит отметить необходимость подробной регистрации и мониторинга событий безопасности в облаке», – подчеркивает Кокин.

Ответственность за безопасность систем, которые используют в работе облачные сервисы, провайдер и клиент несут совместно, соглашается Сидоров. Провайдер гарантирует безопасность сервисов и доступность инфраструктуры, но права доступа к ресурсам клиента, в том числе к виртуальным машинам, контролирует только он сам.

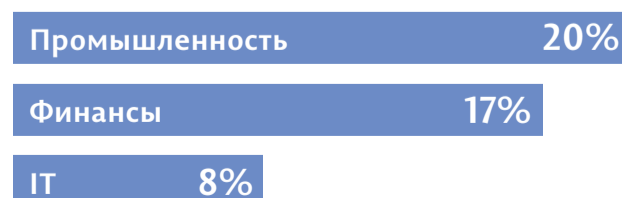
Одна из ошибок компаний заключается в том, что они не используют возможности встроенных средств защиты, доступных в облаке, считает Сидоров. Также клиенты пренебрегают включенными и настроенными средствами аудита и правильной конфигурацией ресурсов. В результате подобных ошибки, например, в мае 2023 г. в открытом доступе оказались данные более чем 2 млн владельцев Toyota, приводит пример эксперт.

«Идеального решения нет, – полагает Нуйкин. – Наиболее эффективной, на мой взгляд, является эшелонированная защита. Используя решения от разных производителей, компания усложняет себе администрирование, но при этом продукты «страхуют» друг друга. Таким образом, вероятность, что мы сможем выявить и нейтрализовать угрозу, выше».

Безопасность будущего

В будущем вектор развития облачной ИБ будет направлен в сторону полной автоматизации процессов кибербезопасности, в том числе с помощью технологий искусственного интеллекта, прогнозирует Кокин. С ним соглашается Нуйкин, добавляя, что по мере появления и развития новых технологий будет расти необходимость в защите от их неправомерного использования. Он надеется, что через пять лет вырастет новое поколение амбициозных специалистов по ИБ, которые смогут эффективно выстраивать процессы противодействия киберугрозам, и вопрос кадрового дефицита будет закрыт. &

Самые атакуемые отрасли в 2023 г.



Источник: «Лаборатория Касперского»

Как ускорить разработку промышленного искусственного интеллекта

Опыт компании «Русал» по использованию облачных сервисов

Алексей Охлопков

Эффект от внедрения решений на базе искусственного интеллекта (ИИ), в том числе машинного обучения, в России может достичь 4,2–6,9 трлн руб. к 2028 г. – такую оценку приводят аналитики «Яков и партнеры» в исследовании «Искусственный интеллект в России – 2023». Около 75% потенциала приходится на шесть ключевых для российской экономики отраслей, в числе которых – добывающая промышленность. Опрос показал, что в 68% компаний внедрение решений на основе ИИ за последний год в среднем оказало влияние на 1–5% от EBITDA (прибыль до вычета процентов, налогов, износа и амортизации). О том, как компании создают такие технологии и как эти разработки можно ускорить с помощью облачных сервисов, «Ведомости&» узнали у производителя алюминия – компании «Русал».

Компания «Русал» применяет различные системы на основе ИИ с 2018 г. В прошлом году компанию признали первым номинантом национальной премии «Лидеры в сфере искусственного интеллекта» за проект по мониторингу выбросов загрязняющих веществ.

Для работы над новыми проектами IT-команде нужно наращивать вычислительные мощности, однако закупка и доставка серверов, развертывание инфраструктуры, в том числе строительство собственных центров обработки данных, – долгий, трудозатратный и недостаточно гибкий процесс.

Если для эксплуатации цифровых продуктов с ИИ используется только собственная инфраструктура (on-premise), то для ускорения темпов разработки «Русал» выбрал гибридную модель IT-инфраструктуры: часть проектов машинного обучения компании разрабатывается на собственных мощностях, другая – с использованием облачной платформы, предоставленной Yandex Cloud.

Интеллект для промышленности

Сейчас у «Русала» в работе более трех десятков проектов с использованием ИИ. Несколько проектов уже внедрено в промышленное производство, один вышел на стадию масштабного тиражирования. Обеспечивать качество разработки и скорость внедрения, а также снижать стоимость эксплуатации цифровых продуктов с ИИ «Русалу» помогает использование решений в области операций машинного обучения – MLOps. Это подход к машинному обучению, в котором применяются практики непрерывной разработки. Модели машинного обучения тестируются и разрабатываются в изолированных экспериментальных системах, а затем готовые и проверенные алгоритмы запускаются в производственной среде.

Три контура безопасности «Русала»

Разработка информационных систем исключительно на физических серверах компании – on-premise – ограничивает динамичность масштабирования доступных вычислительных ресурсов, отмечают в «Русале». Поэтому компания выбрала гибридный трехконтурный вариант разработки новых ИИ-решений.

Первый контур – внутренний. MLOps-платформа «Русала» реализована на базе технологий с открытым кодом (open source framework) SinaraML. Платформа используется как для собственной разработки и обучения ИИ-моделей, так и для их последующей эксплуатации – мониторинга, переобучения и пр.

Второй контур – промежуточный. На мощностях Yandex Cloud развернут экземпляр MLOps-платформы «Русала» с возможностью динамического управления ресурсами. Они нужны как для обучения ИИ-моделей, так и для тестирования решений, которые разрабатывают внешние подрядчики.

Как создают технологии машинного обучения

«Вначале формулируются бизнес-требования – прикладная задача, которую компании необходимо решить с помощью методов машинного обучения. Когда задача определена, начинается сбор данных, разметка и очистка. В отличие от классического программирования, где специалист прописывает алгоритм действий, в машинном обучении алгоритм формируется на основе данных. Данные необходимо подготовить специальным образом: проверить, насколько они полны, актуальны и обладают ли необходимым качеством для реализации проекта.

Данные можно условно разделить на два вида: структурированные данные представлены в виде таблиц, неструктурированные – в виде изображений, видео, звука или текстовой информации. В классическом машинном обучении работают со структурированными данными. Например, это могут быть данные о доходах компании.

Следующий шаг – отладка модели. Данные разделяют на две или три выборки в зависимости от подхода: обучающую, валидационную и тестовую.

Если компания проводит эксперименты, обучается много разных моделей и применяется много разных подходов. Лучшую модель выбирают с помощью валидационной выборки. На базе валидационной выборки выбирают лучшую модель. Затем еще раз проводят ее обучение на обучающей и валидационной выборках одновременно. Тестовая выборка используется, когда модель полностью готова, решение построено и компании нужно рассчитать конечные метрики качества. Финальный замер происходит на тестовой выборке, чтобы удостовериться, что выбранная модель оптимальна», – рассказывает Дмитрий Рыбалко, продуктовый архитектор ML-сервисов Yandex Cloud.

Третий контур – внешний. Подрядчики компании, разрабатывающие цифровые продукты с ИИ, самостоятельно разворачивают на своих мощностях open source framework SinaraML, разрабатывают, обучают и упаковывают в микросервисы ИИ-модели для «Русала».

Такая структура позволяет гибко и динамично масштабировать задействованные вычислительные мощности для ресурсоемкого обучения больших моделей ИИ. Кроме того, провести проверку безопасности решений возможно вне технологического контура компании, что существенно снижает риски.

«Уникальными характеристиками такого подхода является значительное снижение затрат и времени как на разработку, так и на передачу результатов работ, их тестирование и внедрение в продуктовую и последующую промышленную эксплуатацию. Все пайплайны (регламентированный и документированный процесс выполнения типовых задач. – «Ведомости&») разработки и тестирования архитектур инфраструктурных решений бесшовно переносятся между любыми экземплярами платформы», – отмечает Михаил Граденко, директор департамента технологий ИИ «Русала».

На повышенной скорости

Ускорение разработок и тестирования – главный результат интеграции с облаком. К примеру, процесс адаптации подрядчиков к разработке в корпоративном стеке – наборе технологий «Русала» стал многократно быстрее, приводит пример Граденко. Облачные сервисы позволяют IT-команде «Русала» справляться с большим объемом работы. Такой подход обеспечивает защиту данных во всех сегментах инфраструктуры и контроль над процессом разработки.

Еще один фактор экономии времени заключается в том, что цикл закупки и разворачивания инфраструктуры on-premise значительно дольше, чем цикл согласования и выделения облачных мощностей. С помощью облака можно очень быстро начинать эксперименты по разработке новых решений, пока согласовываются и осуществляются закупки необходимого оборудования, говорит Граденко.

По его словам, инструментарий платформы позволяет при разработке сохранять историю изменений кодов отдельных компонентов и пайплайна целиком. В итоге при передаче результатов работ отдается не только обученная модель, но и готовый пайплайн для обучения модели (конвейер по производству моделей для конкретного цифрового продукта. – «Ведомости&»), а также вся история версий всех компонентов, данных и экспериментов по обучению.

Таким образом, использование облачных технологий для разработки, тестирования и внедрения новых ИИ-решений позволяет ускорить процесс на всех этапах, поддерживая при этом высокий уровень информационной безопасности. В будущем «Русал» планирует рассмотреть и другие возможности применения сервисов Yandex Cloud, например облачный доступ к высокопроизводительным графическим процессорам (GPU), что позволит динамично масштабировать вычислительные ресурсы, говорит Граденко. &

Чем полезно облако при работе с машинным обучением

«Для специалистов Data Science важны отказоустойчивость инфраструктуры и возможности масштабирования, которые дает облачная платформа. Некоторые команды работают над проектами удаленно, и это тоже удобнее делать в облаке. Но есть и специфические для машинного обучения преимущества. Во-первых, облачные платформы предоставляют широкий выбор «железа», в том числе наиболее мощных конфигураций. Покупка такой физической инфраструктуры потребовала бы больших вложений, при этом физические серверы используются не всегда оптимально, простаивая часть времени. Во-вторых, оборудование нужно разместить в подготовленном месте и постоянно обслуживать, а облачная платформа берет работу с оборудованием на себя и гарантирует высокий уровень доступности сервисов. Также облачная инфраструктура позволяет отказываться от ресурсов, когда они не нужны. Это особенно важно для проектов, в которых сложно заранее рассчитать необходимое количество мощностей», – поясняет Дмитрий Рыбалко, продуктовый архитектор ML-сервисов Yandex Cloud.

Облачные перспективы

01 → Гибридная сила

Развитие промышленной IT-инфраструктуры в России пойдет по гибридной модели, уверены 70% промышленных компаний, опрошенных в исследовании Yandex Cloud и «УльтимаТека». Гибридной модель называется из-за того, что крупные компании держат критичные данные на своих серверах, а эксперименты проводят в публичном облаке, объясняет Приедитис. Это обусловлено регуляторными требованиями и необходимостью повышенной защиты критичных систем, поясняют авторы исследования.

Гибридный подход набирает популярность, так как позволяет хранить чувствительные данные у себя, но вести разработку, тестирование и апробацию новых технологий в публичном облаке, отмечает Швыдченко. При этом компании все так же могут эффективно справляться с нагрузками и повышать доступность и непрерывность систем, говорит он.

Для того чтобы использовать возможности гибрида, необходимо провести категоризацию данных – определить, какие данные и бизнес-процессы можно переносить в облако, а какие нельзя, говорит Приедитис. Если взять любую систему, например, класса ТОиР (техническое обслуживание и ремонт), то сами по себе данные о ремонте некритично обрабатывать в облаке. Однако, продолжает Приедитис, в системе могут находиться и персональные данные, и инструкции, и регламенты ремонта, и информация об авариях и происшествиях, которые предприятия пока не готовы держать на публичной платформе.

При этом, отмечает Приедитис, можно построить работу таким образом, чтобы забирать из такой системы только часть данных и использовать их для анализа. Это возможно, если согласовать такой проект со службой контроля рисков и отделом информационной безопасности (ИБ), подытоживает эксперт.

Искусственный интеллект предприятия

В 2022 г. российские компании вложили в цифровизацию 480 млрд руб., подсчитало АНО «Цифровая экономика». Промышленные компании внедряют технологии машинного обучения, чтобы более оптимально выстроить производственные процессы, а также процессы закупок и логистики, говорит Приедитис. Кроме того, технологию используют для ускорения бизнес-процессов и задач, связанных с прогнозированием поломок оборудования и выявлением брака на производстве. Эксперт отмечает, что сейчас набирают популярность большие языковые модели (LLM) типа GPT. Один из популярных сценариев использования этих технологий – корпоративный поиск информации. Например, искусственный интеллект (ИИ) может по запросу проверить документацию и найти в ней ответ на вопрос со ссылкой на источник. Есть вариант, когда LLM может отвечать и на вопросы, связанные с технологическими процессами, например составлять краткое содержание документации, поясняет Приедитис.

Несмотря на то что нейросети и технологии машинного обучения активно развиваются, они все еще остаются определенной экзотикой для промышленных предприятий, сетует Швыдченко. Задач, которые можно решить с помощью ИИ, много, но пока он используется точечно. Например, это машинное зрение в части промышленной безопасности или цифровые двойники.

Другая проблема в том, что сбор данных и обучение алгоритмов требуют огромных вычислительных мощностей и собственных хранилищ данных, которые могут позволить себе далеко не все, продолжает Швыдченко. Поэтому вместо того, чтобы создавать собственную инфраструктуру

для разработки, компании предпочитают облачные платформы. Они делают ИИ и машинное обучение доступнее, дают возможность с минимальными затратами и ресурсами, даже при ограниченной компетенции, тестировать те или иные гипотезы, их применимость и проверять эффективность, заключает он.

Аналитика данных

Размер глобального рынка облачных хранилищ данных оценивается в \$117,12 млрд в 2024 г. и, как ожидается, будет расти на 24% ежегодно до 2029 г., прогнозирует Mordor Intelligence.

Хранилища пользуются популярностью, так как дают возможность построить распределенную IT-архитектуру, которая позволяет обрабатывать данные в режиме реального времени максимально близко к источникам, отмечает Швыдченко. По его словам, это позволяет контролировать бизнес-процессы без отправки сырой информации в центры обработки данных. Последнее важно, поясняет Приедитис, потому что у руководителей промышленных компаний есть задача комплексно управлять предприятием, а для этого нужно опираться на актуальные данные. Выполнение производственного плана зависит от многих факторов и руководители хотят понимать, как они вместе влияют на финансовые показатели, указывает он.

Здесь им помогает облако. В нем аналитические проекты запускаются быстрее и могут подстраиваться под изменения источников данных или появление новых критериев, подчеркивает Приедитис. Он говорит, что аналитика – это живой, постоянно меняющийся «организм», который требует моментальной интеграции нововведений и изменений. На облачной платформе это делать быстрее и дешевле. С ним соглашается Швыдченко, отмечая, что с точки зрения цифровизации перед компаниями остро стоят вопросы аналитики всех данных с мгновенной оценкой решений в реальном времени, сбора всей информации и экспертизы, а также быстрой реализации решений и координации действий.

«Компания «Норникель» начала внедрение облачных сервисов для решения задач формирования инфраструктуры для оптимизации процессов разработки новых информационных систем и прототипирования, в том числе под задачи информационного центра компетенций «Металлургия».



Виктория Повелицина
директор по IT-инфраструктуре и связи «Норникеля»

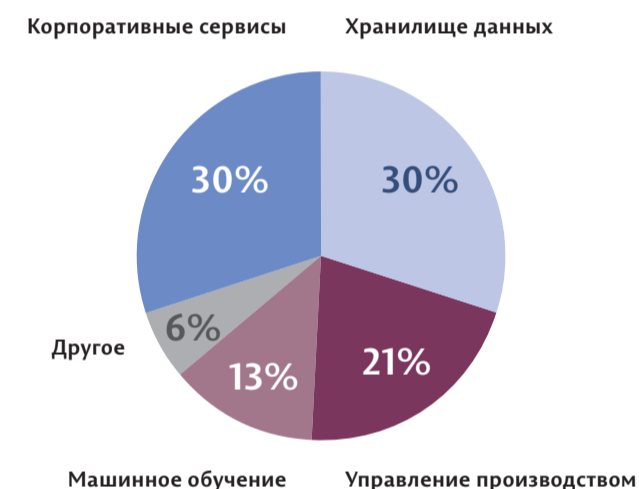
При большом объеме необходимых ресурсов нет существенной разницы, купить сервер или арендовать ресурсы в облаке. Если же нужно создавать нечто новое, проще приобрести облачные сервисы, говорит Приедитис. В случае с «Норникелем», продолжает он, их финансовые расчеты показали, что операционные затраты в сравнении с закупкой и использованием собственного «железа» одинаковы, но, используя облако, можно получить инструмент, который обеспечивает гибкость и скорость разработки.



Безопасность превыше всего

В 2023 г. глобальные потери от киберпреступности превысили \$8 трлн, подсчитала Statista. В России за 2023 г. было отражено свыше 65 000 кибератак на критическую информационную инфраструктуру, заявлял зампред правительства Дмитрий Чернышенко на форуме «Цифровая экономика».

Как промышленные компании используют облака



Источник: Yandex Cloud и «УльтимаТека», 2023

Повелицина отмечает, что для компании критерием выбора IT-инфраструктуры является мнение ее ИБ-отдела относительно рисков кибербезопасности. К ней традиционно высокие требования, поскольку именно на IT лежит ответственность за сохранность данных и сохранение непрерывности деятельности компании. С ней соглашается Лабудев из ООО «Алроса ИТ», утверждая, что сочетание частных и общедоступных облаков позволяет компаниям улучшить производительность, повысить безопасность данных и оптимизировать затраты на IT-инфраструктуру.

Промышленные компании в России пока экспериментируют с публичными облаками, говорит Приедитис. Это связано с тем, что на многих предприятиях просто не оценены риски безопасности и не построены модели угроз. Поэтому каждый проект по миграции в облако требует согласования с командами по ИБ. В этом плане наш рынок только формируется, отмечает он. При этом появляется все больше примеров, когда компании используют облачные платформы для более сложных задач – например, для обработки данных из системы управления производством, предсказательной аналитики, указывает эксперт. &



Рекламно-информационное приложение к газете «Ведомости»

16+

Главный редактор Роман Витальевич Кутузов
Генеральный директор Михаил Нелюбин
Директор по продажам Катерина Осипенко
Верстка Анна Ратафьева
Фоторедактор Наташа Шарапова
Корректор Светлана Борщевская
Менеджер по печати Татьяна Бурнашова
Шрифты: Илья Рудерман, «Студия Артемия Лебедева»; ParaType

Учредитель и издатель АО «Бизнес Ньюс Медиа»
Адрес учредителя, издателя и редакции:
127018 Москва, ул. Полковая, 3, стр. 1, пом. 1, этаж 2, ком. 21
Тел. 7 (495) 956-34-58
Рекламное СМИ

Свидетельство о регистрации:

ПИ № ФС 77-77720 от 17 января 2020 г., выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
Все права защищены ©2023, АО «Бизнес Ньюс Медиа»
Любое использование материалов издания, в том числе в электронном варианте, допускается только с согласия правообладателя

ОАО «Московская газетная типография»,
123995 Москва, ул. 1905 года, 7, стр. 1

Тираж 53 400
Цена свободная