SMART Закупка

14 апреля 2021

6 тенденций, определяющих машинное обучение в постпандемическую эпоху

Сегодня машинное обучение лежит в основе функционирования технологических компаний. Такие инструменты, как визуализация данных, интеллектуальные рабочие процессы и RPA (роботизированная автоматизация процессов), позволяют организациям подготовиться к эре гипер-автоматизации, позволяя различным бизнес-приложениям работать вместе для повышения эффективности.

Чтобы оценить, как развитие машинного обучения повлияет на будущее технологий и защитит критически важные данные и цифровые ресурсы от киберугроз, Toolbox поговорил с экспертами, чтобы понять, как революционные технологии могут изменить экономику в 2021 году и в последующий период.

Сосредоточьтесь на доверии и этике
Джетт Ористальо , Data Science and Product Lead of Trusted AI, DataRobot

Искусственный интеллект и машинное обучение - это мощные технологии, которые открыли безграничные возможности, но в 2021 году во всех отраслях будет вновь уделяться внимание вопросам доверия и этики ИИ. Благодаря печально известным ошибкам ИИ в частном и государственном секторах, таким как предвзятые модели, анализирующие резюме или прогнозирующие результаты обучения, в настоящее время этический ИИ подвергается массовому контролю со стороны общественности, и это справедливо.

«Предприятия, которые предпринимают шаги по внедрению снижения этических рисков на всех этапах разработки ИИ - от подготовки данных до разработки и производства моделей - могут гарантировать, что устранение дефектов и другие оценки моделей происходят на постоянной основе, обеспечивая истинное понимание и ответственное отношение к делу для заинтересованных сторон.

Расширение использования смоделированных данных для обучения алгоритмов машинного обучения
Николай Балдин , генеральный директор и основатель Synthesized

Ключевой тенденцией, определяющей машинное обучение и экосистему данных в 2021 году, станет самообслуживание, при котором предприятиям требуется более быстрый доступ к данным и возможность совместной работы с надежными партнерами. Это поможет им быстро производить продукты и услуги, чтобы эффективно конкурировать.

«Смоделированные данные выглядят, воспринимаются и ведут себя так же, как исходные данные, но личные атрибуты людей были удалены, поэтому они не подпадают под действие правил конфиденциальности. Таким образом, позволяя предприятиям свободно сотрудничать без риска. Смоделированные данные также могут устранять предвзятость, распознавая, когда определенные точки данных были чрезмерно или недостаточно представлены в исходном

наборе данных, и вносить исправления по мере необходимости, чтобы избежать проблем в дальнейшем.

Узнать больше: Создание заслуживающего доверия ИИ в 2021 году и в дальнейшем

Автоматизация задач и устранение сложности разрозненных данных
Арман Руис Габерне , директор по науке о данных и элитной группе искусственного интеллекта в IBM Cloud and Data Platform

Три ключевых тенденции машинного обучения, которые станут мейнстримом в 2021 году: талант, данные и доверие. Во-первых, организации решат проблему нехватки специалистов по обработке данных с помощью автоматизации, такой как новый AutoAI и возможности одной кнопки. Автоматизация низкоуровневых задач для специалистов по данным сокращает время окупаемости.

«Вторая большая тенденция будет заключаться в разрешении сложности разрозненных хранилищ данных, существующих в пространстве гибридного облака. Наконец, доверие станет центральным элементом, поскольку компании стремятся развернуть и масштабировать ИИ. Организации понимают, что они должны иметь возможность доверять своим моделям и своим бизнес-результатам на протяжении всего жизненного цикла ИИ. В 2021 году они продолжат обращаться к таким инструментам, как IBM Watson OpenScale и IBM Watson OpenPages, которые помогут повысить прозрачность, управлять рисками и укрепить доверие к ИИ.

Узнать больше: Adaptive Insights CPO о том, почему машинное обучение нарушает аналитику данных

Повышение роли ОД в банковских операциях
Бенуа Гранже , главный технологический евангелист OneSpan

Будущее банковского сектора заключается в использовании большего количества искусственного интеллекта, машинного обучения и биометрии и меньшего количества паролей. Банки объединят машинное обучение с биометрией, чтобы предоставить новые возможности, такие как проверка лица и отпечатков пальцев вместо паролей. Один из примеров, который мы уже наблюдаем, - это банки, использующие машинное обучение для обнаружения и чтения физических паспортов, что позволяет сканировать документы. Клиенты используют свои смартфоны для сканирования удостоверений личности государственного образца, а затем делают селфи. Затем банки используют биометрические технологии сравнения лиц с функцией определения живучести, чтобы убедиться, что удостоверение личности является подлинным и неизменным, подтверждая личность человека.

Марк Крайтон , старший директор по управлению продуктами безопасности, OneSpan

В настоящее время многие банки и финансовые учреждения имеют разрозненные пулы данных, которые невозможно извлечь, однако в следующем году редко можно будет увидеть, чтобы банки не использовали ИИ эффективно. Когда люди смогут читать и понимать сложные модели обнаружения мошенничества, мы твердо верим, что возможности ИИ проявятся во всей банковской отрасли.

Энди Реншоу , вице-президент по платежным решениям и стратегии в Feedzai

Искусственный интеллект и машинное обучение станут еще более полезными для банков, которым придется выполнять свои требования по борьбе с отмыванием денег в соответствии с такими нормативными актами, как Шестая директива ЕС о борьбе с отмыванием денег (AML6).

Автоматизируя задачи, которые традиционно основывались на ручной работе, такие как проверка знаний своего клиента (KYC), банки и финансовые учреждения смогут повысить точность и снизить уровень ложных срабатываний.

Но будущее решений AI и ML - это прозрачность и мониторинг потенциальной предвзятости - проблема, которую организации больше не могут позволить себе игнорировать. Goldman Sachs, например, стал объектом расследования в 2019 году, когда потребители пожаловались на то, что его карты Apple Cards предлагали кандидатам-женщинам более низкие кредитные линии по сравнению с клиентами-мужчинами. Тем, кто применяет инструменты машинного обучения в рамках своей деятельности, необходимо будет предпринять шаги для обеспечения соответствия технологии строгим этическим стандартам.

Повышенное внимание к безопасности технологий искусственного интеллекта / машинного обучения
Ник Маккуайр , старший вице-президент Enterprise Research CCS Insight

Хотя сегодня большая часть внимания уделяется применению технологий искусственного интеллекта для обеспечения кибербезопасности, компании вскоре приложат больше усилий для защиты своих моделей машинного обучения и обеспечения надежности своих алгоритмов. К 2024 году 50% крупных организаций развернут технологии повышения конфиденциальности для поддержки своих приложений машинного обучения. Ценность данных о клиентах для понимания и персонализации растет, но вместе с тем растут и проблемы с конфиденциальностью, особенно в связи с усилением регулирования во всем мире.

Напряженность между этими областями сохранится в течение следующего десятилетия, особенно в области развития больших данных и искусственного интеллекта. Доверие и уважение к конфиденциальности клиентов имеют важное значение для долгосрочного успеха, поэтому компании должны вкладывать средства в такие технологии, как анонимизация данных, дифференциальная конфиденциальность, синтетические наборы данных и гомоморфное шифрование для своих проектов машинного обучения.

Узнать больше: Как преодолеть разрыв в навыках, возникший из-за автоматизации

Роль машинного обучения в автоматизации задач кибербезопасности
Саманта Хамфрис , старший специалист по безопасности в Exabeam

Машинное обучение и автоматизация могут освободить аналитиков по кибербезопасности для работы над более важными / стратегическими задачами, выполняя трудоемкие задачи, такие как приоритезация предупреждений безопасности, сокращение количества ложных срабатываний и сопоставление устройств с IP-адресами. Они также могут повысить способность группы безопасности быстро обнаруживать поведение злоумышленников, которое в противном случае потребовало бы значительного количества времени для расследования вручную. ML также может создавать профили сотрудников, включая их группы коллег и личные адреса электронной почты, что позволяет аналитикам выявлять внутренние угрозы гораздо быстрее, чем это было возможно раньше.

Отнюдь не сокращая ненужные должности младших сотрудников, ML позволит командам нанять больше сотрудников и поможет им начать работу, предоставив в их распоряжение мощные инструменты и решения безопасности. В 2021 году и в последующий период распространение этих технологий, вероятно, будет способствовать будущему развитию в этом секторе, при этом новые / различные наборы навыков станут более востребованными потенциальными работодателями.

Ссылка на статью: 6 тенденций, определяющих машинное обучение в постпандемическую эпоху