№ 7 (107) | 16.10.2024
Рекламное СМИ

ВЕДОМОСТИ

партнеры материалов:
ВТБ, ДОМ.РФ, MTC RED

Новые финансовые технологии: искусственный интеллект

Читайте материалы выпуска
на сайте vedomosti.ru

16+

Умные деньги

Как искусственный интеллект меняет рынок финансовых услуг

Инна Каминская

В 2022 г. генеративный искусственный интеллект (ИИ) совершил скачок в развитии – вышла модель ChatGPT-3.5, получившая огромное общественное внимание: удобный сервис с низкой стоимостью расширил спектр задач, к которым можно применять ИИ без специального обучения. А уже в марте 2023 г. появилась новая модель – ChatGPT-4, которая была на два порядка больше своей предшественницы и содержала около 100 трлн параметров. Однако финансовые организации, как обладатели большого количества важных данных, начали эксперименты с ИИ на основе машинного обучения еще в 1980-х гг., а в 2010-х уже широко внедряли соответствующие инструменты. Появление новых генеративных ИИ только придало этому тренду дополнительный импульс. «Ведомости&» попросили экспертов и участников рынка рассказать о современных способах использования всех видов ИИ в финансах, а также поделиться прогнозами развития отрасли и сложностями, с которыми сталкивается технология.

Персональный помощник с интеллектом

Один из трендов в развитии ИИ для финансового сектора – это гиперперсонализация и человекоцентричность, когда продукт максимально адаптируется под потребности конкретного человека, считает генеральный директор Ассоциации «ФинТех» Максим Григорьев. Например, ИИ или рекомендательные системы подсказывают агенту дополнительные продукты, которые были бы интересны клиенту, поясняет директор департамента машинного обучения и работы с данными «Альфастрахования» Александр Логачев. Они учитывают как особенности клиента (его демографические данные, предпочтения и историю взаимодействия с компанией), так и специфику продаж агента.

Тенденция персонализации будет только усиливаться. «Генеративный ИИ может глубже погрузиться в контекст клиента и разговаривать с ним на его языке, делая каждую коммуникацию с клиентом уникальной и созданной исключительно для него», – рассказывает лидер направления «Данные» в банке «Точка» Галина Вакулина.

Технологии речевой аналитики позволяют лучше понимать потребности и эмоциональное состояние клиентов. Они анализируют их взаимодействие в контактных центрах и чатах, что позволяет более точно настраивать продуктовые предложения и клиентское обслуживание, добавляет Марина Лященко из Страхового дома ВСК.

В банке ВТБ наибольшие перспективы видят в объединении данных – концепции Data Fusion. Чем больше тот или иной бизнес знает о своем клиенте, тем более качественную услугу он может ему оказать, причем эта услуга будет оказана в наиболее оптимальное время, и финансовый сектор здесь не исключение, отмечает представитель банка.

Автоматический риск-менеджер

С помощью методов ИИ можно проанализировать кредитные данные о конкретном клиенте банка, например историю платежей, общую кредитную нагрузку, уровень дохода и т. д., объясняет Александр Попов, заведующий лабораторией нейронных систем и глубокого обучения МФТИ. Кроме того, ИИ принимает во внимание дополнительные факторы, влияющие на кредитоспособность, вплоть до данных Росстата о социальных условиях в конкретном регионе.

Росбанк уже активно внедряет технологии ИИ для оценки кредитоспособности клиентов, что позволяет расширить доступ к кредитам и улучшить точность анализа рисков, рассказывает директор департамента централизованного управления данными Росбанка Максим Травин.

Генеративный ИИ позволяет создавать более точные модели анализа рисков путем обработки больших объемов данных и выявления скрытых закономерностей. «Это способствует более обоснованным и оперативным решениям, что особенно важно в условиях высокой волатильности рынка. Такие технологии позволяют банкам более эффективно управлять кредитными рисками и улучшать прогнозирование дефолтов», – отметили в Россельхозбанке.

Дмитрий Удод, директор Центра развития искусственного интеллекта компании «Ингосстрах», указывает, что для задач анализа страховых рисков и принятия решений используются методы машинного обучения. В Центре развития ИИ «Ингосстраха» также разрабатываются генеративные модели для антифрода (борьбы с мошенничеством. – «Ведомости&»). «Суть данных моделей – попытаться методами распознавания текста и изображений определить, является клиент мошенником или нет. Например, при обращении клиента к нам с подозрительными параметрами нейронная сеть способна по определенным свойствам выявить этот факт и предварительно сообщить, является ли данный клиент подозрительным», – говорит Удод. Другой пример – оценка ущерба по фотографиям с места ДТП. «Генеративный ИИ при должном уровне его обучения способен распознать тяжесть происшествия», – поясняет Удод.

ИИ может использоваться для обнаружения аномалий в транзакциях, которые могут свидетельствовать о мошеннических действиях, а также для анализа паттернов поведения клиентов для выявления подозрительных операций. Реализация работы антифрод-систем в реальном времени позволяет предотвратить мошенничество до его завершения, рассказывает Травин.

ИИ может существенно помочь в оценке фактов социальной инженерии и противодействии фроду, согласен старший вице-президент по IT банка «Санкт-Петербург» Александр Рыбаков.

Лекарство от рутины

Финтех, как правило, связан с огромным количеством данных, на анализ которых у человека может уйти несколько дней или даже недель, в то время как ИИ справится с задачей за пару минут, объясняет руководитель проектов «Платформы Сфера» Вячеслав Борисов. С помощью технологии можно не только просуммировать данные, но и дополнить исследование собственными выводами: подвести краткие итоги, выделить тренды, добавляет он.

«Наиболее перспективным видится применение ИИ на участках работы, связанных с постоянно повторяющимися действиями», – соглашается Лященко. Это может быть любая ниша, которая требует обработки данных и документов в отраслях и бизнес-процессах.

Алексей Каширин, директор Центра продвинутой аналитики Альфа-банка, указывает, что автоматизация рутинных задач с помощью ИИ освобождает сотрудников «для выполнения более сложных и креативных задач».

Личный финансовый советник

Одним из основных направлений развития ИИ в ВТБ видят создание финансовых советников, основанных на технологиях ИИ. Они могут анализировать огромные массивы данных и предлагать пользователю оптимальные решения не только исходя из рыночной ситуации, но и с учетом анализа его возможностей и потребностей, отметил представитель банка.

«ИИ может использоваться для создания чатботов и виртуальных помощников, которые способны общаться с клиентами на естественном языке и предоставлять персонализированные ответы на их запросы. Такие системы могут учитывать историю взаимодействий клиента, его предпочтения и текущие финансовые потребности», – полагает Дмитрий Демидов, руководитель Лаборатории инноваций НОРБИТ (входит в группу «Ланит»).

На основе анализа регулярных расходов ИИ способен предложить клиенту варианты оптимизации бюджета или помочь в планировании крупной покупки. Если клиент часто делает импульсивные покупки, ИИ предложит стратегии для контроля расходов, приводит примеры Попов из МФТИ.

Синергия с различными базами, возможность аналитики чеков позволит давать рекомендации в том числе по покупкам тех или иных товаров с учетом определенной экономии. Либо позволит оценить, как изменение привычек покупать те или иные товары отражается на бюджете, согласен Михаил Комаров, профессор Высшей школы бизнеса НИУ ВШЭ.

Взгляд в будущее

«В будущем очень серьезный прорыв произойдет в направлении взаимодействия агентов ИИ между собой, это тесно связано с трендом «машина как клиент», – уверен Григорьев из Ассоциации «ФинТех». Прогнозируется, что агентам на основе ИИ человек будет делегировать часть задач и проблем. Взаимодействуя с такими же умными программами со стороны бизнеса, ИИ-агенты будут помогать человеку удобным и безопасным способом получать максимально адаптированные под его потребности сервисы.

«ИИ-инструменты будут становиться автономнее благодаря развитию методов и алгоритмов, позволяющих ИИ обучаться и адаптироваться к

изменениям без вмешательства человека. Также будут разрабатываться алгоритмы, повышающие безопасность, конфиденциальность, надежность и этичность инструментов на базе ИИ», – прогнозирует Илья Левчук, директор департамента индустриальных ПАКов компании Fplus.

«От поиска релевантных сервисов и продуктов из числа уже существующих мы сможем перейти к созданию новых, уникальных предложений для каждого клиента «на лету», подобно тому как в дополнение к поиску информации, уже присутствующей в интернете, генеративный ИИ может помочь в синтезе нового контента, оптимизированного под запрос конкретного пользователя», – прогнозирует Попов.

По мере накопления данных о клиентах финансовые организации смогут создавать их точные цифровые модели и профили – цифровых двойников. Демидов из НОРБИТ уверен, что цифровые двойники позволят моделировать реакцию клиентов на новые продукты и услуги. «Возможность создания на основе больших объемов данных цифровых моделей клиентов (DToC, digital twin of customer) позволит не только симулировать поведение клиента в типичных сценариях, но и прогнозировать различные варианты его поведения в зависимости от состава пакета услуг и их стоимости», – поясняет он.

Банки все чаще будут выделять работу с ИИ в отдельные центры компетенций и центры экспертизы ИИ. «McKinsey в своем докладе «Будущее ИИ в банковской сфере» отмечает тренд на централизацию функций, связанных с экспертизой в ИИ и разработкой ИИ-решений, в рамках единого подразделения, так как подобная организационная структура позволяет финансовым организациям быстрее реализовывать и внедрять ИИ-сценарии», – отмечает старший преподаватель Центра прикладного искусственного интеллекта «Сколтеха» Алексей Зайцев.

Необходимо создавать специализированную инфраструктуру по разработке решений ИИ, считает директор дивизиона искусственного интеллекта Yadro Кирилл Корняков. «Подобно тому как практически все финансовые организации ранее создали собственные подразделения по разработке ПО, теперь стоит задача создания аналогичных подразделений, но уже в отношении ИИ. Это то, что называется MLOps – Machine Learning Operations, программно-аппаратные инфраструктуры, позволяющие построить полный цикл создания ИИ-решений, от сбора и разметки данных до развертывания и мониторинга исполняемых моделей ИИ», – поясняет он.

Проблемы и решения

Использование ИИ в финансовом секторе порождает ряд этических проблем, например вопросы конфиденциальности данных, прозрачности алгоритмов и недопущения дискриминации. «Решение этих вопросов требует разработки строгих стандартов и нормативных актов, а также использования технологий объяснимого, или интерпретируемого, ИИ (Explainable AI), которые позволяют понять логику принятия решений алгоритмами», – считают в Россельхозбанке.

«ИИ дает ответ, но почему именно такой, не объясняет. Устранить проблему можно с помощью добавления в ответ факторов, повлиявших на принятое решение», – соглашается директор по развитию бизнеса компании «Ланит – Би Пи Эм» Максим Волошинов.

Еще одна сложность использования ИИ – в проблеме ответственности. «Условный «последний человек, который нажал на кнопку» в процессе принятия решений с использованием систем ИИ, должен нести ответственность даже в том случае, если собственно катастрофическое решение было принято ИИ», – считает Андрей Кулешов, эксперт Центра прикладных систем ИИ МФТИ. «Конечно, должны возникнуть соответствующие законодательные нормы, практика применения, цифровые компетенции и т. д. Но без разумного и адекватного контроля со стороны носителей естественного интеллекта не обойтись», – подытоживает Каширин.

Наконец, генеративный ИИ иногда способен выдавать правдоподобные, но фактически ошибочные ответы, что тоже может создавать риски в финансовой сфере. Поэтому, по мнению Вакулиной из «Точки», «при внедрении ИИ-моделей необходимы решения для проверки качества информации и фактчекинга».

Риски кибербезопасности и утечки данных – еще одна проблема. «В банковской сфере более широкое развитие ИИ осложняется высокими требованиями по информационной безопасности, которые финансовые организации обязаны соблюдать по закону. Например, некоторые данные, которые необходимы для обучения моделей ИИ, относятся к категории банковской тайны», – говорит управляющий директор Дом.РФ Николай Козак.

Необходимо использовать шифрование данных, применяемых ИИ-системами, а также проводить регулярный аудит безопасности и конфиденциальности, включая тестирование на уязвимости, дополняет Травин из Росбанка. Использование методов анонимизации данных позволит минимизировать риск утечки персональных данных, отмечает эксперт.

Безопасное и эффективное использование ИИ в финансовом секторе требует ряда регуляторных изменений, считают эксперты. Ляшенко отмечает необходимость «разработки и внедрения правил использования ИИ, включая стандарты этики, требования к защите данных, а также механизмы прозрачности и объяснимости решений, принимаемых ИИ».

Однако тут возникает опасность противоположной проблемы – излишнего регулирования. «Для развития использования ИИ в финансах нужно обеспечить свободу использования данных и прозрачность того, как такие данные используются и на их основе принимаются решения. Ограничение свободы тут ведет к технологическому отставанию», – уверен Зайцев из «Сколтеха».

Среди препятствий для более широкого внедрения ИИ в финансах эксперты также называют недостаток компетентных специалистов и ограниченные вычислительные мощности. «Последнее легко решается деньгами. А вот создание команды специалистов требует очень много времени», – говорит Демидов из НОРБИТ.

«Одно из главных препятствий – стоимость собственных разработок. Для создания большой языковой модели, адаптированной под задачи конкретной компании, требуется объемная и сложная инфраструктура данных. Это влечет существенные затраты на аппаратную часть и специалистов, которые в основном могут позволить себе только большие корпорации, лидеры рынка», – дополняет Левчук.

«Россия с точки зрения развития IT – одна из передовых мировых держав. Чтобы ускорить темпы цифровизации как в финансовой сфере, так и в других, нужно больше квалифицированных кадров и вычислительных мощностей, особенно специализированных на ИИ, таких как GPU (графические видеоускорители, применяемые также для обучения моделей ИИ. – «Ведомости&»)», – подытожили в Россельхозбанке. &

10 трендов ИИ-2024

В 2024 г. искусственный интеллект (ИИ) продолжает стремительно развиваться и проникать во все сферы жизни.

Демократизация генеративного ИИ.
Он становится доступнее для широкого круга пользователей благодаря развитию Low-code и No-code сервисов (почти не требующих или совсем не требующих навыков программирования для создания нового продукта. – «Ведомости&»), облачных вычислений и открытых решений.

Появление новых бизнес-моделей и сервисов.
Компании используют ИИ для глубокой трансформации и запуска инновационных продуктов.

Развитие мультимодального ИИ.
Мультимодальный ИИ работает с разными типами данных: текст, изображения, видео, речь и др. Например, «Сбер» представил мультимодальную модель GigaChat, поддерживающую диалог с пользователем и генерацию текстов и изображений.

Применение ИИ в биометрии.
В Московском метрополитене уже более 90 млн раз была использована оплата проезда с помощью биометрии.

Развитие мультиагентных систем.
В них несколько моделей ИИ взаимодействуют для решения сложных задач.

Разработка программного обеспечения при помощи ИИ.
ИИ ускоряет и улучшает процесс создания приложений. ИИ-ассистент GigaCode от «Сбера» может генерировать код в реальном времени, поддерживая более 15 языков программирования.

Безопасность на всех этапах жизненного цикла.
Разработка ИИ требует тщательного подхода к безопасности как используемых для обучения данных, так и самих систем ИИ.

Этичное и ответственное применение ИИ.
В России подписана Декларация об ответственной разработке и использовании сервисов на основе генеративного ИИ.

Обеспечение технологического суверенитета.
Страны стремятся создавать собственные прорывные ИИ-решения. «Яндекс» представил линейку моделей YandexGPT 3, превосходящую ChatGPT-3.5 в ответах на узкие классы запросов.

Государственное стимулирование развития рынка ИИ.
В России утверждена Национальная стратегия развития ИИ до 2030 г. с потенциальным эффектом для экономики в 11,2 трлн руб.

Источник: Ассоциация «ФинТех»

«Искусственный интеллект может вывести предотвращение кибератак на новый уровень»

Ильназ Гатауллин, технический руководитель MTC RED SOC, о защите от кибератак

Число кибератак растет во всем мире. Однако для России эта проблема особенно актуальна – в прошлом году страна вошла в пятерку самых атакуемых. Какими последствиями для бизнеса могут обернуться киберугрозы, как центры мониторинга помогают с ними бороться и на чьей стороне сейчас искусственный интеллект, рассказал Ильназ Гатауллин, технический руководитель центра мониторинга и реагирования на кибератаки MTC RED SOC компании MTC RED («Серенити Сайбер Секьюрити»).

– Когда говорят, что кибератаки в основном приходятся на объекты критической информационной инфраструктуры (КИИ), то о каких отраслях идет речь в первую очередь?

– По нашим данным, в первом полугодии этого года на КИИ пришлось 69% от общего числа высококритичных атак. Самые атакуемые отрасли КИИ сейчас – это промышленность, связь и здравоохранение. И если в медицинских учреждениях предметом интереса злоумышленников чаще всего являются персональные данные клиентов и сотрудников, то в случае с финансовым сектором к этим рискам можно добавить прямое хищение денег клиентов.

Финансовые организации стали подвергаться атакам одними из первых, и сейчас в вопросах кибербезопасности это одна из самых зрелых отраслей. В то же время возможность быстрой монетизации атаки на банк продолжает привлекать высококвалифицированных злоумышленников.

– То есть банки – более сложная цель?

– Да, однако и атакуют их самые профессиональные хакеры. Особенность атак на банки – глубокая кастомизация инструментария злоумышленников под конкретную организацию, ее средства защиты, бизнес-процессы, конкретных сотрудников. Хакеры постоянно совершенствуют методы атак на банки, поэтому и банкам надо так же системно заниматься повышением защищенности.

Кроме того, финансовый сектор подвержен рискам атак через подрядчика. В этом случае злоумышленники взламывают инфраструктуру не самого банка, а менее защищенной организации, которая имеет доступ к банковским информационным ресурсам. Это узкое место, потому что свою инфраструктуру компании защищают по максимуму, а уровень кибербезопасности подрядчиков, как правило, никак не регламентируется и не контролируется. Если хакер получает доступ к инфраструктуре банка через его подрядчика, он может пройти «ниже радаров» стандартных средств защиты. Мы выявляли и отражали такие атаки, и здесь лучшим инструментом остается тщательный контроль действий подрядчиков в IT-инфраструктуре компании. По-другому пока никак.

– А что кроме утечки персональных или производственных данных еще может произойти в результате атаки?

– Например, шифрование или полное удаление всех данных организации. Другой вариант атаки – дефейс веб-сайта (deface – «уродовать«, «искажать«. – «Ведомости&»), когда вместо обычного контента на странице может появиться какой-то лозунг и т. п. Такой инцидент не влияет на безопасность персональных или финансовых данных клиентов, однако несет высокие репутационные риски. А в перспективе любой инцидент, даже относительно несерьезный (такой, как дефейс), может привести к заметному оттоку клиентов.

Ну и, конечно, существует очень много разных вариантов атак, направленных непосредственно на хищение денег. Например, злоумышленники проникают в процессинговый сегмент и подменяют адреса реквизитов, находят уязвимости в личных кабинетах интернет-банка и многое другое.

Чтобы атаки не заходили так далеко, как раз и нужны центры непрерывного мониторинга и реагирования на инциденты (Security Operations Center, SOC). Они позволяют своевременно выявить атаку, свести к минимуму ущерб и сделать так, чтобы подобное не повторилось.

– Как работают центры мониторинга? Что они делают и для чего нужны?

– Ключевые задачи центра мониторинга – это круглосуточное отслеживание событий, происходящих в инфраструктуре заказчика, выявление кибератак и блокирование действий хакеров. Информацию о происходящем в IT-контуре заказчика мы собираем со всех установленных у него средств защиты вне зависимости от вендора.

SOC состоят из нескольких команд специалистов. Первая линия – это аналитики, которые получают информацию о подозрительных событиях в IT-инфраструктуре и проводят первичную обработку по предварительно подготовленным инструкциям.

Если ситуация нетривиальная, она передается аналитикам второй линии, обладающим более высокими компетенциями. Они проводят детальный анализ происходящего и определяют меры, необходимые для реагирования на инцидент. Мы, как коммерческий сервис, можем сами заблокировать развитие атаки в инфраструктуре заказчика или передать ему полный перечень необходимых действий, если компания предпочитает реализовывать процесс реагирования на своей стороне. Но так или иначе после блокирования атаки мы обязательно выдаем рекомендации в отношении того, как ликвидировать или минимизировать последствия, а главное – предотвратить повторение инцидента. То есть каждая попытка атаки становится для заказчика возможностью повысить общий уровень защищенности компании.

IStock

Есть еще аналитики третьей линии, которые занимаются реверс-инжинирингом и разработкой корреляционных правил для выявления новых атак. Реверс-инженеры «разбирают» вредоносное ПО и анализируют, как оно устроено, чтобы создать эффективную защиту от него.

– А что происходит после реверс-инжиниринга?

– Вся информация об инциденте аккумулируется в SIEM-системе, на ее основе мы создаем сценарии выявления кибератак, которые потом используем для защиты других компаний от аналогичных угроз. При этом мы используем не только собственные, но и сторонние данные. В базе MTC RED SOC уже более 500 сценариев выявления кибератак, и она постоянно пополняется. Эти сценарии включают информацию в том числе о тех угрозах, которые появились совсем недавно, и о тех, которые применяются в конкретной отрасли, что очень важно для тех же банков.

Система управления информационной безопасностью и событиями безопасности (SIEM)

класс программных продуктов для сбора и анализа информации о событиях безопасности. Система обрабатывает данные из различных источников, приводит их к единому формату (нормализует), а затем проводит логические операции, выявляет корреляцию и распознает шаблоны атак.

– Любая организация может создать собственный центр мониторинга?

– Да, но это требует больших вложений в инфраструктуру, команду, выстраивание процессов и занимает много времени. Поэтому сейчас очень широко распространен аутсорсинг центров мониторинга. У провайдера уже все это есть: и инфраструктура, и команда, и экспертиза – та же база корреляционных правил, т. е. заказчик сразу получает работающую функцию под ключ. Причем ее можно подключить не только заблаговременно, но и в момент, когда банк уже находится под атакой.

Другой распространенный вариант – гибридные SOC, когда техническая часть, т. е. SIEM-система, размещается в инфраструктуре заказчика, а на аутсорсинг отдаются именно сопровождение, развитие и поддержка, первая и вторая линии аналитиков, т. е. человеческие ресурсы. В текущей ситуации дефицита кадров на рынке кибербезопасности это снимает с заказчиков проблему подбора штата в центр мониторинга. Кроме того, при использовании гибридной модели информация об инцидентах не покидает контура компании, что для некоторых заказчиков является важным условием.

– Сейчас очень популярна тема искусственного интеллекта (ИИ). Говорят, что хакеры уже активно им пользуются. Будет ли ИИ помощником для защитников? В этом направлении ведутся разработки?

–ИИ может взять на себя те процессы, которые легко автоматизировать, или те, где требуется обработка большого объема данных для поиска неочевидных для человека паттернов. В целом деятельность SOC всегда требовала автоматизации. У нас большое число заказчиков из самых разных отраслей – от банков и промышленности до СМИ. Это крупные организации с масштабными и часто территориально распределенными IT-инфраструктурами, и SOC должен обрабатывать все происходящие в них события. Очевидно, что без автоматизации это невозможно, и здесь эту задачу решает SIEM-система. Однако, для того чтобы сделать следующий большой шаг на пути к более быстрому и качественному выявлению и отражению атак, необходимо применять новые технологии. Поэтому мы ведем исследования в направлении ИИ.

В частности, на объеме тех данных, которыми располагает SOC, можно обучить ИИ выявлять и отсеивать так называемые ложноположительные срабатывания – когда легитимные действия пользователей ошибочно принимаются за кибератаку. ИИ может автоматизировать этот процесс и под контролем человека свести число ложноположительных срабатываний к минимуму. Это снизит нагрузку на специалистов и уменьшит риски того, что у них замылится глаз и они пропустят реальную атаку.

В части формирования отчетов об инцидентах и рекомендаций по реагированию на развивающуюся атаку ИИ может использоваться в двух плоскостях. Во-первых, для автоматизации составления базовых отчетов и рекомендаций по противодействию типовым инцидентам. Это даст нам преимущества в скорости реагирования, а она может быть очень важна и в самых простых с точки зрения аналитика случаях – например, при атаке вирусом-шифровальщиком. Во-вторых, там, где для анализа инцидента требуется дополнительная информация, ИИ может помочь с ее сбором и систематизацией. Это позволяет аналитику не тратить время на рутинные действия и сосредоточиться на наиболее интеллектуально трудоемкой работе, а заказчик в результате получает более полный и детализированный отчет об атаке в максимально короткие сроки.

Третий аспект деятельности нашего центра мониторинга, где есть потенциал для автоматизации с применением ИИ, – это выявление аномалий и поиск признаков атак, которые остались незаметными для технических средств защиты от киберугроз (Threat Hunting).

Говоря об ИИ, можно провести аналогию с беспилотным транспортом. В мае в Москве появился первый такой трамвай, по городу он пока ездит под контролем человека, но в депо – сам. Почему для эксперимента выбрали именно трамвай? Потому что он ходит по рельсам, это очень алгоритмизированный маршрут. Это не автобус или электробус, водители которых должны ориентироваться в дорожной ситуации с множеством других участников. Вот так сейчас может работать ИИ – по рельсам, по четкому стандартному маршруту. А центр мониторинга и реагирования на кибератаки как раз решает очень нестандартные задачи, поэтому до замещения человека ИИ еще далеко. Но мы уверены, что ИИ может стать хорошим помощником специалиста по кибербезопасности и в конечном счете поможет добиться еще более высоких показателей качества сервисов SOC.

– А в стандартных ситуациях, на рельсах, так скажем, кто чаще будет ошибаться – человек или ИИ?

– ИИ тоже может ошибаться. Он же обучается на данных, и если в них были неточности или сами данные были неверными, то ИИ будет допускать ошибки и принимать неверные решения. Поэтому мы, например, очень внимательно следим за качеством собираемых данных, чтобы, когда они лягут в основу обучения ИИ, избежать таких проблем.

– Похоже, мы видим извечное соревнование снаряда и брони, только на новом витке. Теперь инструмент – ИИ. Как вы считаете, кто сейчас побеждает в этой борьбе – хакеры или киберзащитники?

– Не вижу пока явного преимущества ни у одной из сторон. Так что битва продолжится, и победит, на мой взгляд, тот, кто научится лучше работать с ИИ. &

Ильназ Гатауллин
технический руководитель
MTC RED SOC

Окончил МЦК-КТИТС по специальности «информационные технологии» и Казанский национальный исследовательский технологический университет по специальности «информационная безопасность». Начал карьеру в сфере кибербезопасности в 2016 г. До MTC RED работал в компаниях «Таттелеком», «РТ-информ» и «Информзащита», где прошел путь от аналитика по кибербезопасности до заместителя директора SOC. В MTC RED Ильназ Гатауллин руководит технологическим развитием и совершенствованием сервисов центра мониторинга и реагирования на кибератаки MTC RED SOC.

MTC RED

Предоставляет российским компаниям экосистему технологий кибербезопасности. Под защитой MTC RED находятся крупнейшие организации России в сфере финансов, IT, промышленности, телекоммуникаций, ритейла и здравоохранения. Портфель MTC RED включает сервисы центра мониторинга и реагирования на кибератаки MTC RED SOC, сервисы по защите от DDoS-атак (Anti-DDoS) и атак на веб-приложения (WAF), сервисы шифрования каналов связи (ГОСТ VPN), многофакторной аутентификации (MFA) и повышения киберграмотности пользователей (Security Awareness). MTC RED также ведет разработку собственных решений в области сетевой безопасности.

В гонке за самым умным

Как российский и мировой финтех развивает цифровых ассистентов: за какими технологиями будущее банков

Егор Сонин

Развитие все более совершенных цифровых ассистентов – один из основных трендов отечественного и мирового финтеха. Учитывая возможности технологий искусственного интеллекта (ИИ), обслуживание клиентов при помощи цифровых ассистентов может не просто не уступать привычному обслуживанию в отделениях, но и по некоторым показателям даже превосходить его. Подобные разработки повышают удовлетворенность клиентов от использования банковских сервисов, позволяют банку оптимизировать внутренние процессы, что в конечном счете обусловливает и рост доходов банка.

Бизнес стремительно умнеет

По прогнозам Goldman Sachs, к концу 2025 г. глобальные инвестиции в направление генеративного ИИ достигнут $200 млрд. При этом массовое использование этих технологий сможет повышать производительность труда в мире на 1 п. п. ежегодно, уверены аналитики.

ИИ помогает банкам

ИИ привлекает финансовые организации повышением продуктивности. Например, JPMorgan Chase разрабатывает программный сервис IndexGPT. Решение, подобное ChatGPT, с помощью ИИ будет помогать клиентам анализировать и выбирать ценные бумаги для инвестиций с учетом их потребностей.
Сингапурский DBS банк до конца 2024 г. оснастит 500 сотрудников службы поддержки клиентов (CSO) виртуальным помощником на базе ИИ. CSO Assistant расшифровывает запросы клиентов в режиме реального времени, выполняет поиск в базе знаний банка, а также помогает с документацией после звонка, предоставляя мгновенные сводки звонков и предварительно заполняя поля запросов на обслужиание.
Шведский банк RBC разработал проект RBC Wealth Management и платформы управления активами на базе ИИ TIFIN AG. Система анализирует финансовое состояние клиента: есть ли у него активные денежные операции, специфику его финансового поведения и нестандартные финансовые события, например получение наследства.

Источники: CNBC, DBS, American Banker

Одна из опций оптимизации рутины – цифровые помощники. В 2023 г. объем мирового рынка цифровых советников оценивался в $6,61 млрд, подсчитали в Grand View Research. Согласно прогнозам аналитиков до 2030 г., он будет расти в среднем на 30,5% в год и может достичь $42,6 млрд.

Лидирующие позиции на рынке цифровых помощников в 2023 г. занимала Северная Америка, на нее приходилось более 37% рынка, по данным Polaris Market Research. Успех связан с развитой финансовой экосистемой региона, строгими нормативными стандартами и культурой инноваций, которые способствовали широкому внедрению цифровых консультативных услуг. Тем не менее, по прогнозам KBV Research, Азиатско-Тихоокеанский регион в ближайшие пять лет может стать самым быстрорастущим рынком цифровых помощников.

В России в 2023 г. генеративный ИИ для решения различных бизнес-задач использовало около 20% компаний, говорится в исследовании «Яков и партнеры» и «Яндекса». Практически все опрошенные компании (94%) отметили сокращение затрат в качестве ключевого эффекта от внедрения ИИ в бизнес-процессы. Около трети компаний, работающих в потребительском секторе, также ожидают, что ИИ способен поднять выручку, увеличить ценность продуктов для клиентов и, как следствие, лояльность последних.

Спектр применения цифровых помощников в России уже весьма широк. К примеру, на «Госуслугах» в тестовом режиме работает робот Макс. Росреестр развивает цифрового помощника Еву. Своих цифровых помощников развивают мобильные операторы, крупные банки и другие компании.

Аналогичные разработки внедряет в свои сервисы и ЦБ: еще в 2022 г. Банк России объявил о запуске «ЦБ-онлайн» – специального навыка голосового помощника Алиса, разработанного совместно с «Яндексом». С его помощью можно сделать перевод через Систему быстрых платежей, решить проблему с погашением кредита и даже пожаловаться в ЦБ.

Создание и развитие полноценных цифровых ассистентов останется одним из ключевых трендов в финтехе в ближайшие несколько лет, считает заместитель президента – председателя правления ВТБ Вадим Кулик.

Личный советник по финансам

По данным McKinsey, генеративный ИИ может потенциально принести банкам $200–340 млрд. Это эквивалентно 9–15% глобальной операционной прибыли сектора.

Развитие технологий цифровых советников станет важным шагом для всего рынка финансовых услуг и будет способствовать созданию новых инновационных решений, уверен Кулик. С развитием советников пользователи смогут получать более точные и выгодные предложения, а компании – улучшать свои процессы и усиливать взаимодействие с клиентами.

Поэтому одно из направлений развития в ВТБ – разработка продвинутых роботов-советников, которые будут активно помогать клиентам оперировать их личными финансами, формировать инвестиционные стратегии и др. В июле 2024 г. ВТБ объявил о создании программы по развитию технологий ИИ «Цифровой помощник». Она объединила в себе все наработки банка по развитию направления цифровых ассистентов. По словам Кулика, сейчас в рамках этой программы банк работает уже по целому пулу кейсов применения цифровых ассистентов.

Одно из этих направлений представляет собой применение технологий ИИ для анализа данных, которыми располагает банк о своем клиенте, его окружении, связях. Основываясь на результатах этого анализа, банк может предлагать более релевантные предложения конкретному клиенту, поясняет Кулик.

Второе направление – саммаризатор внутренних коммуникаций. «В какой-то степени это цифровой ассистент руководителя – он позволяет анализировать содержание рабочих совещаний, составлять конспекты с формированием актуальных задач, используя системы транскрибации и саммаризации текста», – рассказывает Кулик. В расшифровке

Почти как люди

Первые чат-боты появились еще в 60-х гг. XX в. В них не было ИИ, они просто распознавали ключевые слова в запросе пользователя и выдавали заранее запрограммированные ответы. Такие решения работают и сейчас, они могут, как правило, давать ответы на типовые запросы, но сложные задачи они решать не умеют.
В дальнейшем с развитием технологий синтеза и распознавания речи появились и голосовые ассистенты. По сути, это были продвинутые чат-боты, способные понимать заданный вслух вопрос и отвечать на него синтезированным человеческим голосом.
Скачок в развитии цифровых помощников произошел в 2022 г. с появлением чат-бота ChatGPT от компании OpenAI, основанного на работе генеративного ИИ. Это дало возможность на огромных массивах данных обучить глубокую нейронную сеть поддерживать осмысленный диалог, максимально приближенный к взаимодействию с одушевленным собеседником.
«Следующий же этап в развитии цифровых ассистентов, то, что происходит сейчас на наших глазах, – это совершенствование работы генеративного ИИ не только с текстами, но и с изображениями, звуками и видео. Это позволяет делать цифровых ассистентов еще более нативными, буквально стирая грань между общением с живым собеседником и машиной», – говорит Кулик.

Источник: ВТБ

записей встреч применяются глубокие языковые модели. Это один из первых промышленных кейсов применения больших языковых моделей в финансовой сфере.

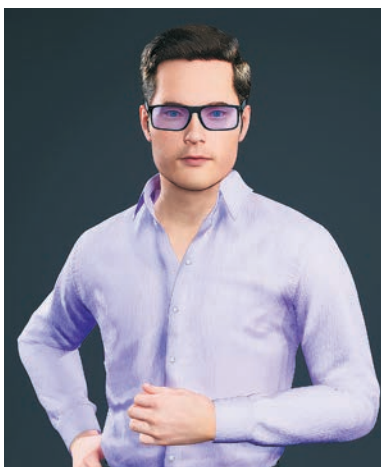
Третий кейс – RAG-платформа: инструмент, который позволяет любую базу знаний (собрание баз данных, пул открытых источников и др.) превратить в цифрового помощника, который может обрабатывать запросы пользователя, анализируя источники в базе знаний при помощи ИИ и выдавая пользователю максимально релевантный ответ.

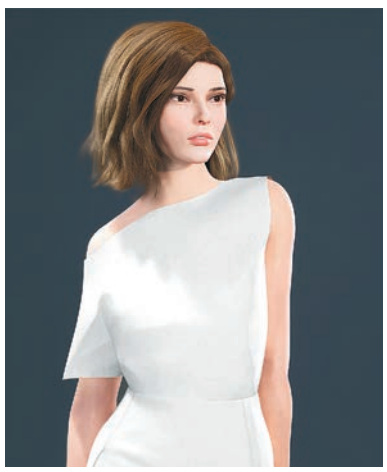
Мы можем наблюдать сегодня самую настоящую гонку цифровых ассистентов. Выиграет в этой гонке тот, чей ассистент будет узнавать о запросах и потребностях пользователя еще до того, как о них узнает сам пользователь

«В той или иной степени разработкой технологий цифровых помощников сейчас занимаются все крупные банки и финтехи. Более того, мы можем наблюдать сегодня самую настоящую гонку цифровых ассистентов. Выиграет в этой гонке тот, чей ассистент будет узнавать о запросах и потребностях пользователя еще до того, как о них узнает сам пользователь», – отметил топ-менеджер.

Совершенствование этих ассистентов позволит сделать их работу еще более нативной, они смогут лучше понимать контекст запросов клиентов и предоставлять более точные и релевантные ответы. Таким образом, к 2026 г. у каждого клиента и сотрудника ВТБ должен будет появиться свой цифровой помощник, говорит Кулик.

В конце 2023 г. банк ВТБ также объявил о разработке виртуального 3D-ассистента Тамара. Пока Тамара выполняет только простые задачи, такие как перевод средств или оплата услуг, но в будущем сможет анализировать предпочтения пользователей и предлагать им более сложные решения. Например, порекомендует оплатить счета в определенный день, чтобы получить бонусы или скидки, т. е. из помощника вырастет до уровня советника. В сентябре 2024 г. в банке также разработали мужской образ виртуального 3D-ассистента – Лео.





Виртуальные ассистенты ВТБ Лео и Тамара

Генеративные модели в будущем можно будет использовать в большом количестве коммуникационных сценариев в банках, ритейле и других отраслях, которые активно взаимодействуют с клиентами, объясняет руководитель группы продуктового развития речевых технологий Yandex Cloud Елена Белоброва. Это автоматизация входящих обращений в контакт-центрах, маршрутизация звонков на замену популярной до сих пор IVR («интерактивное голосовое меню»), автоматизация технической поддержки, обучение персонала, улучшение качества консультаций за счет подсказок операторам и многое другое. Применение генеративных моделей позволит многим компаниям существенно сократить затраты на рутинные операции, улучшить скорость и качество коммуникаций с клиентами, быстрее тестировать и внедрять новые продукты и процессы, перечисляет Белоброва.

Как голосовой помощник помог увеличить прибыль

Bank of America получил $7,41 млрд чистой прибыли во II квартале 2023 г., это на 19% больше по сравнению с аналогичным периодом годом ранее. Как отметил генеральный директор банка Брайан Мойнихан, в немалой степени это заслуга голосового помощника Erica.
С момента запуска в 2018 г. Erica провела более 1,5 млрд консультаций, помогая с переводом денег, информацией о состоянии счетов и поиском ближайшего отделения. Однако уже в 2023 г. более 60% ее взаимодействий с клиентами банка приходилось на более сложные задачи, например персонализированные советы о том, как оптимизировать свои расходы.

Источник: Fortune

ИИ как коллега и друг

С внедрением больших языковых моделей голосовые помощники сделали значительный шаг вперед в плане понимания контекста и способности вести сложные диалоги, говорит директор по направлению ИИ консалтинговой компании «ТеДо» Арсений Груздев. Сегодня, объясняет он, такие системы могут поддерживать разговор на уровне, который ранее казался возможным лишь в научной фантастике. Ассистенты теперь способны реагировать на различные нюансы речи и строить взаимодействие, максимально приближенное к человеческому.

Современные голосовые помощники позволяют значительно улучшить качество взаимодействия за счет более точного понимания контекста и способности адаптироваться к различным речевым стилям, добавляет Груздев. Они могут реагировать на сложные запросы и более качественно поддерживать диалоговый режим.

Свои разработки в области цифровых ассистентов сейчас ведут все крупнейшие банки, но большинство этих советников пока предполагают решения довольно узкопрофильных задач. В дальнейшем же на рынке непременно появятся советники, которые смогут не только сопровождать пользователя в финансовых вопросах, но и находить для него решения во всех основных сферах жизни, отмечает топ-менеджер ВТБ.

Генеративный ИИ поможет и разработчикам голосовых помощников. При классическом подходе к разработке голосовых помощников требуются серьезные ресурсы на настройку ответа под отдельные сценарии, объясняет Белоброва. А за счет генеративных моделей такие проекты удается реализовать быстрее, так как они позволяют формулировать ответы на вопросы, не предусмотренные изначальным скриптом, говорит она.

Несмотря на все преимущества, технология ставит перед разработчиками новые вызовы.

По словам Груздева, основные сложности при внедрении цифровых советников в крупных компаниях, например в крупных банках, связаны с вопросами безопасности и защиты данных. Ведь работа с конфиденциальной информацией требует строгого соблюдения регуляторных норм.

По мнению Белобровой, главный вызов – в скорости ответа. Когда мы общаемся с человеком, то в некоторых случаях можем получить ответ буквально за секунду и даже меньше. Чтобы робот ответил на вопрос, ему нужно распознать речь, отправить запрос к генеративной модели для формирования ответа, а затем синтезировать ответ модели в речь. И если традиционные речевые сервисы могут уложиться в одну секунду, то для генеративной модели нужно немного больше времени. Из-за долгой паузы ответы робота могут звучать неестественно, заключает Белоброва.

Роботы развивают эмоциональный интеллект

Пандемия COVID-19 увеличила частоту использования голосовых помощников, говорится в отчете Voxly Digital. Голосовой банкинг помогает оптимизировать бэк-офисные банковские процессы, ускоряет взаимодействие с клиентами. Согласно исследованию, опубликованному в PennState, люди с большей охотой общаются с ботом, который способен проявлять эмпатию и сочувствие. Рынок технологий, наделяющих роботов эмоциями, в 2022 г. оценивался в $23,5 млрд с прогнозом роста до $42,9 млрд к 2027 г.

Тем не менее, считает Кулик, со временем цифровые советники станут не просто инструментом для решения отдельных задач, но и настоящими компаньонами, способными сопровождать пользователей в любой жизненной ситуации. Такая «самодостаточность» модели возможна в первую очередь благодаря работе с большими объемами данных, которую генеративный ИИ делает быстрее, чем другие доступные на рынке технологии, отмечает он.

Создание полноценного цифрового советника отнюдь не тривиальная задача, констатирует Кулик. «Цифровой помощник должен четко выполнять простейшие команды пользователя, большего от него не ждут. А советник же должен знать о пользователе едва ли не все: кто он, чем занимается, какие товары и услуги он ищет в интернете, какие у него доходы... И на основе мгновенного анализа всех этих данных советник должен проактивно предлагать пользователю те или иные продукты и услуги. И, главное, ложка ведь хороша к обеду – вряд ли вы будете в восторге, если советник разбудит вас в 6 утра предложением взять в банке кредит», – резюмирует Кулик. &

Кредитная история искусственного интеллекта

Какой путь прошла технология

Более 70 лет назад ученые занялись поиском алгоритмов и устройств, способных мыслить, как люди. То, что вначале казалось футуристическими идеями, сейчас – работающий и активно используемый механизм. Поскольку банковская деятельность изначально основана на анализе больших объемов информации, финансовые учреждения стали пионерами применения искусственного интеллекта (ИИ) на основе машинного обучения для оценки данных о заемщиках. Сейчас ИИ используется в финансах гораздо шире – от предотвращения мошенничества до создания умных цифровых помощников для повышения качества услуг.

Чтобы понять, какой путь прошел ИИ за эти годы, мы подготовили ленту времени, в которой выделили знаковые события в становлении технологии.

1940-е **Появление первых скоринговых карт в банках США.** Информация о заемщике позволяет банку объективно принимать решение о том, выдавать ли ему кредит. Чтобы упростить и ускорить процесс оценки, были изобретены скоринговые карты, на которых отмечались стандартные пункты информации о заемщике и каждому на основе статистики присваивался определенный балл. Из суммы баллов формировался кредитный рейтинг. Поначалу кредитные специалисты делали это вручную, сейчас анализом кредитной информации занимаются компьютерные системы.

1943 Американские исследователи Уоррен Маккалок и Уолтер Питтс в научной работе «Логическое исчисление идей, присущих нервной деятельности» **предложили понятие искусственной нейронной сети.**

1950 Выдающийся английский математик Алан Тьюринг предложил **тест Тьюринга** как критерий для определения способности машины к мышлению. Этот тест стал классическим методом оценки ИИ.

1956 Дартмутский научный семинар, на котором был **впервые предложен термин «искусственный интеллект».** Этот семинар считается началом формального исследования ИИ как академической дисциплины.

1958–1960 Фрэнк Розенблатт в Корнеллском университете создал вычислительную систему Mark-1. Это была **первая действующая модель, способная обучаться при решении простейших задач распознавания изображений**: например, она отличала круги от квадратов любого цвета и различала буквы.

1966 Создание программы **ELIZA, первой программы для обработки естественного языка**, разработанной Джозефом Вейценбаумом. ELIZA имитировала поведение психотерапевта и показала потенциал для общения человека и машины.

1971 Советские ученые Владимир Вапник и Алексей Червоненкис публикуют фундаментальный труд, в котором описывают **размерность Вапника – Червоненкиса,** одно из ключевых понятий в их теории о статистическом машинном обучении.

1970-е **Первая «зима» ИИ.** Финансирование и интерес к ИИ снизились из-за разочарования в его реальных возможностях. Ожидания казались завышенными, а практическое применение – ограниченным.

2018 – сегодня **Российские банки активно развивают голосовых ассистентов**, используя как сторонние технологии, так и собственные разработки.

2018 ЦБ РФ назвал ИИ и анализ больших данных (big data) среди технологий, **определяющих развитие российского финансового рынка.**

2022 Компания OpenAI представила **чат-бот на основе генеративного ИИ ChatGPT,** одну из наиболее продвинутых моделей для обработки естественного языка, способную генерировать текст высокого качества и поддерживать осмысленные диалоги.

2010-е **Алгоритмы глубокого обучения (deep learning) и искусственные нейронные сети (Neuro AI) начали масштабно применяться в бизнесе** и показывать значительные успехи в задачах распознавания образов и речи благодаря наличию больших данных и вычислительных мощностей. Крупнейшие банки, такие как JPMorgan Chase, Wells Fargo, Capital One, начинают внедрять системы кредитного скоринга и оценки рисков на основе машинного обучения.

2024 **Генеративный ИИ стал массовой технологией с широким применением в различных областях** – от создания контента до поддержки решений в бизнесе и медицине. Одним из трендов в развитии этого направления, вероятно, станет внедрение все более совершенных голосовых ассистентов в банковских сервисах. Благодаря использованию технологий ИИ общение станет таким же простым и естественным, как общение с человеком.

1980-е Появление и развитие **нейронных сетей, включая изобретение алгоритма обратного распространения ошибки**. Эти методы стали основой для более сложных моделей машинного обучения. В это время также произошел второй всплеск интереса к ИИ с развитием экспертных систем.

2011–2012 Значительный **прорыв в распознавании изображений и объектов** в связи с усовершенствованием алгоритмов сверточных нейронных сетей (например, алгоритм AlexNet, победивший на конкурсе ImageNet с существенным снижением количества ошибок распознавания).

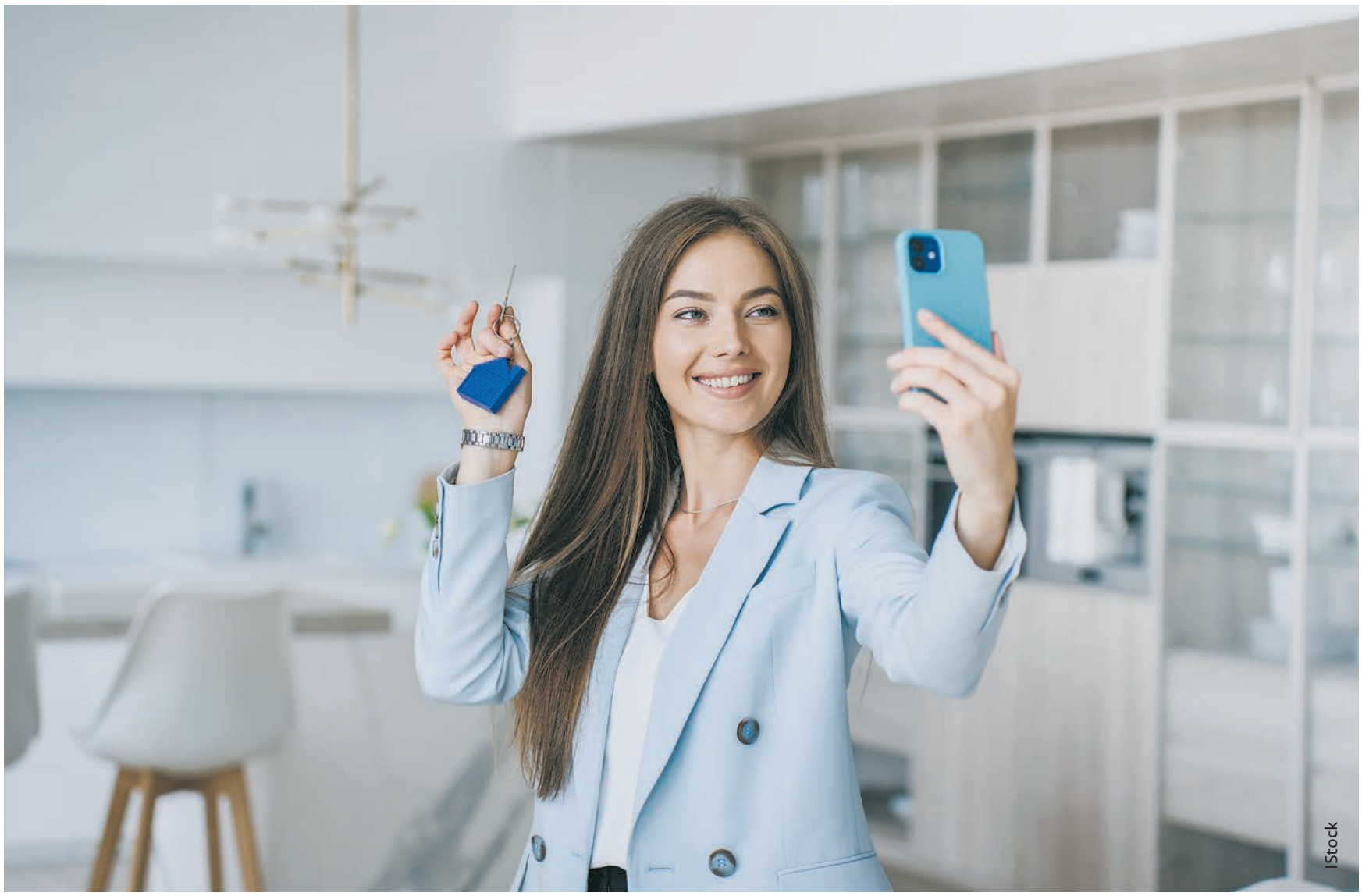
1987 Американский Security Pacific National Bank одним из первых начал использовать **экспертную систему с элементами ИИ** для противодействия мошенничеству и несанкционированному доступу к счетам. Система окупилась всего за два месяца.

2011 Компьютер IBM Watson DeepQA **победил в телевикторине Jeopardy!**, демонстрируя способности ИИ к восприятию естественного языка и быстрой обработке огромных объемов информации. Компания Apple в своем iPhone 4S презентовала Siri, первого полноценного голосового помощника.

1987–1993 **Вторая «зима» ИИ.** Интерес к экспертным системам снизился из-за их дороговизны и ограниченных возможностей. Финансирование и поддержка со стороны промышленности уменьшились.

1997 Суперкомпьютер Deep Blue компании IBM **победил чемпиона мира по шахматам Гарри Каспарова.** Это событие показало потенциал ИИ в решении сложных задач, требующих стратегического мышления.

Источник: Ассоциация «ФинТех», информация из открытых источников



IStock

Ипотека за 20 минут: как искусственный интеллект меняет ипотечные сделки

Новые технологии уже делают клиентский путь более удобным и быстрым

Олеся Ошанина

Российские банки все активнее внедряют инструменты на основе искусственного интеллекта (ИИ). В институте развития жилищной сферы Дом.РФ применение технологий ИИ в ипотеке считают не делом будущего, а «технологиями настоящего»: они уже помогают работать эффективнее на всех стадиях ипотечного цикла – от оценки застройщика до заключения сделки с покупателем квартиры.

Ипотека цифровизируется

Цифровизация в финансовом секторе – мировой тренд, и Россия здесь среди лидеров. По итогам 2023 г. в результате внедрения инноваций доля финансовых цифровых услуг выросла с 78,7 до 83,4%, а доля услуг для бизнеса – с 72,1 до 80,2%, следует из данных ЦБ.

В ипотечном бизнесе, по данным Ассоциации «ФинТех» (АФТ), в 2023 г. более половины (53%) заявок на ипотечный кредит банки получали через цифровые каналы обслуживания.

Еще несколько лет назад проведение ипотечных сделок полностью онлайн казалось невозможным, вспоминают эксперты. «В 2010–2015 гг. неделя ожидания ответа от банка по заявкам на ипотеку считалась нормальным сроком, сейчас процесс занимает минуты», – рассказывает заместитель председателя правления банка Дом.РФ (входит в группу Дом.РФ) Николай Козак. Срок получения ипотеки может по разным причинам варьироваться от 1 до 14 дней, но в среднем, по статистике банка, клиенты, которые подают заявку онлайн и пользуются сервисом цифрового профиля, выходят на сделку на 7–10 дней раньше, чем те, кто предпочитает оформлять все по старинке на бумаге. В первом полугодии 2024 г. цифровой ипотекой в банке Дом.РФ воспользовалось более 21 000 семей – это в 2,5 раза больше, чем за первые шесть месяцев прошлого года. Всего доля дистанционной ипотеки в банке Дом.РФ составляет почти 85%.

ИИ на службе

По словам руководителя управления стратегии, исследований и аналитики АФТ Марианны Данилиной, одной из причин активного развития цифровой ипотеки стало внедрение банками технологий ИИ.

«АФТ разработан бесшовный цифровой клиентский путь в ипотеке. Сделать его полностью цифровым и бесшовным помогает как использование ИИ, так и применение открытых API (программных интерфейсов для взаимодействия разных систем. – «Ведомости&») в рамках обмена информацией между участниками ипотечного процесса. Кроме того, используется цифровой профиль – для быстрого заполнения и андеррайтинга заявки, а также сервис «Госключ» на этапе подписания документов и регистрации залога», – указывает она.

Для развития технологии в 2023 г. Дом.РФ создал ИИ-лабораторию, которая разрабатывает прикладные решения как для бизнес-процессов самой компании, так и для других участников рынка строительства и банковского сектора.

Одним из первых таких решений в ноябре 2023 г. стал интеллектуальный чат-бот в мобильном приложении банка Дом.РФ. Благодаря использованию ИИ-технологий за семь месяцев удалось автоматизировать более 60% обращений клиентов: ответы на запросы предоставляются в среднем за 3,5 клика без необходимости обращаться к операторам, рассказывают в банке. Чат-бот классифицирует обращения, направляет клиента в соответствующие разделы приложения, помогает получить необходимые справки и выбрать подходящую ипотечную программу. В итоге более 90% общих вопросов решается с его помощью.

Одно из новейших решений от Дом.РФ – запущенный в начале июля сервис для распознавания информации из договоров на покупку недвижимости, созданный на базе технологий машинного обучения. Решение уже применяется в системе банка Дом.РФ.

«Если раньше сотрудникам вручную приходилось перебивать информацию из договора застройщика в систему, то теперь это делает ИИ-решение на основе компьютерного зрения. Оно распознает необходимые данные и автоматически заносит их в нужные поля карточки клиента. Оператору остается только проверить сведения и передать информацию для дальнейшего использования. ИИ-модель постоянно обучается и помогает распознавать даже нестандартизированные договоры застройщиков. Таким образом, снижается риск опечаток и ошибок и ускоряется внутрибанковский документооборот», – говорит Козак. Впоследствии банк планирует использовать эту технологию не только для договоров долевого участия, но и для других документов, которые необходимы для сделки, отмечает эксперт.

«Ключевое условие для пилотирования и внедрения ИИ-моделей – это большой объем данных. В ситуации с Дом.РФ эти данные имеются, поскольку банк Дом.РФ занимает 3-е место в России по объему выдачи ипотечных кредитов, а институт развития Дом.РФ обладает информацией по всему жилищному строительству в стране через портал наш.дом.рф. Все это создает базу для создания инноваций с применением ИИ на стыке финансов и жилищного строительства, в частности в ипотеке», – говорит Козак.

ИИ в российских банках

Другие крупные игроки также активно внедряют технологии ИИ в ипотечном кредитовании. В Россельхозбанке (РСХБ) рассказали «Ведомости&», что на сегодняшний день разрабатываются ML-модели (модели машинного обучения. – «Ведомости&») для формирования персонализированных предложений для клиентов на основе их поведенческих данных и потребностей. Также специалисты РСХБ ведут работы по интеллектуальной маршрутизации обращений в контакт-центр, прогнозирование предпочтительного канала коммуникации с клиентом. Первый заместитель председателя правления Сбербанка Кирилл Царев ранее отмечал, что банк внедрил ИИ в основные процессы ипотечного кредитования и сопутствующих услуг – от поиска недвижимости до проведения сделок с жильем.

Николай Козак, заместитель председателя правления банка Дом.РФ

«Ранее ИИ считали «технологией будущего», так как не совсем понимали, какие эффекты можно от него ожидать. Сейчас ИИ – это «технология настоящего», и плюсы от его использования очевидны. Дом.РФ как институт развития в жилищной сфере старается внедрить ИИ-решения на всех этапах и для всех участников жизненной ситуации, связанной с жильем: от старта инвестиционно-строительного цикла застройщика до оповещений об очередном ипотечном платеже в чат-боте. При этом многие улучшения находятся «под капотом», они не видны обычному пользователю, но с ними точно жить стало лучше».

Альфа-банк, согласно официальным сообщениям кредитной организации, использует технологию ИИ для одобрения ипотечных кредитов.

ИИ в песочнице

Сейчас в Технологической песочнице АФТ проходят пилотирование ряд проектов, связанных с применением ИИ как в облачной инфраструктуре, так и в контуре финансовых организаций, говорит Данилина. Пилотные проекты на площадке АФТ по внедрению отечественных больших языковых моделей (разновидность ИИ. – «Ведомости&») уже позволили участникам снизить стоимость решений и длительность их реализации внутри самих компаний. «Результаты пилотов АФТ позволяют нашим участникам ускорить разработку цифровых продуктов и сервисов, – указывает эксперт. – Дополнительно работа с командой АФТ позволяет банкам сделать расчет экономической эффективности внедрения решений на базе ИИ для обоснования открытия соответствующих проектов внутри банков». Участники песочницы ассоциации первыми получают доступ к самым современным технологическим решениям, обмениваются опытом и кейсами применения ИИ в своих организациях, отмечают в АФТ. «Как мы видим на опыте Дом.РФ, адаптация таких кейсов помогает компаниям отрасли создавать новые продукты и сервисы, а также сделать существующие удобнее и безопаснее», – резюмирует глава АФТ Максим Григорьев.

В Дом.РФ рассказали «Ведомости&», что пилотируемые на сегодняшний день проекты банка направлены на внедрение генеративных языковых моделей в ипотечном кредитовании. Один из пилотов уже прошел оценку эффективности и готовится к запуску в эксплуатацию – это сервис анализа тональности новостного фона в рамках мониторинга контрагентов проектного финансирования банка Дом.РФ с применением генеративной языковой модели GPT. «Нейросеть проводит своего рода «скоринг для застройщиков»: анализирует общедоступную информацию о потенциальном получателе кредита и с точностью свыше 93% определяет факторы повышенного риска, на которые стоить обратить внимание при выделении финансирования», – поясняют в Дом.РФ.

Заглядывая в будущее

Эксперты уверены, что в будущем ИИ продолжит играть одну из ведущих ролей в развитии ипотечных сервисов. По данным Deloitte, 86% пользователей ИИ в сфере финансовых услуг говорят, что эта технология будет очень важна или даже критически важна для успеха бизнеса в ближайшие два года.

На сегодняшний день технологии ИИ пока используются в ипотечном бизнесе не в полной мере. «Существует несколько сфер в ипотечном кредитовании, где использование ИИ имеет большой потенциал для развития в будущем, – указывает Данилина. – Например, персонализированные финансовые консультации с помощью ИИ». ИИ-ассистент может анализировать индивидуальные финансовые данные клиентов и предлагать рекомендации по ипотечным продуктам. Система может учитывать не только кредитную историю, но и доходы, расходы и жизненные цели заемщика для создания уникального предложения. Дополнительно повсеместное внедрение систем распознавания документов может помочь полностью избавиться от бумажного документооборота в рамках ипотечной сделки, отмечает она.

В РСХБ добавляют, что одним из перспективных направлений использования ИИ в ипотеке является разработка адресных ипотечных программ – после завершения массовой льготной ипотеки государство планирует перейти к более целевой поддержке определенных категорий граждан, таких как учителя, молодые специалисты и жители отдельных регионов.

Еще одно направление – прогнозирование объемов досрочного погашения ипотечных кредитов. В РСХБ идут работы по данному направлению, подчеркивают в банке. «Наличие такого решения позволит более точно определять размер компенсационных выплат от застройщиков и устанавливать процентную ставку для клиента-физлица за счет выявления поведенческих и продуктовых факторов, – уверены в РСХБ. – Это должно повысить точность прогнозирования темпа досрочных погашений по ипотечным кредитам более чем на 10%».

В Дом.РФ считают, что ИИ может не только существенно сократить время на получение финансовых услуг, но и создать абсолютно новые бизнес-процессы в банках, которые по скорости и удобству будут превосходить предыдущее поколение сервисов.

«Благодаря автоматизации и ИИ мы хотим достичь целевой модели по скорости оформления ипотеки в нашем банке – 20 минут. Таким образом, получить ипотеку под ключ в перспективе можно будет буквально за утренним кофе. Уверен, что со временем появится еще больше сценариев, где ИИ коренным образом изменит путь клиента и создаст «услуги будущего» в финансовой отрасли», – говорит Козак. &

Платить без карты и смартфона

Где и как используют ИИ в биометрии и финтехе

Мария Салтыкова

По данным Transparency Market Research, объем рынка биометрии на основе технологий искусственного интеллекта (ИИ) достигнет $50,5 млрд к концу 2031 г. В России отрасль активно развивается: в метрополитене Москвы оплатой проезда по биометрии воспользовались уже более 90 млн раз, X5 Group и «Сбер» запустили сервис оплаты с помощью улыбки. «Ведомости&» разбирались, где сегодня используют биометрию и ИИ в финтехе, что это дает и насколько это безопасно для пользователей.

Селфи вместо кредитки

Лучший пример использования ИИ в биометрии в финтехе – это биоэквайринг (оплата покупок при помощи биометрических данных, например по фото лица и голосу), уверен советник гендиректора по искусственному интеллекту Ассоциации «ФинТех» Алексей Сидорюк. По его словам, эта технология позволяет упростить процесс оплаты в торговых точках, когда под рукой нет ни карты, ни смартфона.

В перспективе такая технология может применяться практически везде, где нужно что-то оплатить, считают в ассоциации. «Например, при заселении в гостиницу с помощью биометрии человек сначала оплачивает пребывание, затем автоматически регистрируется и получает доступ в номер (без паспорта, без карты, без ключа)», – поясняет Сидорюк. Аналогично, по его словам, клиент может оплачивать продукты с помощью биометрии: «Не пользуясь кредитной картой, картой лояльности и не показывая паспорт при покупке отдельных категорий товаров».

Сейчас среди крупных банков биоэквайринг активно использует «Сбер» – в виде сервиса «Оплата улыбкой», запущенного в 2021 г. В июле 2024 г. банк сообщал, что клиент сделал самую большую покупку с помощью этого сервиса – на 2,2 млн руб., оплатив автомобиль в одном из московских автосалонов.

Национальная система платежных карт (НСПК) в 2024 г. начала делать платформу биометрических сервисов, которая должна выступить связующим звеном между локальными решениями банков по биоэквайрингу. В мае этого года в НСПК сообщали «Ведомостям», что приглашают банки подключиться к тесту. Гендиректор НСПК Дмитрий Дубынин в начале июля заявил, что проект планируется завершить до конца месяца, но компания еще не объявляла итоги эксперимента.

Пока в рамках проекта НСПК по биоэквайрингу ввели только оплату по лицу (FacePay) в Казани – с 30 августа, при поддержке банка «Ак барс». FacePay действует так же, как в Москве, где этот способ используется с 2021 г. По данным отчета Ассоциации «ФинТех», московским FacePay за четыре года воспользовались 90 млн раз, сейчас к системе подключено 330 000 пользователей. В 2024 г. кроме Казани систему планируется распространить еще в пяти городах: Санкт-Петербурге, Нижнем Новгороде, Екатеринбурге, Самаре и Новосибирске.

Ладонь вместо паспорта

Собранные биометрические данные банки обязаны передавать в государственную Единую биометрическую систему (ЕБС), созданную в 2018 г. Большинство банков запрашивают у клиентов (по их желанию) только фото лица и записи голоса. Один из самых крупных участников рынка – ВТБ, по данным пресс-службы банка, собирает такие данные более чем в 1200 отделениях. Фото и аудиозаписи обрабатываются автоматически, с использованием ИИ. На сегодня биометрию сдали уже почти 1,3 млн человек, уточняют в пресс-службе.

Некоторые, как Газпромбанк, используют и другие данные. «В ряде отделений по желанию клиентов оказывается услуга доступа к банковским ячейкам с помощью аутентификации по рисунку вен ладони», – рассказывает вице-президент Газпромбанка Павел Салугин. Обработка биометрических образцов, их преобразование в векторы и сравнение этих векторов с эталонными задействует специальные обучаемые алгоритмы (ИИ), отмечает топ-менеджер.

Биометрия (изображение лица и запись голоса, которые передаются в ЕБС), по словам Салугина, используется для удаленной идентификации граждан, которые пока не являются клиентами банка. После успешного входа на сайте или в мобильном приложении человек может открыть счет и получить полный доступ к дистанционному банковскому обслуживанию без посещения офиса.

В Россельхозбанке в отличие от коллег заявляют, что обходятся без ИИ. По данным пресс-службы, «банк проводит сбор только тех биометрических данных, которые установлены действующим законодательством (фотоизображение лица и запись голоса), и только для целей размещения этой биометрии в ЕБС. Для обработки такой биометрии на стороне банка используются только регламентированные государством и оператором ЕБС решения и технологии, применение ИИ в данном процессе не предусмотрено».

Мошенники против технологий

Современные технологии ИИ применяются и злоумышленниками. Новым типом угроз, как отмечается в отчете Ассоциации «ФинТех», стало использование дипфейков (deepfake) – синтезированных с помощью ИИ видео, изображений, звука и других данных. Банки, которые используют биометрию, впрочем, не боятся угрозы.

«Нейронные сети, которые используются сейчас для проверки биометрии, успешно выявляют различные типы фейков, обнаруживая редактирование изображений и невидимые человеческому глазу артефакты. Более того, именно биометрическая аутентификация позволяет предотвратить мошенничество, подтверждая, что именно этот клиент находится сейчас перед экраном мобильного устройства или предъявляет паспорт в отделении банка», – поясняет Салугин из Газпромбанка.

Сами банки при этом не хранят данные клиентов, ответственность за защиту биометрии возлагается на государство. По закону сбор и хранение биометрии где-либо, кроме государственной системы ЕБС, с 1 июня 2023 г. запрещены, уточнили в пресс-службе ВТБ. Сбор биометрии в банке проводится «с применением типового решения, сертифицированного аттестованной ФСБ лабораторией по защите биометрических персональных данных», указали в пресс-службе.

В НСПК дипфейки не считают чем-то новым и более опасным, чем прежде. «Deepfake – это лишь генерация изображения человека. Для атак мошенники могут использовать и простое фото человека, поэтому создание deepfake-подделок не создает дополнительных угроз», – поясняет директор операционно-технологического департамента НСПК Максим Крукелис.

«Чтобы мошенники смогли использовать deepfake или оригинальное изображение лица для обмана биометрических систем, им нужно показать их, например, с экрана устройства. Для отражения таких атак используют алгоритмы проверки живого присутствия – Liveness-алгоритмы. Они подтверждают, что перед камерой действительно находится живой человек», – рассказывает Крукелис.

По его словам, сейчас мошенники могут также пытаться подменить данные в канале передачи данных на deepfake-подделку. Для защиты от такого рода угроз используется защищенный канал передачи информации. «Дополнительно в контурах биометрических систем могут быть установ-

Почему не все доверяют биометрии

По результатам опроса, проведенного в 2023 г. Всероссийским центром изучения общественного мнения, **32%** россиян негативно относятся к сдаче биометрических данных, **27%** – положительно, **34%** – нейтрально. Еще **7%** респондентов затруднились ответить.
Четверть (**25%**) тех, кто негативно относится к биометрии, объяснили это тем, что сбор биометрических данных нарушает права и свободы человека, **7%** считают, что это контроль и слежка за человеком, **4%** назвали сбор таких данных цифровым концлагерем и отметили, что государство использует эти данные против людей, **11%** опасаются утечек данных.

IStock

лены deepfake-детекторы, они выявляют наличие признаков подделки на изображении», – отмечает эксперт.

Затраты против выгоды

В первые годы после запуска ЕБС некоторые крупные банки жаловались, что затраты на сбор и обработку биометрических данных себя не оправдывают. В частности, Альфа-банк в 2019 г. сообщал, что потратил на создание соответствующей инфраструктуры $1,5 млн, но это «недешевое удовольствие» не окупается, спроса у клиентов нет и инфраструктура простаивает. Впрочем, ситуация быстро изменилась: в 2021 г. доля клиентов, сдавших биометрию, по данным банка, выросла до 25%.

В ВТБ к затратам на внедрение биометрии относятся спокойно. «На начальных этапах такие проекты всегда требуют значительных инвестиций. Мы вкладываемся в это направление, так как в будущем технология позволит оптимизировать многие банковские процессы, а также защитит клиентов от операций с их финансами без их ведома», – сообщили в пресс-службе банка.

Как уточняют в Россельхозбанке, действующее законодательство обязывает банк создать и поддерживать актуальность собственной биометрической системы (для сбора биометрии и предоставления услуг клиентам. – «Ведомости&»). Инвестиции банка в эту сферу, по данным пресс-службы, «носят многослойный характер»: они включают «исполнение регуляторных требований, вложения в развитие передовой технологии, предложение клиентам новых форм дистанционного обслуживания и банковских услуг посредством биометрических сервисов».

Чтобы внедрить оплату по биометрии, банкам нужно создавать инфраструктуру не только у себя, но и у партнеров – например, торгово-сервисных предприятий, отмечает сооснователь консалтинговой компании Futureproof Егор Кривошея. Пока в развитие POS-терминалов (портативных электронных терминалов для оплаты. – «Ведомости&») с биометрией инвестировали только крупнейшие банки, например «Сбер». В итоге пока не ясно, какой тренд победит: уменьшенные версии платежных карт, которые можно носить с собой, такие как стикеры и брелоки, или биометрия (оплата по лицу и т. д.). Но у биоэквайринга хорошие шансы – «его можно использовать и на смартфоне, и в терминалах», считает эксперт.

Пока клиенты банков оценивают соотношение выгод и рисков как не очень приемлемое, для самих банков финансовые затраты на внедрение [биометрии] тоже играют сдерживающую роль, отмечает председатель правления Ассоциации «Финансовые инновации» Роман Прохоров. Сам термин «биоэквайринг», по его мнению, неверен: «Эквайринг – уходящая технология. Скорее это био-СБП (система быстрых платежей. – «Ведомости&»)». Биометрическую идентификацию, по его словам, «вполне безопасно использовать для проведения операций на небольшие суммы – например, до 10 000 руб. Свыше лучше применять многофакторную аутентификацию, сочетающую биометрию и что-то еще, например старые добрые пароли». &

Сколько стоит сбор биометрии

С 2023 г. все биометрические данные россиян должны храниться только в Единой биометрической системе (ЕБС). Компании, которые ранее собирали такие данные, должны передать их в эту систему. Тарифы ГИС ЕБС опубликованы на ее сайте: за векторы на клиентов (математические шаблоны, за счет которых происходит распознавание. – «Ведомости&»), слепки которых сами банки передавали в систему, они должны платить от 2,55 до 3 руб. (2,55 руб. – при запросах от 1 млн в год, 3 руб. – при единичных запросах).
В июле 2023 г. банки обращались к Минцифры с просьбой освободить их от платы за использование биометрии. По оценке Национального совета финансового рынка, такая модель тарификации предполагала затраты более 500 млн руб. в год для базы размером около 20 млн образцов и делала сбор биометрии «нецелесообразным».

& ВЕДОМОСТИ

Рекламно-информационное приложение к газете «Ведомости»

16+

Фото на обложке: IStock

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

Учредитель и издатель АО «Бизнес Ньюс Медиа»
Адрес учредителя и издателя: 127018 Москва, вн. тер. г. муниципальный округ Марьина Роща, ул. Полковая, 3, стр. 1
Адрес редакции: 127018 Москва, ул. Полковая, 3, стр. 1, пом. I, 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)

Отпечатано в типографии ООО «Типография «Галла-М»
Адрес: Москва, ул. Прянишникова, 19 А, стр. 4

Тираж 48 000
Цена свободная

Риски от ума

Как будет развиваться страхование искусственного интеллекта

Алексей Охлопков

Финансовые организации активно применяют искусственный интеллект (ИИ) для решения самых разных задач – от риск-менеджмента и выявления мошенничества до автоматизации рутинных процессов. Однако внедрение ИИ несет не только очевидные выгоды, но и новые риски, причем как для самих финансовых организаций, так и для их клиентов. «Ведомости&» поговорили с экспертами страхового рынка о том, какие возможности открывает и какие сложности создает для отрасли новая сфера деятельности в области страхования ИИ.

Новые риски и старые угрозы

Внедрение ИИ в финансовом секторе создает специфические риски, отличающиеся от традиционных угроз, считает генеральный директор Ассоциации «ФинТех» Дмитрий Ищенко. В отличие от традиционного программного обеспечения (ПО) ИИ обладает возможностью адаптивного поведения, сложностью и непрозрачностью алгоритмов, динамической обработкой данных и высокой степенью автономности. «Эти особенности делают ИИ мощным инструментом, но также источником новых и более сложных рисков, требующих обновленных стратегий управления. Например, системы ИИ могут самостоятельно изменять свои решения на основе новых данных, что делает их поведение менее предсказуемым по сравнению с традиционным ПО», – поясняет эксперт.

Финансовый сектор уже не первое десятилетие занимается попытками внедрения ИИ-алгоритмов в свою работу, говорит Михаил Мосесов, руководитель управления развития андеррайтинга и работы с рисками СК «Абсолют страхование». Сейчас ИИ активно работает в направлениях риск-менеджмента и антифрода (борьбы с мошенничеством). В частности, в процессах оценки клиента и сопутствующих ему финансовых рисков. По мнению Мосесова, основные риски использования ИИ в финансах можно разделить на две категории. Первая – риски для самих финансовых организаций, которые сводятся к «контролю за качеством разработки». Вторая – риски для клиентов – физических лиц, главным из которых является «алгоритмическая предвзятость» (дискриминационное поведение ИИ по отношению к людям из-за ошибок в его обучении и настройке. – «Ведомости&»).

Игорь Лаппи, генеральный директор «Совкомбанк страхования» и руководитель Страховой группы Совкомбанка, считает, что в общем ИИ в финансовом секторе не создает принципиально новых рисков, а скорее становится новым источником уже известных угроз. «Все они так или иначе связаны с традиционными угрозами для клиентов финучреждения и самого фининститута. Это утечка критически важных персональных данных, выдача необеспеченных кредитов и т. п. То есть все те ошибки или умышленные деяния, которые может совершить человек, случайно или умышленно, может допустить и ИИ», – объясняет он.

К специфическим рискам, связанным с особенностями функционирования систем ИИ, эксперт относит непрозрачность внутренней логики работы моделей ИИ (работа по принципу черного ящика), что затрудняет аудит/контроль бизнеса, рассказывает Лаппи. Кроме того, есть риски, связанные с алгоритмическими ошибками, вырождением моделей, изменением паттерна данных и рыночных условий – все это может приводить к тому, что ИИ-модели становятся неактуальными. Помимо этого остается опасность, что сами модели ИИ могут быть использованы не по назначению. Например, когда в важных для бизнеса процессах используются модели, обученные на данных и особенностях других бизнес-кейсов, либо допущено «галлюцинирование нейронных сетей» (так называется эффект, когда генеративный ИИ начинает выдавать случайные или неадекватные запросу результаты. – «Ведомости&») в критически важных процессах, перечисляет Лаппи.

Инструменты страхования

Само по себе страхование ответственности при использовании ИИ вписывается в общую концепцию страхования киберрисков, полагает Анар Бахшалиев, исполнительный директор СОГАЗа. По его словам, основным драйвером данного вида страхования является постоянное увеличение участия информационных систем в бизнес-процессах компаний, рост их автономности и повышение уровня решаемых задач. «В такой модели роль киберстрахования возрастает, поскольку контролировать убытки, вызванные нарушениями в работе информационных систем, становится все сложнее», – указывает он.

На мировом рынке уже существуют специализированные страховые продукты, такие как киберстрахование, страхование профессиональной ответственности и страхование технологических рисков, которые покрывают убытки от инцидентов с участием ИИ, отмечает Ищенко. В России похожие продукты тоже есть, и они могут быть адаптированы для покрытия рисков, связанных с ИИ. Такие страховые решения становятся все более востребованными по мере роста использования ИИ в финтехе, но в целом рынок находится в начале своего развития, считает эксперт.

В большинстве случаев существующие продукты являются частью более общих программ страхования киберрисков. Например, ущерб от перерывов в деятельности или расходы на восстановление информационных систем. Однако спрос на такие продукты не очень высок, согласен представитель Всероссийского союза страховщиков (ВСС).

Точка роста для рынка

По оценке Deloitte, при годовом темпе роста около 80% к 2032 г. страховщики в глобальном масштабе смогут записать на свой счет около $4,7 млрд страховых премий за страхование рисков, связанных с ИИ.

«Тем не менее инциденты, такие как сбои в алгоритмической торговле, кибератаки и ошибки в автоматизированных системах скоринга, демонстрируют потенциальные риски. Финансовые и страховые организации активно готовятся к таким угрозам и прорабатывают соответствующие страховые продукты для их покрытия», – объясняет Ищенко.

Помимо корпоративного страхования от киберрисков на рынке есть множество других продуктов, связанных с ИИ. Например, страхование беспилотных летательных аппаратов, в котором страхуется как сам аппарат, так и ответственность перед третьими лицами. В этом случае страховая компания не выделяет сбой работы мотора от сбоя в работе ИИ. Другим примером продуктов может быть страхование беспилотных автомобилей, которое страховой рынок предлагает уже сравнительно давно, рассказывает директор департамента машинного обучения и работы с данными «Альфастрахования» Александр Логачев.

ОСАГО для ИИ

О возможном ущербе от ИИ и способах застраховаться от него задумались и законодатели. В июне 2024 г. Госдума в третьем чтении приняла поправки в закон «Об экспериментальных правовых режимах (ЭПР) в сфере цифровых инноваций в РФ». Согласно поправкам, создатели технологий на основе ИИ, работающие в ЭПР, будут обязаны страховать ответственность за возможный вред жизни, здоровью или имуществу, связанный с применением их разработок.

По мнению Ищенко из Ассоциации «ФинТех», принятие нового закона об обязательном страховании вреда от ИИ в рамках ЭПР окажет значительное влияние на страховую отрасль и финансовый сектор. Он как минимум повысит доверие к ИИ-технологиям, а также простимулирует развитие специализированных страховых продуктов и увеличит конкурентоспособность финансовых организаций, уверен он.

Риски уже здесь

В июне 2023 г. два нью-йоркских адвоката и их юридическая фирма были оштрафованы в общей сумме на $5000 за предоставление в суд недостоверной информации о прецедентах, которую они получили с помощью генеративного ИИ ChatGPT.

В сентябре 2023 г. 17 известных авторов книг, включая Джорджа Мартина и Джона Гришема, подали иск против компании OpenAI, разработчика ChatGPT. По мнению истцов, компания без разрешения использовала тексты их книг для обучения своего ИИ.

В августе 2024 г. нью-йоркская репетиторская компания iTutorGroup согласилась на урегулирование спора в размере $365 000 с Комиссией США по равным возможностям при трудоустройстве после обвинений в том, что ее ПО для проверки кандидатов на работу с использованием ИИ дискриминировало людей старше 55 лет.

Источник: Reuters, Inc., The Verge

Принятие этих поправок может существенно повлиять на развитие рынка страхования ИИ-рисков, согласны в ВСС. Пока зарегистрированных в ЭПР компаний не так много – около 200. Но в союзе надеются, что сектор будет расширяться. «В целом ИИ, существующего вне рамок ЭПР, гораздо больше, чем в реестре. Но желание добровольно страховать свои риски будет обусловлено тем, как риски, связанные с использованием ИИ, будут реализовываться в будущем и как будет меняться регуляторная среда», – добавляют в ВСС.

Важнейшим вопросом в контексте страхования ИИ-рисков является оценка ущерба и урегулирование убытков. Эксперты ВСС отмечают, что с 2025 г. это будет зависеть от того, используется ИИ в рамках ЭПР или нет.

«В законе описано и как определять ответственное лицо, и как должны расследоваться инциденты. Предполагается, что на уровне Минэкономразвития или – в случае инцидента на финансовом рынке – на уровне Банка России будут создаваться соответствующие комиссии, которые будут осуществлять расследование. Если ИИ использовался вне ЭПР, то факт причинения вреда, причинная связь и размер причиненных убытков будут определяться в рамках обычного гражданского оборота», – поясняют в ВСС.

Развивать нормативно-правовую базу в сфере страхования ИИ-рисков надо и дальше, уверен Лаппи из «Совкомбанк страхования». «Необходимо четко классифицировать понятие риска по отношению к ИИ, определить зону ответственности разработчика и его ПО, которым, по сути, сегодня является ИИ, установить прямую причинно-следственную связь между действиями ИИ и причиненным ущербом. Определить характеристики страхового случая, способы урегулирования убытков, причиненных ИИ, меру ответственности», – перечисляет он.

ИИ под присмотром

Один из ключевых вопросов как для финансовых организаций, так и для страховщиков – оценка и минимизация рисков, связанных с использованием ИИ. По мнению экспертов ВСС, уровень риска напрямую зависит от того, какие функции выполняет система. «Если ИИ используется в целях поддержки принятия решений, уровень риска ниже. Если ИИ самостоятельно принимает решения, то риск возрастает. Это также влияет на размер возможного ущерба», – говорит представитель ВСС.

Пространство для экспериментов

ЭПР – это так называемая регуляторная песочница, в которой разработчикам новых технологий разрешается соблюдать действующее законодательство с рядом особенностей, которые как раз и позволяют им работать, оставаясь при этом в правовом поле. Необходимость создания таких песочниц объясняется тем, что процесс законотворчества не успевает за научно-техническим прогрессом. Новые технологии, такие как ИИ, блокчейн, большие данные, квантовые технологии, виртуальная реальность, благодаря регуляторным песочницам могут теперь обкатываться в самых разных сферах: медицине, транспорте, сельском хозяйстве, дистанционной продаже товаров и услуг, финансовой деятельности, строительстве, промышленности, связи и т. д.

Источник: Минэкономразвития

IStock

При этом, как отмечают в ВСС, процедуры оценки риска ИИ-системы должны учитывать не только ее технические характеристики, но и особенности бизнес-процессов, в которые она встроена. «Оценить риск от использования ИИ может бизнес-аналитик, проанализировав, как выстроены бизнес-процессы в финансовой организации и уровень риска, который увеличивает или снижает использование в них ИИ, а также IT-специалист – в части надежности самих технологических решений. Вполне логично делать аудит ИИ-систем перед заключением страхового договора и с разумной периодичностью в течение срока его действия. Либо запрашивать страхователя о таком аудите, проделанном внешними подрядчиками», – поясняют в ВСС.

По мнению Ищенко, для адекватного регулирования рисков ИИ в финтехе необходимы значительные изменения нормативно-правовой базы. Нужно вводить стандарты разработки, обязательные аудиты и сертификацию ИИ-систем и помимо прочего правила для предотвращения дискриминации, уточняет он.

Представитель компании «Зетта страхование» рекомендует в первую очередь повышать квалификацию специалистов, работающих с ИИ. Иногда даже стоит умышленно упрощать модели для большей интерпретируемости и репрезентативности результатов, считает он. Кроме того, нужно анализировать взаимосвязи между интегрируемыми моделями, повышать культуру работы с данными, постоянно отслеживать и валидировать (проверять на достоверность. – «Ведомости&») получаемые результаты и искать причины аномалий в работе систем.

Эксперты ВСС, в свою очередь, также рекомендуют финансовым организациям внимательно относиться к новым непроверенным решениям, больше времени уделять пилотному тестированию и регулярным проверкам результатов работы ИИ-систем, говорит представитель ВСС.

В «Альфастраховании» считают, что для эффективного управления рисками ИИ необходимы специализированные технические решения. Например, системы логирования (протоколирования действий. – «Ведомости&») и проведения экспериментов, системы контроля за качеством и описанием данных (Data Governance). «Системы мониторинга моделей позволяют определить, когда стоит переобучить модель в связи с изменившимися внешними условиями или ее естественным устареванием. Системы кибербезопасности защищают как данные, так и модели от несанкционированного доступа или атак с целью злоупотребления или влияния на алгоритмы», – поясняет Логачев.

По его мнению, ключевым фактором успеха является также наличие у компании сильной команды своих специалистов или проверенных консультантов высокого уровня извне. «И тогда они смогут минимизировать риски, связанные с использованием ИИ», – резюмирует он.

Взгляд в будущее

В ближайшие 5–10 лет рынок страхования рисков ИИ в финтехе ожидает активное развитие благодаря росту спроса на специализированные полисы и повышенному вниманию со стороны регуляторов, уверены в Ассоциации «ФинТех». «Финансовые организации будут стремиться минимизировать риски, связанные с ИИ, что будет способствовать созданию более точных и эффективных страховых продуктов. Ожидается увеличение доверия к страхованию ИИ-рисков за счет роста числа застрахованных инцидентов и успешных страховых выплат. В результате рынок станет более безопасным и устойчивым для внедрения ИИ», – считает Ищенко.

Пока что рынок находится в зачаточном состоянии – по крайней мере, ВСС не известно о страховых случаях или инцидентах в связи с причинением вреда в результате действий ИИ, говорит представитель союза.

«На сегодняшний день мы не видим широкого спроса конкретно на страхование рисков, связанных с ИИ. Можно ожидать, что вместе с расширением использования технологий ИИ в производственных и хозяйственных процессах компаний будет возникать и спрос на включение данных рисков в страховое покрытие», – согласен Бахшалиев из СОГАЗа.

Рынок страхования ИИ будет развиваться постепенно, по мере оптимизации затрат компаний на разработку ИИ-технологий, которые сейчас в приоритете, считает Логачев из «Альфастрахования». «В ближайшей перспективе очевидно, что финтех не планирует оптимизации подобных расходов, видя в применении ИИ конкурентные преимущества, а в некоторых случаях и суровую необходимость», – говорит эксперт.

Страхование поможет сократить финансовые риски и обеспечить более строгие регуляторные соответствия, повышая прозрачность и безопасность ИИ-систем. «В результате финансовый сектор и страховая отрасль станут более устойчивыми и защищенными от рисков, связанных с внедрением ИИ», – уверен Ищенко. &

FINOPOLIS 2024

ФОРУМ ИННОВАЦИОННЫХ ФИНАНСОВЫХ ТЕХНОЛОГИЙ

ГЛАВНОЕ ФИНТЕХ-СОБЫТИЕ ГОДА

16-18 ОКТЯБРЯ

Федеральная территория «Сириус»

Регистрируйтесь на finopolis.ru