УДК 004.8, 336

ПРИМЕНЕНИЕ НОВЫХ ТЕХНОЛОГИЙ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ БЕЗОПАСНОСТИ ДАННЫХ В КИБЕРПРОСТРАНСТВЕ И В ФИНАНСОВОМ СЕКТОРЕ

Андрей Анатольевич ГОРБАТИКОВ[1], к.э.н.,
Александр Сергеевич МИКУЛЕНКОВ[2],
Сергей Александрович ВАСИЛЬЕВ[3], д.э.н.

[1]Исполнительный директор научно-исследовательского и инжинирингового центра инновационных технологий МФТИ, заместитель директора Бизнес-школы высоких технологий Московского физико-технического института (национального исследовательского университета), г. Долгопрудный

Адрес для корреспонденции: А.А. Горбатиков, 141700, Московская обл., г. Долгопрудный, Институтский пер., д. 9

Т.: +7 (498) 713-91-83. E-mail: gorbatikov.aa@mipt.ru

[2]Директор центра науки и технологий искусственного интеллекта Московского физико-технического института (национального исследовательского университета), г. Долгопрудный

Адрес для корреспонденции: А. С. Микуленков, 141700, Московская обл., г. Долгопрудный, Институтский пер., д. 9

Т.: +7 (498) 713-91-81. E-mail: mikulenkov@gmail.com

[3]Советник ректора,

Автономная некоммерческая организация высшего образования «Международный банковский институт имени Анатолия Собчака», Санкт-Петербург, Россия

Адрес для корреспонденции: 191023, Россия, Санкт-Петербург, Невский пр., д. 60

Аннотация

В статье рассматриваются технологические тренды в финансовом секторе, направления разработки и применения новых технологий искусственного интеллекта. Описано устройство и процесс функционирования нейронной сети. Отмечено несколько трендов, выявленных Gartner, которые влияют на безопасность и конфиденциальность данных в киберпространстве. Выделяются как мировые тенденции технологического развития – защита данных, программное и аппаратное обеспечение, которые будут определять ближайшее будущее глобального экономического развития. Исследуются проблемы безопасности и конфиденциальности данных в киберпространстве. Клиенты финансового сектора ежедневно проводят транзакции через цифровые каналы, и они привыкают к простоте, скорости и персонализированным услугам. Банковский сервис стремится оправдать растущие ожидания клиентов. Приводятся примеры использования искусственного интеллекта в банковском секторе и виртуальном пространстве.

Ключевые слова

Искусственный интеллект, нейросеть, криптовалюта, токенизированная акция, кибербезопасность.

UDC: 004.8, 336

APPLICATION OF NEW AI-BASED TECHNOLOGIES FOR DATA SECURITY IN CYBERSPACE AND THE FINANCIAL SECTOR

Andrey A. GORBATIKOV[1], PhD in Economics

Aleksandr S. MIKULENKOV[2]

Sergey A. VASILIEV[3], Doctor of Economics

[1]Executive Director, the Research and Engineering Center for Innovative Technologies, Moscow Institute of Physics and Technology, Deputy Director, Business School of High Technologies, Moscow Institute of Physics and Technology (National Research University), Dolgoprudny

Address for correspondence: A.A. Gorbatikov, 9 Institutskiy per., Dolgoprudny, Moscow Region, 141701, Russian Federation

T.: +7 (498) 713-91-83. E-mail: gorbatikov.aa@mipt.ru

[2]Director, Center for Science and Technology of Artificial Intelligence, Moscow Institute of Physics and Technology (National Research University), Dolgoprudny

Address for correspondence: A.S. Mikulenkov, 9 Institutskiy per., Dolgoprudny, Moscow Region, 141701, Russian Federation

T.: +7 (498) 713-91-81. E-mail: mikulenkov@gmail.com

[3]Advisor to the rector, Autonomous nonprofit organization of higher education «International

Banking Institute named after Anatoliy Sobchak», Saint-Petersburg, Russia

Address for correspondence: 191023, Russia, St. Petersburg, Nevsky prospect, 60

Abstract

The article discusses technological trends in the financial sector, the development and application of new artificial intelligence technologies. Device and process of neural network functioning are described. Several trends identified by Gartner were noted that affect the security and confidentiality of data in cyberspace. It highlights how global trends in technological development, data protection, software and hardware will shape the near future of global economic development. Security and privacy issues in cyberspace are being investigated. Customers of the financial sector conduct transactions through digital channels daily, and they get used to simplicity, speed and personalized services. The banking service seeks to meet the

growing expectations of customers. Examples of the use of artificial intelligence in the banking sector and virtual space are given.

Keywords

Artificial intelligence, neural network, cryptocurrency, tokenized stock, cybersecurity.

Введение. Искусственный интеллект (ИИ) – сложное программное обеспечение, позволяющее выполнять задачи, похожие на человеческие. ИИ помогает разрабатывать новые способы снижения затрат, увеличения продаж, оптимизации бизнес-процессов и улучшения понимания клиентов. В каждой отрасли существует высокий спрос на его возможности. ИИ – это обширная область исследования, которая включает множество теорий, методов и технологий.

Цель исследования. Обобщить технологические тренды, проблемы безопасности и конфиденциальности данных в киберпространстве и финансовом секторе; рассмотреть примеры использования ИИ в банковском секторе и виртуальном пространстве.

Материалы, методы и объекты исследования. Обобщены современные концепции ИИ, аналитические данные по технологическому развитию, новые технологии на основе ИИ.

Результаты исследования. Современные концепции ИИ называют моделирование процессов человеческого интеллекта компьютерными системами, способными к самообучению при постановке цели человеком. Экспертным сообществом выделяется три вида ИИ: слабый (ANI, Narrow AI), сильный (AGI, Strong AI) и супер-ИИ (ASI, Super AI) [1].

В настоящее время первый вид, ANI, имеет широкое применение и ориентирован на выполнение определённых задач: распознать лицо, речь, осуществлять маркетинг в социальных сетях, найти партнёров в приложениях, поддерживать некоторые надёжные приложения и двигаться в автоколонне автономным транспортным средствам.

AGI – генеративный ИИ, который имеет наиболее равный человеческому интеллект и, по определению Алана Тьюринга, обладает самосознанием. AGI будет способен решать проблемы, учиться и планировать будущее. Предполагается, что на него к 2025 году будет приходиться около 10% всех производимых данных, а сформируется он, по мнению экспертного сообщества, примерно к 2050 году. Оригинальные

данные смогут использоваться в целях создания программ климатического, социального, военного назначения. Примерно через 30 лет после достижения AGI наступит время ASI [2].

ASI должен превзойти интеллект и способности человека во всех областях, иметь возможность перепрограммирования и совершенствования, которые позволят разработать новые системы и алгоритмы самостоятельно. ASI пока носит теоретический характер, но исследования возможностей его развития продолжаются.

В качестве примера того, как устроена и работает нейронная сеть

Нейросеть имитирует работу человеческого мозга и пытается добиться лучших результатов при решении сложных задач, самообучаясь и учитывая предыдущий опыт. Нейросеть – это упрощённое представление биологических нейронных сетей, которое моделируется на компьютерах с последовательным подключением, в то время как в будущем предусмотрена крупномасштабная параллельная реализация. Каждый искусственный нейрон может использоваться и для ввода и для вывода данных, а неполные или недостающие данные аппроксимируются с помощью ряда сохранённых корреляций в матрице памяти. Нейросеть до некоторой степени может компенсировать потерю данных с помощью распределённой памяти. Для определённых задач топология сети может быть сгенерирована случайным образом. Главный недостаток нейросети – невозможность объяснять свои решения.

Нейросеть, подобно биологическим нейронам, имеет многоуровневую структуру. Данная нелинейная система способна адаптироваться, имитируя естественные нейроны. На рисунке 1 показан процесс работы нейросети при распознавании цифры почтового индекса.

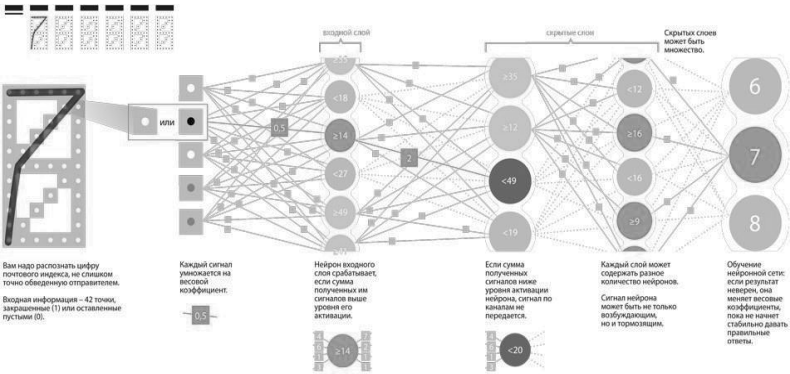

Рисунок 1 – Процесс работы нейросети при распознавании цифры почтового индекса [3]

В октябре 2021 года аналитики консалтинговой компании Gartner представили *топ-12 технологий с применением нейронных сетей*. Каждая из тенденций, отобранных и описанных аналитиками, будет определять технологическое развитие в области ИИ. В данной статье рассматривается несколько трендов, отмеченных Gartner, которые влияют на безопасность и конфиденциальность данных в киберпространстве. Среди таких трендов прежде всего необходимо отметить следующие:

Территориально-распределённые предприятия (Distributed Enterprise) требуют обеспечить защиту и контроль доступа к данным, централизацию и управление общим контентом и кибербезопасностью. Эти усилия не будут напрасны, исследование Gartner показывает, что 75% предприятий, применяющие распределённые предприятия, к 2023 году предполагают опережать своих конкурентов в росте доходов на 25%.

Облачные платформы (Cloud-Native Platforms) позволяют увеличивать доход за счёт снижения затрат на операции инфраструктуры, извлекать выгоду из устойчивости, безопасности, эластичности и масштабируемости. По исследованиям Gartner, применение облачных цифровых услуг возрастёт с 40% в 2021 году до 95% в 2025 году.

Вычисления, укрепляющие конфиденциальность (Privacy-Enhancing Computation, PEC), позволяют извлекать пользу из данных, получать на их основе точные результаты, и при этом способе совместной работы не происходит обмена личными или конфиденциальными данными. По

результатам исследований Gartner, данную технологию к 2025 году будут использовать 60% крупных компаний.

Сеть кибербезопасности (Cybersecurity Mesh) является технологией, создающей безопасный периметр вокруг корпоративной сети и позволяющей экономить затраты на безопасность от её взлома. Архитектура ячеистой сети кибербезопасности (CSMA) защищает активы, где бы они ни находились, гарантирует безопасный доступ ко всем данным, службам и устройствам. Специалисты Gartner к 2025 году прогнозируют уменьшение у компаний, внедряющих CSMA, финансовых последствий инцидентов, связанных с нарушением безопасности, – на 90% [1].

Как видно из данного прогноза, проблема кибербезопасности – защиты данных (личной и конфиденциальной информации), программного и аппаратного обеспечения на основе технологий ИИ (ПАК для ИИ) выделяются как мировые тенденции технологического развития, которые будут определять ближайшее будущее глобального экономического развития.

Исследование проблем безопасности и конфиденциальности данных в киберпространстве

Для широкого круга пользователей Интернет привлекателен прежде всего возможностью свободного общения (в том числе в режиме видеосвязи): в 2019 г. более 63% взрослого населения пользовались социальными сетями, почти 59% совершали телефонные и видеозвонки, более 49% общались в мессенджерах.

Коммерческие организации и государственные учреждения всё больше осведомляются об информации, позволяющей установить личность: о данных населения, номерах паспортов, банковских карт потребителей услуг, товаров. При этом клиенты и покупатели заявляют, что не считают, что 80% компаний делают всё возможное для защиты конфиденциальности данных потребителей. С течением времени этот риск становится ещё более важным, и проблема устранение его становится всё более серьёзной.

Рассматривая технологические тренды в экономике и на финансовых рынках, нельзя не отметить появление криптовалют на финансовом рынке, использование цифрового актива в области инвестиций, торговли. Главное достоинство криптовалюты – это анонимность, имена всех участников зашифрованы. Смарт-контракты помогают совершать транзакции с

криптовалютой без участия центрального органа. Государство не может контролировать данные финансовые потоки, и, как следствие, появляется возможность снизить налоговую базу. При этом сегмент криптовалют продолжает увеличивать количество участников рынка и расширять проникновение в другие сферы экономики и обращения капитала. Криптовалюты и традиционные финансовые рынки начинают проникать друг в друга. На биржах с использованием технологии блокчейн торгуют токенизированными акциями, производными инструментам, стоимость которых определяется базовым активом, акциями.

Инвестиционные банки США приняли криптовалюту в качестве класса активов. JPMorgan готовится предложить некоторым частным клиентам управляемый биткоин-фонд. Goldman Sachs тестирует производные финансовые инструменты, созданные на криптовалютах. В 2021 году Goldman Sachs уже провёл первые крупные миллионные сделки между инвестиционным банками по продаже деривативов, созданных на криптовалютах.

Криптоэкосистема позволяет ранее не охваченным банковскими услугами частям мира осуществлять быстрые и простые платежи. Быстрый темп развития цифровых активов создаёт трудности для регулирующих органов: нужно защищать участников рынка и создавать для них равные условия. Органы власти могут отследить незаконные транзакции, но могут быть не в состоянии идентифицировать стороны таких сделок. Большинство транзакций на криптобиржах происходит через организации, которые работают в оффшорных зонах, поэтому без международного сотрудничества не обойтись. Координацию стран усложняют различающиеся нормативные базы.

Финансовые инструменты в киберпространстве, мобильные технологии онлайн-банкинга могут провоцировать значительные потери денежных средств и убытки для банковского сектора. Как показал 2021 год, *проблема денежных потерь* стала очень актуальной: число краж с использованием интернет-банкинга выросло в два раза по сравнению с 2019 годом, по данным прокуратуры г. Москвы [4].

С начала 2021 года Роскомнадзором также отмечается резкое увеличение случаев кибермошенничества в финансовом секторе, в частности онлайн-банкинге. По данным компании BI.ZONE (входит в экосистему

«Сбера»), в России в 2021 фейковых сайтов кредитных организаций достигло более 15 тыс. Банковский регулятор подчёркивает, что подобные сайты наносят урон не только гражданам, но и репутации банков, по информации «Известий» [5].

Кроме того, к концу 2021 года компания BI.ZONE выявила резкий всплеск мошеннических операций с подставными реквизитами. К октябрю 2021 года число случаев такого рода мошенничества возросло почти до 7 тыс., в октябре было выявлено около 5 тыс. сайтов, в начале года всего 55.

С целью оценки масштабов таких атак, эксперты BI.ZONE также проверили новые регистрируемые домены на предмет подобной аномалии. Более 45 тыс. из них зарегистрированы через специальный хостинг, который принимает оплату в биткоинах. Появление таких доменов было зафиксировано в мае 2020 года, а заметный всплеск и продолжительный рост фиксируется с марта 2021 года. В июне было зарегистрировано более 5 тыс. фишинговых доменов, что в 35 раз больше количества, зафиксированного за аналогичный период в 2020 году [5].

Из международной практики, по информации экспертов BI.ZONE, потери от аналогичных махинаций в США в 2020 году составили $1,8 млрд, по данным ФБР.

Одним из факторов, создающих угрозу безопасности данных, является также то, что всё большая доля корпоративных данных начинает храниться на ноутбуках, смартфонах и других устройствах дистанционно работающих сотрудников. В связи с этим уровень требований, предъявляемых к безопасности корпоративных данных, будет подниматься всё выше и выше.

Проблема разработки новых методов защиты данных и разработки новых решений на основе передовых технологий ИИ приобретает особую *актуальность*. Резкий всплеск мошеннических операций в финансовом секторе в 2021 году создаёт реальную проблему безопасности в виртуальном пространстве. Среди новых возможностей *применения технологий на основе ИИ* для обеспечения конфиденциальности данных и для борьбы с кибермошенничеством можно отметить следующие, это:

- использование методов PEC-вычислений, укрепляющих защиту данных пользователей и обеспечивающих безопасный обмен и анализ данных без ущерба для конфиденциальности;

- создание доверенных систем хранения данных (СХД) и развитие облачных сервисов и сетей кибербезопасности;

- разработка новых алгоритмов ИИ, которые умеют предсказывать вероятность кибератак.

Одним из направлений защиты конфиденциальности данных является применение *облачных сервисов* в корпоративном секторе. Ожидается, что облачные сервисы позволят компании сохранить информацию в нескольких средах, знать, где хранится информация, что с ней происходит, выявлять и устранять угрозы безопасности, вредоносные ПО, регулировать доступ.

В ближайшие пять лет прогнозируется стремительное распространение облачных сервисов и *облачных платформ* крупных операторов, что является мировым трендом. Одной из мировых тенденций развития технологий ИИ является увеличение объёма периферийных вычислений и формирование инфраструктур, реализующих принципы распределённых вычислений. Ожидается, что в перспективе облачным платформам удастся перейти от чисто облачных решений к полноценным бизнес-инструментам на границе облака и автономных устройств, дающих возможность быстро перевести в электронный вид любую информацию компании.

Периферийные микросхемы ИИ (на периферийных умных устройствах), позволяя обрабатывать большие объёмы данных локально, могут снизить риск перехвата или неправомерного использования личных или корпоративных данных. Микросхемы для периферийных вычислений (EdgeAI) также могут распознавать более широкий спектр голосовых команд, выделяя их из общего фона, поэтому в облаке нужно анализировать меньше звука. Более точное распознавание речи может предоставить дополнительное преимущество, помогая умным динамикам более точно определять «пробуждающее слово», предотвращая прослушивание несвязанного разговора.

Доверенные системы хранения данных (СХД) – это системы, построенные на основе аппаратных компонент и программного обеспечения российских производителей. Доверенные СХД представляет новый класс систем хранения данных, объединяющие современные доверенные платформы с интегрированными средствами защиты информации. Одними из эффективных российских разработок на рынке кибербезопасности являются доверенные платформы компании Kraftway.

Противоречивая ситуация складывается вокруг *технологий компьютерного зрения*, широкое распространение которых для видеонаблюдения и распознавания лиц привело к расширению ограничений, связанных с безопасностью и конфиденциальностью данных, распространением приложений для отслеживания контактов. Интеллектуальные камеры видеонаблюдения с обработкой данных на борту, например, могут снизить риски потери конфиденциальности: камеры анализируют видео, чтобы определить, какие сегменты видео являются релевантными, и отправлять в облако только те, которые являются целевыми, аномальными.

Информационной безопасности в киберпространстве в России традиционно уделяется особое внимание, это такие компании, как АО «Лаборатория Касперского» (разработка программных продуктов для сетевой безопасности с нейросетевыми решениями) и InfoWatch (разработка программно-аппаратных комплексов, экранов и фильтров для сетевой безопасности).

Финансовый сектор России переживает революционные изменения в связи с распространением технологий ИИ: круг традиционных банковских операций, связанных с кредитованием клиентов, платёжными сервисами, валютным диллингом, трейдерскими операциями на финансовых рынках, арбитражной торговлей на международных биржах значительно расширился за пределы круга банковских операций.

Банки сталкиваются с усилением конкуренции со стороны необанков и растущей конкуренцией со стороны крупных технологических компаний; с растущими ожиданиями клиентов и цифровыми экосистемами, стремящимися избавиться от посредников в традиционных финансовых услугах. Клиенты проводят растущую долю своих ежедневных транзакций через цифровые каналы, и они привыкают к простоте, скорости и персонализированному обслуживанию, предлагаемому цифровыми компаниями; ожидания клиентов от банковского сервиса растут.

Технологии ИИ могут помочь увеличить доходы банков через повышение персонализации услуг для клиентов и снижение затрат за счёт повышения эффективности посредством снижения затрат на рабочую силу, более точный учёт клиентов и снижение различных рисков. Кредиторы также

могут открыть новые возможности, основанные на улучшенной способности генерировать идеи на основе анализа огромных массивов данных (ML).

По оценкам международной консалтинговой компании McKinsey, внедрение технологий ИИ может потенциально приносить банковскому сектору дополнительную прибыль на сумму до 1 трлн долларов в год [6].

Технологии ИИ уже стали неотъемлемой частью нашего мира. Максимально автоматизируя процесс кредитования, банки могут улучшить качество обслуживания каждого клиента за счёт более быстрого утверждения кредита и выплаты средств, меньшего количества запросов на документацию и кредитных предложений, которые точно соответствуют потребностям клиентов.

Примеры использования ИИ в банковском секторе и виртуальном пространстве

ИИ изменяет все аспекты банковского процесса, ускоряя их, делая безопаснее, а внутренние операции более эффективными. Использование чат-ботов и голосовых помощников становится заметным трендом в клиентском обслуживании многих банков. Сокращается время решения вопросов и количество обращений в службу поддержки клиентов (по статистике АО «Хоум Кредит Банк» 91% не обращается) после общения с ИИ. АО «Тинькофф Банк» использует голосового помощника для перевода денег и покупки акций.

ИИ помогает банкам быстро оценить заявку клиента, исключая человеческий фактор, основываясь только на объективных данных и кредитной истории; построить прогноз поведения по аналогичным случаям, снижается количество ошибок в оценке кредитоспособности клиента.

Сбербанк 100% решений принимает с использованием ИИ, иногда, в 5% случаев, привлекается человек.

Банк ВТБ (ПАО) использует ИИ для определения удобных мест для размещения отделений и банкоматов, внедрил модель машинного обучения, которая анализирует большие данные и прогнозирует спрос на банковские услуги. Благодаря ИИ банк стал выдавать займов на 18% больше, чем раньше.

HSBC использует ИИ для распознавания голоса и идентификации владельца карты в момент звонка по поводу её блокирования.

К 2021 году АО «Тинькофф Банк» расширил применение ИИ в финансовых услугах, на его основе предоставляет индивидуальные консультации, персонализирует интерфейс, автоматизирует повторяющиеся финансовые задачи и интерактивный контент, стимулируя взаимодействие и улучшая качество обслуживания [7].

В то же время виртуализация услуг банков увеличила передачу информации, составляющей коммерческую тайну, и различных элементов персональных данных в интернет-пространстве, которое более уязвимо для кибератак и мошенничества, в том числе с применением технологий ИИ (банковские голосовые ассистенты, распознавание лиц клиентов, идентификация по биометрическим данным) по сравнению с традиционными банковскими технологиями.

Вместе с распространением технологий ИИ мы наблюдаем проникновение банковского бизнеса в такие небанковские сегменты рынка, как розничная торговля, телекоммуникации, социальные сети. В числе основных причин данного явления можно отметить представленные ниже.

Драйвером роста использования ИИ в банковском секторе и одним из примеров проникновения банков в небанковские секторы рынка и отрасли экономики является также новый тренд, задаваемый лидером в банковском секторе России – Сбербанком. На конец 2021 года количество дочерних компаний Сбера превысило 300 компаний, выручка нефинансовых сервисов за 9 месяцев 2021 года составила свыше 121 млрд руб. (рисунок 2).

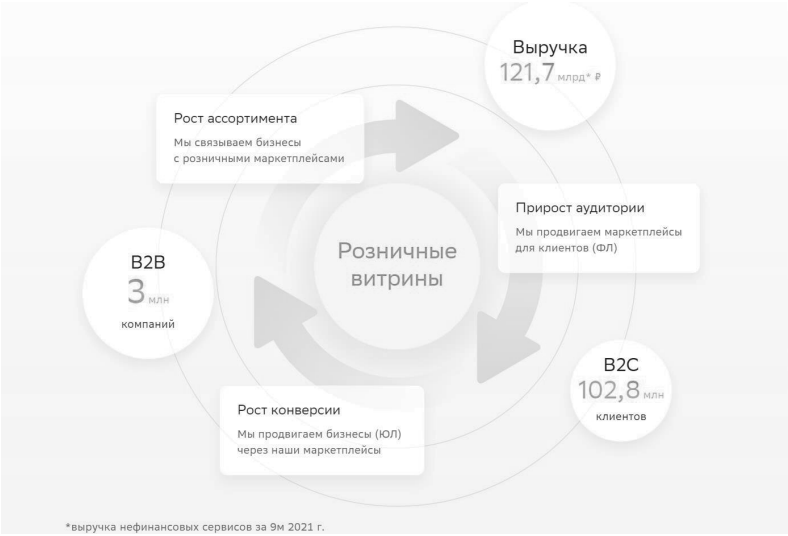

Рисунок 2 – Драйверы роста Сбербанка [8]

Бизнес-стратегия банка сфокусирована на повышении клиентоориентированности. Цифровая экосистема Сбера предполагает создание вокруг человека-клиента очень удобной системы оказания услуг, необходимых для его жизни.

Облачные сервисы *SberCloud* Сбербанк предоставляет с использованием *суперкомпьютера «Кристофари»*, который был создан специалистами Сбербанка и SberCloud, в партнёрстве с компанией NVIDIA в 2019 году специально для работы с алгоритмами ИИ. Суперкомпьютер используется для создания и развития внутренних сервисов *экосистемы*, обучения различных моделей нейросетей с использованием большого объёма данных в короткие сроки.

«Кристофари» – самый мощный суперкомпьютер в России, эффективная производительность составляет 6,7 PFLOPs (согласно тесту LINPACK). Этопозволяет значительно ускорить создание продуктов на основе ИИ. Суперкомпьютер предназначен также для пользователей, работающих в различных отраслях экономики – научно-исследовательском и финансовом секторе, медицине, телекоммуникациях, нефтегазовой, электроэнергетике, тяжёлой промышленности, ритейле, здравоохранении и прочих.

Основные выводы

Рассмотренные технологические тренды развития бизнес-среды и общества по направлению безопасности и конфиденциальности данных в киберпространстве, и прежде всего в финансовом секторе, будут определять направления разработки и применения новых технологий ИИ, аналитики данных и аппаратных решений для ИИ на горизонте 5–10 лет.

Повышение конкуренции внутри банковского сектора вследствие внедрения технологий ИИ, разработка новых банковских продуктов и новых видов услуг с применением ИИ приводит к тому, что банки выходят за стандартный перечень банковских операций и расширяют свой отраслевой ландшафт до розничной электронной торговли, умных устройств, мобильной связи, телекоммуникаций, предоставления облачных сервисов и вычислительных мощностей клиентам для разработки новых продуктов.

Для того чтобы конкурировать и процветать в новом цифровом мире, традиционным банкам необходимо будет уделять первоочередное внимание развитию технологий ИИ в своей стратегии и операциях, создать новое ценностное предложение, основанное на передовых возможностях искусственного интеллекта и аналитики. Банки должны интегрировать ИИ особенно потому, что они сталкиваются с растущей угрозой со стороны крупных технологических компаний в банковском секторе, стремящихся перейти к финансовым услугам (в том числе торговых гигантов Amazon, Alibaba, платёжных платформ Q-platform и других цифровых экосистем).

Список источников

1. Аналитики Gartner отобрали 12 самых перспективных технологий 2022 года. URL: https://trends.rbc.ru/trends/innovation/617122b79a7947a8d7cc0ebf (дата обращения 09.10.2021).

2. На что способен искусственный интеллект сегодня и каков его потенциал. URL: https://trends.rbc.ru/trends/industry/cmrm/619766d59a79471862e77e8a (дата обращения 09.10.2021).

3. Нейросети: как искусственный интеллект помогает в бизнесе и жизни. URL: https://habr.com/ru/post/337870/ (дата обращения 09.10.2021).

4. В Москве в 2020 году в два раза выросло число телефонных и кибермошенничеств. URL: https://tass.ru/obschestvo/10439693 (дата обращения 09.10.2021).

5. С начала года количество лжебанков выросло в 125 раз. URL: https://iz.ru/1261817/2021-12-09/s-nachala-goda-kolichestvo-lzhebankov-vyroslo-v-125-raz (дата обращения 10.10.2021).

6. Отчёт консалтинговой компании McKinsey, отчёт: «Building the AI bank of the future». URL: https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge (дата обращения 10.10.2021).

7. Искусственный интеллект в банках: что это дает клиенту и почему его не нужно бояться. URL: .https://www.banki.ru/news/columnists/?id=10942804 (дата обращения 11.10.2021).

8. Интернет-портал Сбербанка. URL: https://www.sberbank.com/ru/eco (дата обращения 11.10.2021).

References

1. Analitiki Gartner otobrali 12 samyh perspektivnyh tekhnologij 2022 goda. URL: https://trends.rbc.ru/trends/innovation/617122b79a7947a8d7cc0ebf (data obrashcheniya 09.10.2021).

2. Na chto sposoben iskusstvennyj intellekt segodnya i kakov ego potencial. URL: https://trends.rbc.ru/trends/industry/cmrm/619766d59a79471862e77e8a (data obrashcheniya 09.10.2021).

3. Nejroseti: kak iskusstvennyj intellekt pomogaet v biznese i zhizni. URL: https://habr.com/ru/post/337870/ (data obrashcheniya 09.10.2021).

4. V Moskve v 2020 godu v dva raza vyroslo chislo telefonnyh i kibermoshennichestv. URL: https://tass.ru/obschestvo/10439693 (data obrashcheniya 09.10.2021).

5. S nachala goda kolichestvo lzhebankov vyroslo v 125 raz. URL: https://iz.ru/1261817/2021-12-09/s-nachala-goda-kolichestvo-lzhebankov-vyroslo-v-125-raz (data obrashcheniya 10.10.2021).

6. Otchet konsaltingovoj kompanii McKinsey, otchet: «Building the AI bank of the future». URL: https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge (data obrashcheniya 10.10.2021).

7. Iskusstvennyj intellekt v bankah: chto eto daet klientu i pochemu ego ne nuzhno boyat'sya. URL: https://www.banki.ru/news/columnists/?id=10942804 (data obrashcheniya 11.10.2021).

8. Internet portal Sberbanka. URL: https://www.sberbank.com/ru/eco (data obrashcheniya 11.10.2021).