

ная мера. Под общим словом «анонимайзер» как правило понимают сервисы VPN и Proxu. Оба этих сервиса в первую очередь используются для усиления безопасности работы в интернет и создания безопасных соединений между филиалами компаний или их сотрудниками на удаленном режиме работы.

Отвергая предложенные пути решения проблемы хочется обратиться к имеющимся насущным проблемам. Как можно видеть из анализов результатов борьбы государства с фишингом главная проблема состоит в идентификации владельца фишингового ресурса. Данная проблема вызвана полным отсутствием регулирования на государственном уровне как хостинга (англ. hosting) так и выделения доменных имен что порождает возможность анонимного создания страниц противоправного содержания. Стоит отметить, что хостинг, как деятельность по предоставлению технической возможности размещать страницы с общим доступом в сети интернет не трактуется Роскомнадзором как деятельность, требующая лицензирования, поскольку имеющийся Федеральный закон «О связи» предполагает необходимость факта передачи информации, который в понятие хостинг не входит [8].

Так один из крупнейших регистраторов доменных имён в РФ осуществляет свою деятельность на основе договора, в котором прописываются данные достаточные для однозначной идентификации клиента [9]. С другой стороны, на рынке присутствуют организации, которые предоставляют эти услуги на условиях публичной оферты [10]. Аналогичная ситуация наблюдается с хостингом. Очевидно, что имея злонамеренный умысел преступник обратится к услугам фирм, не требующим подписания полноценного контракта и идентификации личности. Учитывая изложенную выше информацию, становится очевидной необходимость модернизации законодательства в части обязывания компаний, предоставляющих услуги хостинга и выделения доменных имен, регистрировать и заключать договора со своими клиентами, только при полной и однозначной идентификации. Можно предположить, что введение таких мер заставит мошенников перейти на зарубежный хостинг. С целью предупреждения обхода ограничения таким образом необходимо ввести запрет для эквайринговых организаций на работу с сайтами, каким-либо образом зарегистрированным или работающим за пределами Российской Федерации. Учитывая санкционную ситуацию на конец 2022 года, в частности недоступности сервиса SWIFT, данная мера не будет избыточной или критически ограничивающей.

В дополнение стоит организовать на базе Роскомнадзора реестр доверительных сайтов с подключенными механизмами удаленной оплаты, содержащий достоверные и полные данные о получателе денежных средств. С дру-

гой стороны, под надзором Минцифры разработать приложения для разных операционных систем ПК и смартфонов, которые позволяли бы проверять наличие открытой на устройстве ссылки или страницы в упомянутом ранее реестре, с указанием информации о получателе платежа или данных пользователя.

#### Список литературы

1. Состояние преступности (январь-октябрь по годам). Министерство Внутренних Дел Российской Федерации. Официальный сайт. [Электронный ресурс]. URL: <https://мвд.рф/folder/101762> (дата обращения: 12.12.2022).
2. Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате». СПС «КонсультантПлюс».
3. Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». СПС «КонсультантПлюс».
4. Киберустойчивость финансового сектора и противодействие кибермошенничеству // офиц. сайт Банка России. [Электронный ресурс]. URL: [https://cbr.ru/about\\_br/publ/results\\_work/2021/obespechenie-ustoychivosti-finansovogo-gyunka](https://cbr.ru/about_br/publ/results_work/2021/obespechenie-ustoychivosti-finansovogo-gyunka) (дата обращения: 12.12.2022).
5. Законопроект № 514780-7 О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма» и иные законодательные акты Российской Федерации (о создании информационной системы проверки сведений об абоненте) // Система обеспечения законодательной деятельности. [Электронный ресурс]. URL: <https://sozd.duma.gov.ru/bill/514780-7> (дата обращения: 12.12.2022).
6. Завьялов А.Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения // Baikal Research Journal. 2022. Т. 13. № 2. DOI 10.17150/2411-6262.2022.13(2).36.
7. Озеров И.Н., Озеров К.И. Проблемы предупреждения мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий // Проблемы правоохранительной деятельности. 2021. № 1. С. 30-34.
8. Разъяснения Роскомнадзора по вопросу лицензирования деятельности провайдеров хостинга. Официальный сайт Роскомнадзора. [Электронный ресурс]. URL: <https://rkn.gov.ru/it/control/p852/> (дата обращения: 12.12.2022).
9. Форма договора для физического лица. RUcenter. [Электронный ресурс]. URL: [https://www.nic.ru/help/forma-dogovora-dlya-fizicheskogo-lica\\_3641.html](https://www.nic.ru/help/forma-dogovora-dlya-fizicheskogo-lica_3641.html) (дата обращения: 12.12.2022).
10. Справочная информация. A100.RU. [Электронный ресурс]. URL: <https://a100.ru/131-2/> (дата обращения: 12.12.2022).

### ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ФИНАНСОВОЙ СФЕРЕ

Голодрыга Л.В.

*ФГБОУ ВО «Финансовый университет  
при Правительстве РФ», Москва,  
e-mail: [www.msluiza.com@mail.ru](mailto:www.msluiza.com@mail.ru)*

Искусственный интеллект это сочетание новых технологий, процессов и методов, имеющих все большее значение для текущего и будущего развития экономики. Искусственный интеллект сегодня применяется в различных отраслях, таких как медицинская диагностика, оптическое

распознавание символов, автономное вождение автомобилей и финансовые услуги. Уже сегодня крупные корпорации, а также малые и средние предприятия в России используют технологии искусственного интеллекта. Искусственный интеллект стал частью повседневной жизни миллионов потребителей. Применение искусственного интеллекта рассматривается как потенциальная движущая сила прорывного технологического развития и инноваций.

Искусственный интеллект это неограниченная скорость эволюции и масштабирование, эффективная работа с большими объемами данных и многозадачность. Традиционно финансовый сектор основан на больших объемах данных, поэтому его автоматизация за счет технологии искусственного интеллекта является новым последовательным и ожидаемым решением.

Искусственный интеллект как современный подход в финансовом секторе имеет множество преимуществ: точные процессы помогают минимизировать человеческий фактор; автоматизация способствует снижению затрат; решение повторяющихся задач становится все более эффективным благодаря подходу «человек в цикле», используемому в гиперавтоматизации. Клиенты, в свою очередь, получают более качественные и персонализированные рекомендации от службы поддержки в режиме реального времени. Технология искусственного интеллекта помогает точно контролировать личные финансы и инвестиции. Чаще всего искусственный интеллект используется для автоматизации поддержки клиентов, исследования и анализа рынков, в алгоритмической торговле и системах обнаружения мошенничества.

Боты сейчас являются наиболее обсуждаемой темой, поскольку, по мнению ИТ-экспертов, боты скоро изменят способ использования устройств [1, с.92]. Некоторые из финансовых ботов помогают пользователям совершать покупки в Интернете, совершать платежи, переводить деньги и даже использовать биткоин-кошелек. Боты-консультанты распространены в банковской сфере. Они могут быстро ответить на простые вопросы, которые могут возникнуть у пользователей. Barclays Africa была одной из первых компаний, которая начала использовать чат-бота для консультирования клиентов. В июле 2016 года российский банк «Точка» запустил финансового бота [6, с.40]. Этот бот помогает клиентам просматривать информацию о своих банковских счетах, находить ближайший банкомат в их местоположении, звонить в службу поддержки и совершать платежи. Финансовые боты – это полезный, удобный и довольно дешевый инструмент. Помимо получения прибыли, ключевой целью каждой фирмы является удовлетворение потребностей своих клиентов.

Боты становятся все более популярными как среди стартапов, так и среди традиционных

финансовых институтов. Автоматизированные консультанты и планировщики помогают пользователям принимать правильные финансовые решения. Например, некоторые роботы отслеживают оценку цен на финансовых рынках, анализируют ее и дают рекомендации по покупке или продаже некоторых ценных бумаг. Такие компании, как ПАО Сбер, ПАО ВТБ, же внедряли технологию искусственного интеллекта в свои сервисы.

Ограниченное управление рисками делает финансовые учреждения, фирмы и домохозяйства более подверженными потрясениям, чем они могли бы быть, и, возможно, является ключевым фактором финансовых кризисов. Искусственный интеллект и машинное обучение могут взять на себя многие бизнес-процессы, требующие работы с большими наборами данных. Применение искусственного интеллекта в финансах и экономике позволит лучше прогнозировать результаты принимаемых решений, намечать различные пути развития и помогать компаниям выбирать наиболее подходящие стратегии для снижения бизнес-рисков.

Предотвращение мошенничества – еще один пример использования искусственного интеллекта в финансах и банковском деле. Чтобы быстрее реагировать на мошенничество и защищать своих клиентов, финансовым компаниям необходимо внедрять инновационные решения в области искусственного интеллекта. Технологии машинного обучения и глубокого обучения доказали свою высокую эффективность как в предотвращении, так и в расследовании незаконной финансовой деятельности.

Уголовный кодекс РФ определяет мошенничество как чужое имущества или приобретения права на чужое имущество путем обмана или злоупотреблением доверия (п. 1 ст. 159 УК РФ).

Специфика финансового мошенничества состоит в той области отношений, в которой совершается обман. Современные финансовые мошенничества: интернет-мошенничество, мошенничество с использованием банковских карт, финансовые пирамиды, мошенничество на рынке недвижимости.

Такие алгоритмы основаны на контролируемом обучении, типе подхода к обучению модели, который включает в себя проверку результатов человеком. Решения на основе ML могут работать с оповещениями, тщательно изучать большие наборы данных или выполнять анализ подозрительных транзакций в кратчайшие сроки и с высокой точностью.

Искусственный интеллект как современный подход также используется в цифровых кошельках. Они изучают привычки и потребности пользователей и консультируют их о том, как управлять своими личными финансами. Такие приложения, как Digit, Mint, WealRo и Cleo, работают в этой области. Например, мобильный

банк в Гонконге Neat (запущен весной 2016 года) сочетает в себе технологию искусственного интеллекта и биометрическую безопасность [7, с. 87]. В РФ у ПАО ВТБ есть чат-бот на самой платформе банка. У ПАО Сбер есть СберБизнесБот и SaluteBot.

ПАО Сбер и ВТБ применяют искусственный интеллект к платежным данным пользователей, создавая различные поведенческие кластеры в сочетании с геолокацией, чтобы предлагать пользователям персонализированные и локальные предложения.

Все больше и больше компаний обращаются к ИИ для автоматизации различных задач, таких как бухгалтерский учет, аудит и финансовая отчетность. Этот сдвиг в сторону автоматизации во многом обусловлен растущей доступностью данных и достижениями в области алгоритмов машинного обучения.

Автоматизированные системы могут обрабатывать большие объемы данных гораздо быстрее и точнее, чем люди, что приводит к повышению эффективности и точности процесса учета.

Оптическое распознавание символов (OCR) – популярный тип разработки проектов искусственного интеллекта [1, с. 90]. Эта уникальная технология широко используется банками для извлечения большого объема информации. С помощью OCR банки могут обрабатывать, отслеживать и оценивать огромные объемы данных, будь то внутренняя отчетность, информация о клиентах или информация о безопасности.

Некоторые азиатские банки, такие как DBS, Axis Bank и ICICI Bank, используют OCR для инновационного взаимодействия с клиентами. Благодаря автоматическому распознаванию данных клиента оптическое распознавание символов обеспечивает быстрый и соответствующий требованиям процесс верификации клиента.

Искусственный интеллект поддерживает решения для биометрической идентификации и распознавания, такие как распознавание лиц, голоса и отпечатков пальцев. Алгоритмы распознавания лиц проверяют личность, извлекая черты лица из изображений или видео и сравнивая их с лицами, доступными в наборах данных. Затем технология усиливает безопасность искусственного интеллекта и может быть использована для обеспечения необходимого уровня безопасности как для онлайн-сервисов, так и внутри офисов.

Например, идентификаторы лиц широко распространены среди таких банков, как HSBC, Chase, Citibank, Bank of America и Wells Fargo [2, с. 65]. Эти финансовые учреждения уже разработали приложения для онлайн-банкинга с распознаванием лиц. У нас в России такая система применяется в ПАО Сбер (с 17 октября 2022 г.), ГУП Мосметрострой (с октября 2021 г.) и МЦД (с 16 марта 2022 г.). Порядок сбора биометрии регулируются: ФЗ РФ № 152 «О персональ-

ных данных» и ФЗ РФ № 149 «Об информации, информационных технологиях и о защите информации». В статье 11 ФЗ РФ № 152 указано, что сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных. Согласно статьи 14.1 ФЗ РФ № 149 обработка, включая сбор и хранение, параметров биометрических персональных данных для идентификации реализуется с применением информационных технологий и технических средств, имеющих подтверждение соответствия требованиям. В соответствии со ст. 152. 1 ГК РФ обнаружение и дальнейшее использование изображения человека возможно только с его согласия.

Президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам протоколом от 24.12.2018 г. № 16 был утвержден паспорт национальной программы «Цифровая экономика в РФ» и с 1 января 2018 г. сбор биофизических параметров своих клиентов начали крупные банковские организации для идентификации клиентов по голосу и видео.

Вступление в силу ФЗ РФ № 479 от 29.12.2020 г. установило использование ЕБС для удаленной идентификации при получении широкого спектра финансовых и государственных услуг.

Технология машинного обучения (ML) также позволяет машинам распознавать голоса на основе таких характеристик, как артикуляция, высота тона и так далее. Системы распознавания голоса создают и хранят уникальный «голосовой отпечаток». Затем финансовые компании с искусственным интеллектом могут внедрить голосовой отпечаток вместо пароля или вместе с ним, чтобы сделать процесс авторизации пользователя безопасным и плавным. В феврале 2019 года HSBC впервые внедрил распознавание голоса в услуги, предоставляемые своим клиентам.

В сфере финансовых услуг технология искусственного интеллекта позволит компаниям создавать новые бизнес-модели, снижать риски и затраты, а также повышать производительность. Это также могло бы позволить как крупным, так и малым фирмам предлагать финансовые услуги на уровне сложности, индивидуализации и масштаба, который ранее был невозможен.

Сегодня искусственный интеллект в финансах является конкурентным активом, который обеспечивает контекстуализированные финансовые предложения, тем самым увеличивая прямую и косвенную прибыль банков и кредитных союзов. В ближайшие годы автоматизация про-

ложит новые пути в отрасли и станет стандартом для персонализированных финансовых услуг.

#### Список литературы

1. Бердышев А.В. Искусственный интеллект как технологическая основа развития банков // Вестник университета. 2018. № 5. С. 91-94.
2. Искусственный интеллект в банковском секторе // Эксперт РА. 2018.
3. Искусственный интеллект и бизнес: есть контакт? // ВЦИОМ. 2019.
4. Матвеевский С.С., Бердышев А.В. Fintech-компании и их взаимодействие с банками: международный и российский опыт // Вестник университета. 2020. № 11. С. 174-180.
5. Туркина Д.Е. Три ключевые проблемы внедрения искусственного интеллекта в российских банках на современном этапе развития экономики // Инновации и инвестиции. 2018. № 12. С. 335-336.
6. Agarwal A., Singhal Ch., Thomas R. AI-powered decision making for the bank of the future. McKinsey & Company. 2021. March.
7. Accenture Hessens. Ambitionen für Künstliche Intelligenz, Ein Beitrag zur nationalen KI-Strategie am Beispiel des Finanzsektors. 2018. Available online at: [https://wirtschaft.hessen.de/sites/default/files/media/hmwv1/20180925\\_ki\\_studie\\_hessen\\_report\\_final\\_im\\_auftrag\\_von\\_0.pdf](https://wirtschaft.hessen.de/sites/default/files/media/hmwv1/20180925_ki_studie_hessen_report_final_im_auftrag_von_0.pdf).
7. Accenture Hessens. Ambitionen für Künstliche Intelligenz, Ein Beitrag zur nationalen KI-Strategie am Beispiel des Finanzsektors. 2018.
8. Weg ohne Ziel? Wie Deutschland ein Spitzenstandort für Künstliche Intelligenz werden kann. 2018.

### ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ БЛОКЧЕЙН ТЕХНОЛОГИИ

Емжуева О.В.

*Финансовый университет при Правительстве РФ,  
Москва, e-mail: olesya200162@gmail.com*

Сегодня не вызывает сомнений, что развитие всех сфер жизни общества неразрывно связано с цифровизацией. В результате внедрения технологий предполагается создание условий, которые повысят конкурентоспособность нашей страны на мировой арене, а также качество жизни внутри страны.

Несмотря на то, что взят активный курс на цифровизацию, не все области способны быстро перестроиться под требования современности. Поскольку право является достаточно консервативной средой, на данный момент законодательство не в полной мере может охватить все технологические новинки. Так, до сих пор не введено легальное определение блокчейн-технологии. В общем виде блокчейн-технология – это выстроенная по определенной системе «цепочка блоков» или база данных, в которой хранится информация обо всех произведенных транзакциях. В основе данной технологии лежат криптографические алгоритмы. Блокчейн своему названию обязан способу хранения данных в блоках, которые образуют взаимосвязанную цепочку. С каждой новой транзакцией новый блок добавляется в конце общей цепи, записывает и подтверждает время и последовательность транзакций [1, С.13]. Особенность заключается в том, что в каждом блоке есть свой уникальный идентификатор,

информация о недавних транзакциях и «цифровой след» предыдущего блока. Таким образом блоки оказываются связаны друг с другом, а любое вмешательство становится заметным. В результате невозможно незаметно добавить какой-либо блок между существующими или изменить их содержимое. Такая система позволяет избежать взлома блокчейна и наделяет его характеристикой неизменности.

Попытка сформировать подобное понятие была предпринята в Федеральном законе «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», который был принят только в 2020 году. В данном законе было введено определение распределенного реестра, под которым понимается совокупность баз данных, тождественность содержащейся информации в которых обеспечивается на основе установленных алгоритмов [2]. Несмотря на наличие этого положения, в законе прямо не говорится, что под таким распределенным реестром можно понимать блокчейн-технологии, более того, делается оговорка, что данное понятие принято для целей этого федерального закона. Предполагается, что таким образом законодатель решил пойти по пути «аккуратного» регулирования сложных технологий, потенциал которых раскрыт еще не в полной мере. Сегодня также при использовании технологии распределенного реестра, например, в финансовой сфере, применяются общие нормы законодательства, в том числе, нормы о защите прав потребителей и идентификации клиентов.

Чаще всего блокчейн используется для хранения цифровой информации, обмена цифровыми активами, для автоматического исполнения смарт-контрактов и так далее. В России существует ряд стратегических государственных программ, главной задачей которых является активное внедрение технологий в бизнес-процессы. В рамках реализации Стратегии развития информационного общества в Российской Федерации 2017–2030 г. была разработана программа «Цифровая экономика». В соответствии с данной программой блокчейн является одной из ключевых технологий, способствующих развитию технологической независимости нашей страны. Например, начиная с 2016 года в России активно действует блокчейн-сеть «Мастерчейн», использующая отечественные криптографические инструменты. Так, в конце 2020 года ПАО «ВТБ» и ПАО «МТС» стали первыми компаниями, которые провели сделку по оформлению цифровой банковской гарантии на основе «Мастерчейна».

При рассмотрении вопросов применения блокчейн-технологии с точки зрения права необходимо понять, какие общественные отношения складываются в процессе ее использования. Выделяют несколько групп общественных отно-