DOI dx.doi.org/10.24866/VVSU/2073-3984/2019-4/062-073

УДК 5341.171

Э.В. Горян

Владивостокский государственный университет экономики и сервиса
Владивосток. Россия

Зарубежный опыт использования технологий искусственного интеллекта в обеспечении информационной безопасности банковского сектора

Объектом исследования являются отношения, возникающие при обеспечении информационной безопасности в банковском секторе с использованием технологий искусственного интеллекта. Рассматриваются текущее состояние развития технологий искусственного интеллекта в России и опыт их применения за рубежом.
В исследовании были использованы общие (системно-структурный, формально-логический и герменевтический методы) и специальные юридические методы научного познания (сравнительно-правовой и формально-юридический методы).
Существующие программные решения с использованием искусственного интеллекта, применяемые для обеспечения информационной безопасности банковского сектора, относительно примитивны и высокозатратны. Эти факторы замедляют широкое применение технологий. Дополнительными факторами, усложняющими выполнение функций безопасности, выступают злонамеренное манипулирование данными со стороны злоумышленников, а также взаимосвязанность систем, подключенных к искусственному интеллекту. В итоге технологии искусственного интеллекта не могут работать автономно, поскольку к процессам вынуждены подключаться специалисты, обладающие навыками анализа, присущими человеческому сознанию. Вопросы, которые требуют регламентации, касаются определения вида и пределов ответственности в случае аутсорсинга процессов и услуг, а также оценки и управления рисками. Неоднозначность решения указанных проблем затрудняет расширение сферы применения искусственного интеллекта в банковском секторе.

Ключевые слова и словосочетания: искусственный интеллект (ИИ), технологии, информационная безопасность, критическая информационная инфраструктура, программное обеспечение, банковский сектор, финансовый сектор.

Горян Элла Владимировна – канд. юрид. наук, доцент кафедры гражданско-правовых дисциплин, доцент; e-mail: ella.goryan@vvsu.ru

E.V. Gorian

Vladivostok State University of Economics and Service
Vladivostok. Russia

Foreign experience in the use of artificial intelligence technologies in ensuring information security of the banking sector

The object of the study is the issue of providing the information security by means of artificial intelligence technologies. The current situation of development of AI technologies in Russia and cases of their application in foreign countries are considered.

The study used general (system-structural, formal-logical and hermeneutic methods) and special legal methods of scientific knowledge (comparative legal and formal-legal methods).

Existing software solutions which use the artificial intelligence for information security providing in the banking sector, are relatively primitive and costly. These factors slow down the widespread use of technology. Additional factors that complicate the performance of security functions are malicious data manipulation by attackers, as well as the interconnectedness of systems connected to AI within the banking system. As a result, AI technologies cannot work autonomously, since specialists with human analysis skills are in need to interfere the processes. Issues that require legal regulation are the determination of the type and extent of responsibility in the case of outsourcing of processes and services, as well as issues of risk assessment and management. The ambiguity in solving thlts of the pattern safety estimation for traffic in the Tsugaru Strait and the Tokyo Bay are given.

Keywords: artificial intelligence, technology, information security, critical information infrastructure, software, banking sector, financial sector.

Актуальность темы исследования. Технологии искусственного интеллекта (далее – ИИ-технологии) приобретают все большую популярность в банковском и финансовом секторах. Как отмечают аналитики Business Insider Intelligence, около 80% банковских учреждений с активами более 100 млрд долларов США и чуть менее половины банков с активами менее 100 млрд долларов США в настоящее время реализуют проекты с применением ИИ. Результаты прогнозируются впечатляющие: в течение ближайших трех лет отрасль существенно сэкономит 447 млрд долларов США, причем только во фронт-офисе (работа с клиентами) и мидл-офисе (противодействие мошенничеству с платежами) ожидается показатель сэкономленных средств на уровне в 416 млрд долларов США [20]. В России лидерство в использовании ИИ-технологий принадлежит Сбербанку России: на основании решений, принимаемых искусственным интеллектом, выдается 100% кредитных карт, более 90% потребительских кредитов и свыше 50% ипотечных кредитов, а к 2020 году ИИ-технологии будут ответственны за принятие около 100% кредитных решений [10]. Следует отметить, что с 18 июля 2019 года мобильное приложение Сбербанка функционирует на основе ИИ-технологий [9]. Ежегодные всероссийские конференции участников банковского и

финансового секторов свидетельствуют о растущем интересе к ИИ-технологиям. Последние три года активно обсуждаются такие вопросы, как технологии вывода на рынок нового потребительского финансового продукта; технологии удаленной верификации клиентов и защиты от мошенничества; монетизация новой парадигмы отношений с клиентами; технологии работы с клиентами на бирже; цифровизация финансовых услуг; препятствия при переходе банков на цифровое обслуживание; влияние финансовой грамотности на продажи компании [13]; недоверие акционеров банков технологиям FinTech (несмотря на то, что уже более 50% российских банков активно инвестируют в FinTech-стартапы) [11]; нехватка решений в b2b-сегменте; кибербезопасность и новые возможности в регуляторной области; применение искусственного интеллекта в fintech-компаниях [22]. Использование ИИ-технологий в сфере розничных банковских услуг становится стандартным технологическим процессом, на очереди – инвестиционный банкинг. Такие впечатляющие результаты не должны снижать внимание к ИИ-технологиям: поскольку они представляют собой вид информационных технологий, то закономерно возникает вопрос об их безопасности. Кроме того, банковский и финансовый секторы относятся к критической информационной инфраструктуре, что определяет их в качестве одной из приоритетных целей в случае кибератак. Поэтому вопрос соотношения ИИ-технологий и обеспечения информационной безопасности является актуальным и существенным для формирования устойчивого и эффективного механизма кибербезопасности.

Постановка проблемы исследования. ИИ-технологии используются в системе мидл-офиса (для защиты объектов критической информационной инфраструктуры банковского и финансового секторов), но в то же время они могут быть использованы в инструментах кибератак (например, вредоносных программ – malware). Банковские учреждения могут использовать ИИ-технологии как при самостоятельной разработке систем информационной безопасности, так и прибегать к уже готовым решениям, предлагаемым частным сектором. Трудности в использовании ИИ-технологий заключаются как в технологическом аспекте (повышение скорости реагирования и ликвидации источника и последствия таких атак), так и в организационно-правовом.

Цели и задачи исследования. Цель исследования – охарактеризовать тенденции использования искусственного интеллекта для обеспечения кибербезопасности в банковском секторе зарубежных стран. Для достижения поставленной цели определены задачи исследования, заключающиеся в характеристике аспектов применения ИИ-технологий при обеспечении кибербезопасности в банковском секторе зарубежных стран и определении возможности применения положительного опыта в России.

Методология. В данном исследовании будут использованы общие (системно-структурный, формально-логический и герменевтический методы) и специальные юридические методы научного познания (сравнительно-правовой и формально-юридический).

Источниковая база исследования. Выбранная нами для исследования тема мало представлена в российской научной литературе. В большинстве своем встречаются экономические исследования, в частности, речь идет о необходимости расширения сферы использования искусственного интеллекта при разработке стратегии развития банка [4, с. 193]; подчеркивается ведущая роль финансового регулятора в регулировании процессов распространения технологий искусственного интеллекта и роботизации [3, с. 252]; проводится анализ случаев успешного внедрения искусственного интеллекта и машинного обучения в различных банках России и разработаны предложения по возможному использованию систем и платформ в банковском секторе [8, с. 479].

В ряде научных исследований ученых Сингапура и КНР рассматриваются организационно-правовые и технические особенности обеспечения информационной безопасности финансово-банковских систем в аспекте децентрализованного подхода (каждого субъекта отдельно от всей системы) [15; 28], однако в случае аутсорсинга процессов уязвимость банковской системы становится решающим фактором, определяющим необходимость централизованной разработки стандартов аутсорсинга, в том числе в случае использования так называемых облачных технологий. Некоторые исследователи Сингапура обращают внимание только на техническую сторону проблемы [17; 25], оставляя вне поля зрения организационно-правовую ее часть. Важную роль в обеспечении кибербезопасности играет система управления рисками, позволяющая распределить все имеющиеся ресурсы в зависимости от того или иного сценария негативного воздействия на операционные системы финансово-банковских учреждений [23; 29]. Разработанные финансовыми регуляторами КНР, Сингапура и Таиланда нормативные положения по вышеперечисленным вопросам гарантируют относительную устойчивость критической информационной инфраструктуры банковского и финансового секторов.

Основная часть. Наиболее известным определением искусственного интеллекта считается дефиниция Джона Маккарти (John McCarthy), заведующего лабораторией искусственного интеллекта Университета Стенфорда, согласно которой ИИ – наука и техника создания интеллектуальных машин [26]. ИИ также может быть определен как «когнитивные технологии», применяемые в машинном обучении, включая глубокое обучение и прогнозную аналитику, обработку естественного языка (NLP), включая перевод, классификацию, кластеризацию и извлечение информации [14]. На ИИ возлагаются большие надежды в разных сферах человеческой деятельности. Несмотря на широко обсуждаемые в научной и публицистической литературе потенциальные последствия такого широкого вовлечения ИИ, существует необходимость легальной дефиниции ИИ, определения его места в правоотношениях, а также решения большого круга вопросов юридического характера. Речь идет о «слабом» ИИ (weak artificial intelligence), противоположностью которого является так называемый «сильный» ИИ (strong artificial intelligence) – искусственный общий интеллект (artificial general intelligence), который соответствует человеческому интеллекту или превосходит его, определяется как способность «рассуждать, представлять

знания, планировать, учиться, общаться на естественном языке и интегрировать все эти навыки для достижения общей цели» [14]. Новейшие современные разработки представляют собой «слабый» ИИ, способный упрощать и ускорять выполнение определенных информационно-технологических процессов, – технологии искусственного интеллекта (далее – ИИ-технологии). Несмотря на ограничения, накладываемые современным уровнем развития техники, вычислительные мощности растут в геометрической прогрессии (согласно закону Мура вычислительная мощность процессора будет увеличиваться в геометрической прогрессии в 2 раза каждые 18–24 месяца), и уже через десять лет человечество будет обладать вычислительными мощностями, в двести раз превышающими современные, что, в свою очередь, приведет к соответствующему росту возможностей систем ИИ [14]. Представители многих отраслей экономики пытаются использовать существующие ИИ-технологии для оптимизации и качественного развития процессов, в результате чего как в краткосрочной, так и в долгосрочной перспективе рынок будет поделен между теми участниками, которые сделали ставку на внедрение ИИ-технологий.

Перед обзором зарубежного опыта использования ИИ-технологий в банковском секторе в аспекте информационной безопасности рассмотрим текущее положение дел в инновационной сфере в Российской Федерации.

В России развитие технологий ИИ получило свое нормативное обоснование в 2016 году в рамках реализации программы Национальной технологической инициативы (далее – НТИ) [6], обозначенной еще в 2014 году главой государства одним из приоритетов национальной политики [7]. По направлению «Искусственный интеллект» на базе ФГАОУ ВО «Московский физико-технический институт (государственный университет)» был создан Центр НТИ, охватывающий в своем консорциуме более 20 научных и образовательных учреждений, партнеров из индустрии и малых инновационных компаний, среди которых банковскую сферу представляет ПАО Сбербанк. Центр НТИ осуществляет комплексное развитие сквозной технологии «Искусственный интеллект». Для банковской сферы это выразится в получении принципиально новых технологий биометрической идентификации пользователей с помощью анализа и интеллектуальной обработки рефлекторных реакций человека – разработке технологии и сервиса для удаленной биометрической идентификации на основе рефлекторных реакций человека на возбуждающие стимулы, рассчитанных на недоверенность клиентского устройства (например, смартфона), для верификации ответственных транзакций при оказании банковских и государственных услуг [12].

Уже в 2019 году развитие ИИ стало осуществляться в рамках отдельной национальной стратегии [5], закрепившей принципы развития и использования технологий ИИ и установившей цели и основные задачи развития искусственного интеллекта. Данный документ интересен прежде всего тем, что закрепил легальное определение ИИ и технологий ИИ. Под первым понятием понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты,

сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений (п. 5(а)) [5]. ИИ-технологии основаны на использовании ИИ, включая компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы ИИ (п. 5(б)) [5]. Следует отметить такую особенность определения ИИ-технологий через открытый перечень процессов, в которых ИИ может быть задействован (после перечисления наиболее перспективных на сегодняшний день законодатель использовал формулировку «перспективные методы» ИИ, что оставляет возможности включения и других технологий, которые могут появиться в будущем с учетом вышеуказанного закона Мура).

Среди задач развития ИИ следует отметить две, тесно связанные с безопасностью (в том числе банковского и финансового секторов): разработка и развитие программного обеспечения, в котором используются ИИ-технологии (п. 24(б)) [5], и создание комплексной системы регулирования общественных отношений, возникающих в связи с развитием и использованием ИИ-технологий (п. 24(е)) [5]. В качестве средства решения указанных задач определено формирование комплексной системы безопасности при создании, развитии, внедрении и использовании ИИ-технологий (п. 25(е)) [5]. Такая система должна включать специально разработанные единые стандарты в области безопасности (в том числе отказоустойчивости) и совместимости программного обеспечения, эталонных архитектур вычислительных систем и программного обеспечения, а также конкретно определенные критерии сопоставления программного обеспечения и критерии эталонных открытых тестовых сред (условий) в целях определения качества и эффективности программного обеспечения (п. 34(г)) [5]. Нормативно-правовая основа для регулирования указанных процессов должна функционировать к 2024 году и предусматривать гарантии доступа к данным и установления процедур упрощенного тестирования и внедрения технологических решений, устранение административных барьеров внешнеторговой деятельности, создание единых систем стандартизации и оценки соответствия технологических решений, гарантии инвестиционной деятельности и этические правила взаимодействия человека с ИИ (п. 49) [5].

По мнению специалистов, банковский сектор России является лидером по внедрению инновационных технологий по сравнению с европейскими странами [11]. Объяснение этому лежит в плоскости деятельности финансового регулятора Российской Федерации – Банка России, регламентирующего деятельность инфраструктурных проектов (цифровая идентификация, система быстрых платежей) и вопросы кибербезопасности [2; 11]. Следует отметить также готовность банковских учреждений привлекать готовые FinTech-решения извне (так называемый аутсорсинг услуг), что может способствовать инвестиционной активности в секторе.

Перейдем теперь к рассмотрению зарубежного опыта. Лидером в реализации ИИ-технологий в банковском и финансовом секторе выступают США и

КНР, где привлекаются крупные инвестиции для развития ИИ-проектов. В Европейском Союзе ситуация с массовым применением ИИ усложнена в связи со вступлением в силу Общего регламента по защите данных (General Data Protection Regulation, далее – GDPR) в 2018 году. Этот документ содержит ряд положений, препятствующих автоматизации процессов принятия решений (причем не только в банковско-финансовой сфере, но и во всех других сферах экономики и управления). Так, статья 22 GDPR гарантирует право субъекта данных не подвергаться решению, основанному исключительно на автоматизированной обработке, включая профайлинг. Как раз это положение и препятствует инструментам ИИ принимать автоматические решения. Для снятия этого ограничения необходимо участие персонифицированного субъекта для принятия окончательного решения, предлагаемого ИИ-инструментами. Еще одно положение GDPR (статья 13) содержит клаузулу о «раскрытии»: лицо имеет право быть ознакомленным с мотивацией принятия того или иного решения (так называемая «логика решения», например: при отклонении заявки на кредит лицо должно быть уведомлено о причинах такого решения. Однако особенностью ИИ-инструментов как раз и является непредсказуемость и непрозрачность (black box) принятых решений). Поэтому для выполнения положений статьи 13 необходимо вовлечение программистов в осуществление процессов ИИ, что затрудняет ожидаемое повышение их эффективности [24].

Тем не менее, на сегодняшний день ИИ активно используется в технологиях, обеспечивающих кибербезопасность банковского сектора и охватывающих следующие направления: борьба с отмыванием денег и мошенничеством; агрегирование данных безопасности; мониторинг киберугроз и предотвращение кибератак. Следует отметить, что все продукты, включающие ИИ-технологии, разработаны представителями частного сектора – компаниями профиля FinTech. Как указывалось ранее в наших исследованиях, обеспечение кибербезопасности невозможно без тесного сотрудничества субъектов частного и публичного сектора [1], а нижеследующее подтверждает этот тезис. Рассмотрим успешные технологии подробнее.

Борьба с отмыванием денег и мошенничеством. Компания Feedzai предлагает программное обеспечение для обработки данных OpenMLEngine, способное обнаружить и предотвратить отмывание денег и мошенничество [21]. Эта программа позволяет специалистам банковских служб безопасности создавать собственные модели обнаружения мошенничества с использованием уже существующих в программном обеспечении паттернов моделей. Платформа Feedzai обычно интегрируется в системы банка или продавца услуг и предупреждает аналитиков рисков только о тех случаях мошенничества, которые действительно считаются высокорисковыми (основанными на заранее определенных факторах), тем самым ускоряя процессы обнаружения мошенничества и уменьшая количество ложных срабатываний.

На сегодняшний день это программное обеспечение работает в 10 крупнейших банках США. Такая система оценки рисков отклоняет новые заявки на счета и принимает клиентов только с низкой вероятностью совершения мошенни-

чества. Платформа была развернута в ядре существующих корпоративных систем банка с использованием собственных дата-центров банка, что позволило программе стать центральным механизмом принятия решений в процессе регистрации клиентов в Интернете и проверки личности, проверки соответствия требованиям и оценки риска мошенничества в режиме реального времени. В тех случаях, когда у программного обеспечения не было достаточно данных для принятия решения при подаче онлайн-заявки, оно автоматически генерировало дополнительные вопросы, специфичные для клиента, заранее сформулированные группой по адаптации банка.

Система обеспечивает направление заявок высокого риска экспертам по безопасности на ручную проверку, а факторы риска понятны для облегчения принятия решений с целью сокращения времени, затрачиваемого экспертами по безопасности при рассмотрении каждого случая. В результате количество утвержденных заявок увеличилось на 70%, а время, затрачиваемое на ручную проверку, сократилось. Несмотря на прирост пользователей банковских услуг, количество мошеннических действий сократилось [16].

Агрегирование данных безопасности. Компания DefenseStorm создает программное обеспечение для автоматизации процессов кибербезопасности с помощью машинного обучения [19]: PatternScout и ThreatMatch осуществляют мониторинг внутренних систем в режиме реального времени на предмет поиска аномальных процессов. Программные инструменты помогают банку обнаружить и идентифицировать угрозы кибербезопасности в своей сети, что позволяет сэкономить на долгосрочных затратах на безопасность и избежать утечек данных. Используя распознавание образов на основе машинного обучения на исторических сетевых данных, платформа может поддерживать деятельность по обеспечению безопасности и эксплуатации в масштабах всей компании. Такие SaaS-решения способны помочь банковскому персоналу по информационной безопасности получить доступ к данным, связанным с событиями безопасности, в одном месте через единую панель управления. Сотрудники могут войти в панель управления и быстро среагировать на угрозы безопасности, выявленные программным обеспечением.

Например, в случае банка LiveOak компания DefenseStorm помогла решить проблему объединения расположенных на всей территории США центров обработки данных, использующих различные технологии и приложения для поддержки своих платформ для кредитования малого бизнеса и депозитов. В результате сотрудники информационной безопасности банка смогли использовать аналитическое решение SaaS для обновления существующих систем управления данными и аналитики LiveOakBank. После интеграции LiveOakBank смог оптимизировать поиск больших данных, в результате обнаружение киберинцидентов улучшилось на 50–60%: если раньше сотрудники затрачивали на обнаружение и определение процесса как киберугрозы 15–60 минут, то после интеграции платформы это время сократилось до 1–5 минут [16].

Мониторинг киберугроз и предотвращение кибератак. Компания Darktrace разработала программное обеспечение EnterpriseImmuneSystem, использующее

машинное обучение для обнаружения киберугроз и реагирования на них в таких цифровых средах, как облако, виртуальные сети, IoT (интернет вещей) и промышленные системы управления [18]. Один из инструментов программного обеспечения EnterpriseImmuneSystem – DarktraceThreatVisualizer, представляющий собой панель управления, которая может использоваться банковским персоналом по информационной безопасности для мониторинга киберугроз в режиме реального времени. На сегодняшний день пользователями программного продукта являются более 40 компаний из различных сфер экономики [16].

Компания PatternEx предлагает программное обеспечение на основе ИИ, позволяющее выявлять опасные намерения пользователя и прогнозировать и предотвращать кибератаки [27]. Платформа VirtualAnalyst анализирует данные (например, IP-адреса, пользователей или сеансы) миллионов пользователей и обнаруживает подозрительные действия (транзакции с IP-адресов, используемых для совершения мошеннических действий). Шаблоны, составленные платформой, оцениваются аналитиками по информационной безопасности, которые подтверждают, какие события являются фактическими атаками, а какие – ложными срабатываниями. Затем система использует выводы аналитиков в своих моделях для следующего сбора данных для анализа.

Исследователи подчеркивают, что на настоящий момент наиболее массовыми и успешными в применении являются инструменты с ИИ-технологиями, направленные на обнаружение мошенничества и борьбу с отмыванием денег, а в ближайшие 3–5 лет на рынок выйдут программные продукты для банковских и финансовых учреждений, решающие проблему обнаружения угроз мошенничества в реальном времени [16].

Выводы. Несмотря на уже существующие программные решения с ИИ для обеспечения кибербезопасности банков, следует отметить их относительную примитивность и высокую затратность. Только крупные банки и финансовые учреждения располагают достаточным бюджетом и персоналом для использования ИИ-технологий, в то время как качество качество выполненных программами заданий еще далеко от идеального. Следующий момент касается уязвимости ИИ перед злонамеренным манипулированием данными (создание фиктивных данных, массовое увеличение данных, замедляющее процессы обработки). В результате инструменты ИИ будут принимать решения, основанные на ложных посылках, и дискредитировать (вплоть до дискриминации) определенных субъектов. Еще одной проблемой может стать взаимосвязанность систем, подключенных к ИИ, а также использование ИИ во вредоносных программах, поражающих информационные системы банков. В итоге решение всех названных проблем лежит в плоскости осуществления постоянного наблюдения специалистов. Как видно из вышесказанного, обеспечение кибербезопасности в условиях внедрения ИИ зависит от ряда условий как технического, так и организационно-правового характера. Наряду с проблемами защиты прав и законных интересов субъектов банковских и финансовых отношений возникают проблемы определения вида и пределов ответственности в случае аутсорсинга некоторых процессов и услуг, а также вопросы оценки и управления рисками. Все эти вопросы,

возникающие в зарубежных странах, еще не находят однозначного решения, что затрудняет расширение сферы применения искусственного интеллекта в банковском секторе.

1. Горян Э.В. Институциональные механизмы обеспечения безопасности критической информационной инфраструктуры Российской Федерации и Сингапура: сравнительно-правовой аспект // Административное и муниципальное право. 2018. № 9. С. 49–60.
2. Горян Э.В. Роль финансового регулятора в обеспечении кибербезопасности в России и Сингапуре: сравнительно-правовой аспект // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2019. Т. 11, № 2. С. 83–101.
3. Ломакин Н.И., Киселева С.Р., Самородова И.А. Финансовые технологии и искусственный интеллект банковского сектора в новой финансово-технологической экосистеме будущего // Будущее науки-2017: сб. науч. статей / отв. ред. А.А. Горохов. – М., 2017. С. 250–253.
4. Максимова К.Ю., Харламова Е.Е., Ломакин Н.И. К вопросу о совершенствовании стратегии управления финансами организации // Молодежь и системная модернизация страны: сб. науч. статей / отв. ред. А.А. Горохов. – М., 2018. С. 190–194.
5. О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): указ Президента Российской Федерации от 10 октября 2019 г. №490 [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/ cons_doc_LAW_335184/
6. О реализации Национальной технологической инициативы (вместе с «Правилами разработки и реализации планов мероприятий («дорожных карт») Национальной технологической инициативы», «Положением о разработке, отборе, реализации и мониторинге проектов в целях реализации планов мероприятий («дорожных карт») Национальной технологической инициативы», «Правилами предоставления субсидий из федерального бюджета на реализацию проектов в целях реализации планов мероприятий («дорожных карт») Национальной технологической инициативы»): Постановление Правительства РФ от 18.04.2016 №317 (ред. от 31.08.2019) [Электронный ресурс] // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/ cons_doc_LAW_196930/
7. Послание Президента Федеральному Собранию 4 декабря 2014 года [Электронный ресурс] // Президент России: официальный сайт. URL: http://kremlin.ru/ events/president/news/47173
8. Пушечкин А.Д. Возможности использования искусственного интеллекта и машинного обучения в банковской сфере РФ // Цифровая экономика и Индустрия 4.0: тенденции 2025: сб. тр. науч.-практ. конференции / под ред. А.В. Бабкина, 2019. С. 479–483.
9. Сбербанк внедрил искусственный интеллект в мобильное приложение [Электронный ресурс] // РБК. URL: https://www.rbc.ru/finances/18/07/2019/5d2f3a809a79470f1a2399f6
10. Сбербанк доверит искусственному интеллекту 100% решений о выдаче кредитов населению [Электронный ресурс] // АО «КоммерсантЪ». URL: https://www.kommersant.ru/doc/4080855
11. Сюткина В. Банки открылись FinTech-стартапам [Электронный ресурс] // ComNews. URL: http://www.comnews.ru/content/202326/2019-10-14/2019-w42/banki-otkrylis-fintech-startapam
12. Центр компетенций НТИ по направлению «Искусственный интеллект» [Электронный ресурс] // Национальная технологическая инициатива: официальный сайт. URL: http://nti2035.ru/technology/competence_centers/mipt.php

13. Чумак Л. Как прошла конференция FinTech Russia 2018 [Электронный ресурс] // RusBase. URL: https://rb.ru/story/ftr2018/
14. AI in Law: Definition, Current Limitations and Future Potential // LegalTechBlog. URL: https://legal-tech-blog.de/ai-in-law-definition-current-limitations-and-future-potential
15. Baluta T., Ramapantulu L., Teo Y.M., Chang E.-C. Modeling the effects of insider threats on cybersecurity of complex systems // Proceedings – Winter Simulation Conference, 2018. P. 4360–4371.
16. Bharadwaj R. AI for Cybersecurity in Finance – Current Applications. URL: https://emerj.com/ai-sector-overviews/ai-cybersecurity-finance-current-applications/
17. Challa S., Das A.K., Gope P., Kumar N., Wu F., Vasilakos A.V. Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems // Future Generation Computer Systems, 2018.
18. Darktrace. URL: https://www.darktrace.com/en/
19. DefenceStorm // DefenceStorm. – URL: https://www.defensestorm.com/
20. Digalaki E. The $450B opportunity for the applications of artificial intelligence in the banking sector & examples of how banks are using AI. URL: https://www.businessinsider.com/the-ai-in-banking-report-2019-6
21. Feedzai: Fraud Prevention with Machine Learning. URL: https://feedzai.com/
22. FinTech в России и мире: тренды, инфраструктура, участники рынка [Электронный ресурс] // РИФ+КИБ/2017. URL: http://2017.russianinternetforum.ru/news/1288/
23. Jin Z., Liu G., Yang H. Optimal consumption and investment strategies with liquidity risk and lifetime uncertainty for Markov regime-switching jump diffusion models // European Journal of Operational Research, 2019.
24. Kaya O. Artificial intelligence in banking // Deutsche Bank Research, June 04, 2019. URL: https://www.dbresearch.com/PROD/RPS_EN-PROD/ PROD0000000000495172/ Artificial_intelligence_in_banking%3A_A_lever_for_pr.pdf
25, Li Z. CKshare: secured cloud-based knowledge-sharing blockchain for injection mold redesign X. Liu, W.M. Wang, A.Vatankhah Barenji, G.Q. Huang // Enterprise Information Systems. 2019. №13 (1). P. 1–33.
26. McCarthy J. What is artificial intelligence? Basic Questions // Stanford University. URL: http://www-formal.stanford.edu/jmc/whatisai/node1.html
27. PatternEx. URL: https://www.patternex.com
28. Ter K.L. Singapore's cybersecurity strategy // Computer Law and Security Review. 2018. №34 (4). P. 924-927.
29. Zhang P., He Y., Chow K.-P. Fraud track on secure electronic check system // International Journal of Digital Crime and Forensics. 2018. №10 (2). P. 137–144.

Транслитерация

1. Goryan E.V. Institucional'nye mekhanizmy obespecheniya bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i Singapura: sravnitel'no-pravovoj aspekt // Administrativnoe i municipal'noe pravo. 2018. № 9. P. 49–60.
2. Goryan E.V. Rol' finansovogo regulyatora v obespechenii kiberbezopasnosti v Rossii i Singapure: sravnitel'no-pravovoj aspekt // Territoriya novyh vozmozhnostej. Vestnik Vladivostokskogo gosudarstvennogo universiteta ekonomiki i servisa. 2019. T. 11. № 2. P. 83–101.
3. Lomakin N.I., Kiseleva S.R., Samorodova I.A. Finansovye tekhnologii i iskusstvennyj intellekt bankovskogo sektora v novoj finansovo-tekhnologicheskoj ekosisteme budushchego // Budushchee nauki-2017: sb. nauch. statej / otv. red. A.A. Gorohov. M., 2017. P. 250–253.

4. Maksimova K.Yu., Harlamova E.E., Lomakin N.I. K voprosu o sovershenstvovanii strategii upravleniya finansami organizacii, // Molodezh' i sistemnaya modernizaciya strany: sb. nauch. statej / otv. red. A.A. Gorohov. – M., 2018. P. 190–194.
5. O razvitii iskusstvennogo intellekta v Rossijskoj Federacii (vmeste s «Nacional'noj strategiej razvitiya iskusstvennogo intellekta na period do 2030 goda»): Ukaz Prezidenta Rossijskoj Federacii ot 10 oktyabrya 2019 g. №490 [Elektronnyj resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_LAW_335184/
6. O realizacii Nacional'noj tekhnologicheskoj iniciativy (vmeste s «Pravilami razrabotki i realizacii planov meropriyatij («dorozhnyh kart») Nacional'noj tekhnologicheskoj iniciativy», «Polozheniem o razrabotke, otbore, realizacii i monitoringe proektov v celyah realizacii planov meropriyatij («dorozhnyh kart») Nacional'noj tekhnologicheskoj iniciativy», «Pravilami predostavleniya subsidij iz federal'nogo byudzheta na realizaciyu proektov v celyah realizacii planov meropriyatij («dorozhnyh kart») Nacional'noj tekhnologicheskoj iniciativy»): Postanovlenie Pravitel'stva RF ot 18.04.2016 №317 (red. ot 31.08.2019) [Elektronnyj resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_ LAW_196930/
7. Poslanie Prezidenta Federal'nomu Sobraniyu 4 dekabrya 2014 goda [Elektronnyj resurs] // Prezident Rossii: oficial'nyj sajt. URL: http://kremlin.ru/events/president/news/47173
8. Pushechkin A.D. Vozmozhnosti ispol'zovaniya iskusstvennogo intellekta i mashinnogo obucheniya v bankovskoj sfere RF // Cifrovaya ekonomika i Industriya 4.0: tendencii 2025: sb. tr. nauch.-prakt. konferencii / pod red. A.V. Babkina. 2019. P. 479–483.
9. Sberbank vnedril iskusstvennyj intellekt v mobil'noe prilozhenie [Elektronnyj resurs] // RBK. URL: https://www.rbc.ru/finances/18/07/2019/5d2f3a809a79470f1a2399f6
10. Sberbank doverit iskusstvennomu intellektu 100% reshenij o vydache kreditov naseleniyu [Elektronnyj resurs] // AO «Kommersant"». URL: https://www.kommersant.ru/doc/4080855
11. Syutkina V. Banki otkrylis' FinTech-startapam [Elektronnyj resurs] / V. Syutkina // ComNews. URL: http://www.comnews.ru/content/202326/2019-10-14/2019-w42/banki-otkrylis-fintech-startapam
12. Centr kompetencij NTI po napravleniyu «Iskusstvennyj intellekt» [Elektronnyj resurs] // Nacional'naya tekhnologicheskaya iniciativa: oficial'nyj sajt. URL: http://nti2035.ru/technology/competence_centers/mipt.php
13. Chumak L. Kak proshla konferenciya FinTech Russia 2018 [Elektronnyj resurs] // RusBase. URL: https://rb.ru/story/ftr2018/

Для цитирования: Горян Э.В. Зарубежный опыт использования технологий искусственного интеллекта в обеспечении информационной безопасности банковского сектора // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2019. Т. 11, № 4. С. 62–73.

For citation: Gorian E.V. Foreign experience in the use of artificial intelligence technologies in ensuring information security of the banking sector, *The Territory of New Opportunities. The Herald of Vladivostok State University of Economics and Service*, 2019, Vol. 11, № 4, pp. 62–73.

DOI dx.doi.org/10.24866/VVSU/2073-3984/2019-4/062-073

Дата поступления: 05.11.2019.