

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ И СЕРВИСА
ИНСТИТУТ МЕЖДУНАРОДНОГО БИЗНЕСА,
ЭКОНОМИКИ И УПРАВЛЕНИЯ
КАФЕДРА ЭКОНОМИКИ И УПРАВЛЕНИЯ

ОМ

ОТЧЕТ

по учебной практике по получению навыков
исследовательской работы
ФГБОУ ВО «ВГУЭС», ИМБЭУ,
кафедра экономики и управления, г. Владивосток

Студент
группы БЭУ-21-1

Андрей А.Ю. Крыщенко

Руководитель практики от кафедры:
канд. экон. наук, доцент

Мария М.Н. Арнаут

Нормоконтролер
канд. экон. наук, доцент

Мария М.Н. Арнаут

Владивосток 2022

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ И СЕРВИСА
ИНСТИТУТ МЕЖДУНАРОДНОГО БИЗНЕСА,
ЭКОНОМИКИ И УПРАВЛЕНИЯ
КАФЕДРА ЭКОНОМИКИ И УПРАВЛЕНИЯ

**ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА
УЧЕБНУЮ ПРАКТИКУ ПО ПОЛУЧЕНИЮ НАВЫКОВ
ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ**

Студент: Крыщенко А.Ю.

Группа: БЭУ-21-1

Срок сдачи: согласно приказа

Содержание задания на практику:

Введение: определить цель и задачи практики, основные методы, необходимые для их достижения **Раздел 1.** Характеристика исследуемой проблемы: искусственный интеллект в банковском секторе.

Краткое содержание исследуемой проблемы и ее актуальность, степень разработанности исследуемой проблемы (перечень авторов, внесших вклад в решение проблемы; отражение проблемы в государственных нормативных документах и т.п.); цель и задачи исследования (УК-1.1в, УК-1.3в). **Раздел 2.** Современное состояние исследуемой проблемы. Сущность исследуемой проблемы в авторском изложении с иллюстрацией статистическим и аналитическим материалом, перспективы дальнейших исследований по данной теме (УК-1.1в).

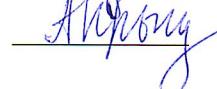
Заключение. Обобщения и выводы. Список использованных источников (включаются источники не старше 2017 года).

Руководитель учебной практики
канд. экон. наук, доцент



Арнаут М.Н.

Задание получил:



Крыщенко А.Ю.

РАБОЧИЙ ГРАФИК (ПЛАН)

Студент Крыщенко Анастасия Юрьевна
Фамилия Имя Отчество

Кафедра Экономики и управления гр. БЭУ-21-1

Руководитель практики Арнаут Марина Николаевна
Фамилия Имя Отчество

Инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности прошел

А
 ФИО уполномоченного лица
(подпись уполномоченного лица, МП)

С правилами трудового распорядка ознакомлен Аннаут
(подпись обучающегося)

Этапы практики	Виды работы	Срок выполнения	Отметка руководителя о выполнении
1. Подготовительный	Организационное собрание	Участие в организационном собрании; получение индивидуального задания в соответствии с выбранной темой исследования; прохождение инструктажа по технике безопасности; встреча с сотрудниками РИАЦ	<u>А</u>
	Инструктаж по технике безопасности		<u>А</u>
2. Исследовательский	Формулировка целей и задач исследования	Анализ содержания исследуемой проблемы, степени ее актуальности и разработанности; формулировка цели исследования; формулировка задач исследования; разработка плана исследования	<u>А</u>
3. Аналитический	Подбор и анализ информации по теме исследования	Определение списка источников, необходимых для решения поставленных задач; сбор, систематизация и анализ информации; формулировка выводов; определение возможных направлений дальнейших исследований по выбранной теме	<u>А</u>
4. Заключительный	Подготовка и защита отчета по практике	Подготовка, оформление и защита отчета по практике	<u>А</u>

Руководитель учебной практики
 канд. экон. наук, доцент

Арнаут М.Н.

Содержание

Введение	3
1 Аспекты изучения работы с искусственным интеллектом	4
2 Искусственный интеллект в банковском секторе	5
Заключение	12
Список использованных источников	13

Введение

Цели научно-исследовательской практики: совершенствование профессиональных знаний в выбранной сфере; овладение необходимыми профессиональными компетенциями по написанию научных статей, в том числе выбирать необходимые методы исследования, модифицировать существующие, обрабатывать полученные результаты, анализировать и осмысливать их с учётом имеющихся литературных данных.

Задачи научно-исследовательской практики: овладение научным методом познания и на его основе углубленное и творческое освоение учебного материала; овладение методикой и средствами самостоятельного решения научных и технических задач; приобретение навыков работы в научных коллективах и ознакомление с методами организации научной работы.

В современном мире человек сталкивается со множеством экономических проблем, в связи с эти люди часто прибегают к решению проблем при помощи сомнительных способов заработка, что часто только усугубляют положение, так как оказывается мошенничеством. Примерно 40 лет назад, люди стали задумываться об искусственном интеллекте, сегодня технологиям искусственного интеллекта удалось продвинуться далеко вперед, а их применение стало обоснованной необходимостью в различных сферах экономики.

Не исключением стал и банковский сектор, который, с помощью внедрения синтетических технологий, стремится обеспечить наивысшее качество и скорость обслуживания своих клиентов, повысить скорость проведения ряда банковских операций, а также облегчить доступ к ряду банковских операций.

Аспекты изучения работы с искусственным интеллектом

На сегодняшний день наука подошла к решению большей части финансовых проблем человека в современном мире. В данный момент на базе множества банков разрабатывается все больше программ, которые по мышлению не уступают человеку. Они будут призваны облегчить каждому человеку взаимодействие с финансами, но из этого проистекает несколько актуальных проблем.

1 Проблема незнания: многие люди даже не представляют, как часто они сталкиваются с искусственным интеллектом. Многие из систем искусственного интеллекта могут значительно упростить жизнь.

2 Проблема безопасности и сверхинтеллекта: сможет ли общество использовать для расширения своего знания познавательные модели сверхумного искусственного интеллекта – этот вопрос остается открытым.

Цель исследования: изучить понятие искусственного интеллекта в банковской сфере, познакомиться с технологией программирования систем искусственного интеллекта для работы в банке, а также с методами их использования пользователем.

Методы исследования: научно-теоретические (анализ, синтез теории по данному вопросу, индукция и дедукция).

Продуктом исследования является модель: "взаимодействие человека с искусственным интеллектом в банковской сфере".

Задачи исследования:

- 1) рассмотреть, что такое искусственный интеллект и понять способы его работы в банках;
- 2) проанализировать виды искусственного интеллекта, использующегося в современной банковской отрасли;
- 3) выработать свое понимание эффективного взаимодействия человека с искусственным интеллектом в банковской сфере.

Гипотеза исследования: благодаря выбору правильного алгоритма взаимодействия человека с искусственным интеллектом возможно существенное сокращение проблем с его использованием в банковской сфере.

Искусственный интеллект в банковском секторе

В научной среде современный искусственный интеллект понимается как наука и технология, основанная на таких дисциплинах, как информатика, психология, биология, лингвистика, математика, машиностроение, робототехника, программирование.

Автором термина «искусственный интеллект» является Джон Маккарти, изобретатель языка Лисп, основоположник функционального программирования и лауреат премии Тьюринга за огромный вклад в области исследований искусственного интеллекта и сознания человека. Можно выделить три направления развития искусственного интеллекта на современном этапе.

1 Решение проблем, связанных с освоением специализированных систем ИИ и их интеграция в экономическую сферу.

2 Приведение искусственного интеллекта к уровню самостоятельного анализа мирового рынка, а также предоставление ИИ возможности выработки вариантов предложения решений поставленной проблемы.

3 Создание искусственного разума, представляющего интеграцию уже созданных систем искусственного интеллекта в единую систему, способную автономно решать финансовые проблемы, вплоть до мирового кризиса.

Искусственный интеллект уже нашел свое место в российских банках, что существенно расширило их возможности. Например, в приложении «Биометрия» от «Ростелекома» для iOS возможно открытие накопительного счета в «Почта банке». Более широкий перечень – в личном кабинете на портале госуслуг: помимо продуктов «Почта банка» предлагается кредитная карта Совкомбанка, накопительный счет и кредит от Промсвязьбанка, кредит на покупку товара в интернет-магазинах от «Хоум кредит» [1]. В «Тинькофф Банке» компьютерное зрение с точностью в 90% распознаёт документы. Эту технологию также используют, чтобы идентифицировать лица клиентов. Благодаря такому решению удалось в шесть раз сократить случаи мошенничества с поддельными документами.

В настоящее время банки используют искусственный интеллект для

решения ряда задач оперативного получения отчетности, выполнения рутинной работы бэк-офиса, оценки кредитоспособности заемщика, недопущения проведения сомнительных операций, мошенничества и отмывания денег, а также для персонализации предлагаемых клиентам банковских продуктов. Так компьютерные программы предоставляют возможности преобразования банковской деятельности по следующим основным направлениям: общение с клиентами, замена рутинных операций, обработка документов, риск-менеджмент. Рассмотрим данные возможности подробнее.

Общение с клиентами. Наиболее заметные изменения отмечаются в этом направлении, что объясняется, во-первых, обострением борьбы за клиентуру (привлечение новых клиентов и удержание в своей орбите старых) и, во-вторых, готовыми технологиями, которые могут осуществлять эту функцию более эффективно и с меньшими издержками, чем оператор. В последние годы ИИ, созданный по образу оператора человека, в процессе общения с клиентом строго придерживается «скрипта» (сценария диалога), отклоняться от которого не имеет полномочий. Как только диалог перестает вписываться в рамки утвержденного сценария, оператор, используя клишированную фразу, переводит разговор на человека, работающего с индивидуальными случаями. Идея разработки чат-ботов привлекает банки тем, что обеспечивает постоянный доступ к банку с моментальной реакцией на обращение, а это, естественно, важно для клиента.

В настоящее время работам поручают с определенной периодичностью связываться с клиентом, предлагать новые продукты и услуги, информируя об их преимуществах, напоминать о необходимости совершить те или иные клиентские операции и многое другое.

Второе важное направление в общении с клиентом – это персонализация продукта и услуги. Персонализация выступает в качестве конкурентного оружия банков. Прежние критерии конкурентоспособности – «цена» банковского продукта, скорость предоставления, доступность – в значительной мере отходят на второй план, в том числе потому, что современные технологии уравнивают возможности конкурентов, не оставляя места для ощутимого превосходства.

Острота соперничества за внимание потребителя переходит на технологический уровень, с акцентом на способность создать адаптированный к потребностям конкретного клиента продукт, разработать убедительные рекомендации (вплоть до готовых решений) с учетом особенностей его характера и стиля мышления и довести их до его сведения.

Замена рутинных операций и оптимизация процессов. Парадоксально, но это тот случай, когда вмешательство человека может скорее помешать, чем помочь. Для повторяющихся действий (например расчетов), где не требуется принятие решений, искусственный интеллект подходит как нельзя лучше, как считает партнер Santander InnoVentures П.Бовье, представляющий подразделение, которое занимается проблемами финтеха и искусственного интеллекта. «На таких участках все определено, не требуются никакие экстравагантные и малопонятные программы, существует полная правовая прозрачность – это путь к оптимизации, автоматизации. Умной автоматизации, робототехнике. Замечательный шанс для банков снизить издержки» [2].

Обработка документов. Передовые технологии с одинаковым успехом справляются как с обработкой, так и с составлением документации. Современные сканирующие программы могут распознавать стандартные документы и передавать их исполнителям. Естественно, такие программы содержат специальные фильтры, которые направляют документы, не укладывающиеся в заданные характеристики, на рассмотрение эксперта. Более того, современные системы позволяют распознавать типовые документы и давать на них типовые же ответы. А это уже серьезный аргумент для использования таких программ в юридическом отделе банка.

Финансовые учреждения нашли применение искусственного интеллекта и в системе управления персоналом. Интеллектуальные технологии контролируют решения сотрудников, оперативно реагируя на неправомерные действия с их стороны, тем самым предупреждая нарушение законодательных норм по вине банка, а также в общем составляют статистику работников, позволяя увеличить продуктивность на местах.

Риск-менеджмент. В среднем, только 20% проектов внедрения цифровых технологий нацелено на снижение издержек или повышение производительности. Большинство направлено на распознавание потенциальных рисков и минимизацию их последствий. Искусственный интеллект может идентифицировать схемы, применяемые злоумышленниками, причем не только стереотипные. Обрабатывая большие базы данных, ИИ способен найти, например, признаки мошенничества или попытки отмывания денег, полученных нелегальным путем, как внутри системы, так и снаружи.

Самый простой, но не теряющий значимости вариант – выявление схем или преступных личностей. Искусственный интеллект способен охватить обширные базы данных и уловить схемы, которые ускользают от внимания человека. В этом его огромное преимущество. В результате продвинутые технологии в этой области позволяют определять людей и компании с повышенными для банка рисками и соответствующим образом выстраивать дальнейшие отношения с ними.

Так, например, один из крупнейших банков в мире HSBC Holdings plc. использует искусственный интеллект в автоматизации процессов пресечения отмывания средств, шведский коммерческий банк Nordea Bank AB применяет виртуальных сотрудников в области обработки информационных процессов, банки The Royal Bank of Scotland Plc, Bank of America и др. пользуются услугами чатботов, которые обрабатывают административные задачи, дают советы по управлению, информируют об угрозах сотрудников отдела экономической безопасности банка [4].

Однако вместе с несомненным удобством от применения искусственного интеллекта возникают и проблемы – это необходимость повышения осведомленности об алгоритмах работы искусственного интеллекта и налаживание безопасности при использовании искусственного интеллекта в банковском секторе.

На этот счет статистика, на основе данных глобальной сети, включающей более 34 тыс. сайтов и приложений, показывает, что в 2021 году уровень атак на мошенничество с платежами в сфере финтеха резко вырос на 70%, что является самым высоким показателем среди всех секторов сети. Рост мошенничества с

платежами также коррелирует с массивным 121%-ным ростом объемов транзакций в сфере финтех в сети Sift по сравнению с 2020 годом, что делает этот сектор привлекательной целью для киберпреступников.

Эти растущие атаки были направлены в первую очередь на альтернативные платежи, такие как цифровые кошельки, где наблюдался 200%-ный рост мошенничества с платежами, а также на поставщиков платежных услуг (+169%) и криптовалютные биржи (+140%) [5].

Компания Group-IB оценила ущерб для клиентов российских банков от мошеннической схемы с использованием подложных платежных систем в 3,15 млрд. руб. Сообщение компании об этом поступило в РБК. «Круг пострадавших в этой схеме достаточно широк — это и клиенты банков, потерявшіе свои деньги, и банки-эмитенты, одобравшие транзакцию, онлайн-сервисы или магазины, сайт которых подделали злоумышленники, и платежные системы, чьи бренды нелегально и без их ведома используются в мошеннической схеме», — пояснили специалисты [6].

Анализируя данные о самых популярных способах мошенничества, видим, что главной проблемой в данном секторе является неосведомленность людей о схемах работы искусственного интеллекта, как следствие – разглашение данных третьим лицам. И возраст не всегда играет ключевую роль, ведь согласно данных рисунка 2.2.

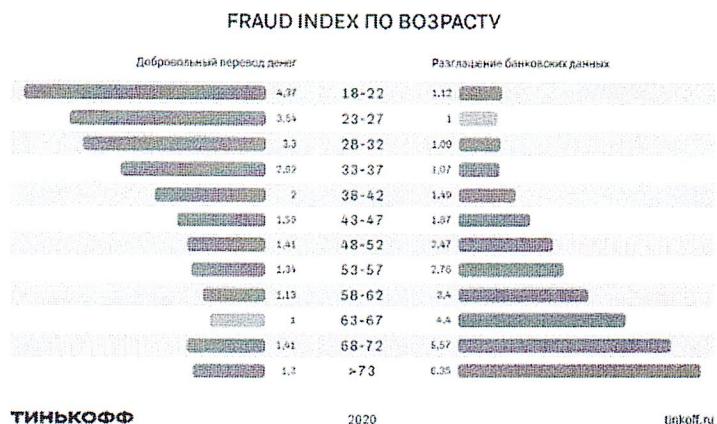


Рисунок 2.2 – Fraud index по возрасту [3]

Риск безопасности скорее зависит от вида мошенничества, чем от возраста пострадавшего. Можно также заметить, что с каждым годом растет процент самостоятельных переводов, возглавляя список популярных видов мошенничества, что видно по рисунку 2.3.

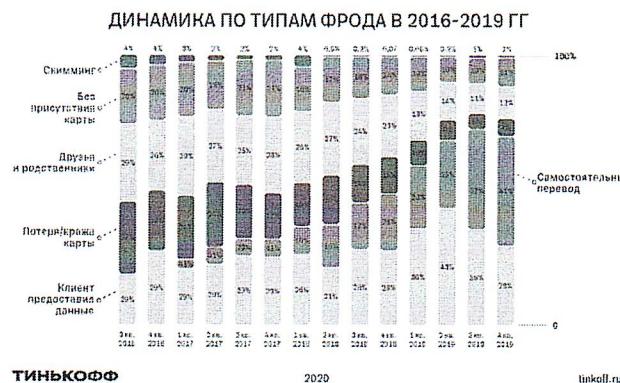


Рисунок 2.3 – Динамика роста по типам фрода [3]

Самый распространенный способ мошенничества - социальная инженерия. Применяя этот способ, мошенники уговаривают жертву либо выдать данные карты или пароль из смс, либо перевести деньги. Такие случаи составляют 70% от всех преступлений.

На втором месте — «френдли-фрода»: деньги с карты или банковского приложения на смартфоне тратит друг или родственник человека. Это 12% всех преступлений.

На третьем - операции без присутствия карты. Речь идет о взломах личных кабинетов сервисов, где надо привязывать карту: такси, доставки еды, интернет-магазины и т.д. Мошенники, завладев данными банковской карты, оформляют дорогостоящие заказы. На такие случаи приходится 11% мошенничеств.

Самый непопулярный способ мошенничества - скимминг. Речь здесь идет о случаях, когда мошенники воруют данные карты с помощью специальных считывающих устройств, которые устанавливают на банкоматы и магазинные терминалы. На скимминг приходится 1% всех мошенничеств.

Скимминг постепенно становится редкостью: большинство карт имеют чипы бесконтактной оплаты, а считывающие устройства мошенников позволяют

подделывать только магнитную полосу карты. Поэтому если мошенники делают копию карты и платят потом ей в другом месте, то платят не бесконтактно, а магнитной полосой. В этих случаях деньги почти всегда возвращают клиенту [7].

Решить проблемы финансового мошенничества в банковской сфере непросто. Для этого необходимо повышать общий уровень осведомленности и грамотности населения в области искусственного интеллекта и обеспечивать максимальный уровень безопасности данных клиентов банка.

Бессспорно, введение всех доступных механизмов сразу может стать дорогоим и малоэффективным из-за несогласованности разных способов и систем борьбы с мошенничеством. Предлагаем модель для возможного решения обозначенных проблем. Начать, в любом случае, стоит с просвещения: дополнительное образование и курсы, введение учебной дисциплины в школах и вузах, направленной на освоение работы алгоритмов искусственного интеллекта. Это поможет как выпускну более профессиональных кадров, так и повышению уровня грамотности населения при работе с искусственным интеллектом.

Если же говорить о мерах обеспечения безопасности самих банковских организаций, то предлагаем следующие меры: налаживание межбанковских связей в системе кибербезопасности, так как в настоящее время многие люди являются клиентами сразу нескольких банков; повсеместное введение фрод-мониторинга и биометрической защиты данных.

Заключение

Исследование, развитие и последующее внедрение искусственного интеллекта в банковский сектор – основа формирования эффективных алгоритмов работы и обеспечения безопасности и сохранности данных. Искусственный интеллект занимает ключевую роль в борьбе с мошенничеством в банковском секторе на современном этапе. Он позволяет своевременно обнаруживать вмешательство в работу банка, попытки похитить данные клиентов банка или их денежные средства и оперативно бороться с ним.

С развитием технологий совершенствуются и мошеннические механизмы и схемы; устаревают такие способы с использованием специального оборудования, алгоритм сводится лишь к хищению данных на расстоянии – контакт становится необязательным, а похитить данные проще и быстрее. И только улучшение механизмов работы ИИ, повышение общего уровня знаний алгоритмов работы с искусственным интеллектом способно дать ощутимые результаты в борьбе с мошенничеством в секторе банковского дела. А повсеместное внедрение ИИ поможет более качественно и быстро выполнять банковские операции и взаимодействовать с клиентами.

Список использованных источников

- 1 Открытие банковского счета при помощи биометрии – настоящий квест: [сайт]. – 2020. – URL: https://www.vedomosti.ru/personal_finance/articles/2020/05/04/829556-otkritie-bankovskogo-scheta-pri-pomoschi-biometrii (дата обращения 10.04.22).
- 2 Искусственный интеллект в операционной деятельности банка будущего [сайт]. – 2020. – URL: http://gashevsn.narod.ru/Intell.htm_ (дата обращения 12.04.22).
- 3 Пульс - социальная сеть для инвесторов и трейдеров: [сайт]. – 2020. – URL: <https://feedback.tinkoff.ru/pulse> (дата обращения 16.04.22).
- 4 Sennaar K. AI in Banking – An Analysis of America’s 7 Top Banks: [сайт]. – 2022. – URL: <https://www.techemergence.com/ai-inbanking-analysis> (дата обращения 19.04.22).
- 5 Мошенничество в финтех-сервисах в мире взлетело на 70%: [сайт]. – 2022. – URL: <https://www.iksmedia.ru/news/5879488-Moshennichestvo-v-fintexservisax.html> (дата обращения 21.04.22).
- 6 Group-IB оценила ущерб клиентов банков от новой мошеннической схемы — РБК: [сайт]. – 2021. – URL: <https://www.rbc.ru/finances> (дата обращения 26.04.22).
- 7 Как мошенники снимают деньги с карт: данные статистики: [сайт]. – 2020. – URL: <https://help.tinkoff.ru> (дата обращения 29.04.22).