**Министерство науки и высшего образования**

**Российской Федерации**

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«Российский университет дружбы народов»**

Факультет физико-математических и естественных наук

Кафедра информационных технологий

«Допустить к защите»

И.о. заведующего кафедрой  
информационных технологий  
д.ф.-м.н., профессор  
\_\_\_\_\_\_\_\_\_\_\_\_ Ю.Н. Орлов

« » 20 г.

**Выпускная квалификационная работа**

**бакалавра**

Направление 09.03.03 «Прикладная информатика»

ТЕМА «Искусственный интеллект как технология противодействия мошенничеству в банковской сфере»

Выполнил студент **Кипчакбаев Рамил Маратович**

|  |  |
| --- | --- |
| Группа НПИбд-01-19 | Руководитель выпускной  квалификационной работы |
| Студ. билет №1032192949 | к. ф-м. н., доц. Шорохов С. Г. |
|  |  |
|  | Автор Кипчакбаев Р.М. |

г. Москва

2023

**Федеральное государственное автономное образовательное учреждение**

**высшего образования**

**«Российский университет дружбы народов»**

**Аннотация**

**выпускной квалификационной работы**

Кипчакбаева Рамила Маратовича

на тему: Искусственный интеллект как технология противодействия мошенничеству в банковской сфере

Дипломное исследование посвящено изучению проблемы мошенничества в банковской сфере и возможностям использования искусственного интеллекта (ИИ) для повышения безопасности финансовых операций.

Объем дипломной работы составляет TODO страниц. Работа состоит из: введения, теоретической главы, главы проектирования системы, главы реализации проекта, заключения.

Во введении обосновывается актуальность темы, ставятся цели и задачи исследования, а также описываются методы исследования.

В первом разделе определяются понятия мошенничества в банковской сфере, раскрываются основные способы мошенничества, анализируются последствия и риски, связанных с мошенничеством в банковской сфере.

Во втором разделе рассматриваются существующие методы борьбы с мошенничеством, а также современные технологии ИИ и их применение в банковском секторе, проектируются сервис онлайн-платежей и модель обнаружения и предотвращения мошеннических действий.

В третьем разделе представлена реализация системы предотвращения мошеннических транзакций, оценка её эффективности и сравнение с существующими системами.

В заключении обобщены результаты исследований в данной области, сделаны выводы о применимости и эффективности искусственного интеллекта в борьбе с мошенничеством в банковской сфере и предложены рекомендации по применению ИИ для выявления мошеннических действий.

Автор ВКР

(Подпись) (ФИО)

TODO заполнить номера страниц

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ](#_Toc102888864) 3

[1. ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ](#_Toc102888865)

[**1.1. Сущность, содержание и основные виды мошенничества**](#_Toc102888866)

[**1.2. Искусственный интеллект и его применение в банковской сфере**](#_Toc102888867)

[**1.3. Проблемы и вызовы, связанные с применением искусственного интеллекта в борьбе с мошенничеством**](#_Toc102888868)

[2. АНАЛИТИЧЕСКИЙ РАЗДЕЛ](#_Toc102888869)

[**2.1.Описание предметной области**](#_Toc102888870)

[**2.2. Анализ существующих решений на основе искусственного интеллекта для борьбы с мошенничеством в банковской сфере**](#_Toc102888871)

[**2.3. Оценка эффективности применения искусственного интеллекта в борьбе с мошенничеством**](#_Toc102888872)

[3. ПРОЕКТНЫЙ РАЗДЕЛ](#_Toc102888873)

[**3.1. Проектирование сервиса онлайн-платежей**](#_Toc102888874)

[**3.2. Разработка модели искусственного интеллекта для противодействия мошенничеству в банковской сфере**](#_Toc102888874)

[**3.3. Тестирование разработанной модели на реальных данных**](#_Toc102888875)

[**3.4. Оценка эффективности разработанной модели и сравнение ее с существующими решениями**](#_Toc102888876)

[ЗАКЛЮЧЕНИЕ](#_Toc102888877)

[Список литературных источников](#_Toc102888878)

[**Приложение 1.**](#_Toc102888879)

[**Приложение 2.**](#_Toc102888880)

[**Приложение 3.**](#_Toc102888881)

# **ВВЕДЕНИЕ**

В настоящее время банковская сфера является одной из самых важных и ответственных в экономике любой страны. Однако, с развитием технологий и электронных платежных систем, появились и новые угрозы, связанные с мошенничеством и киберпреступлениями. Мошеннические операции наносят значительный ущерб не только банкам, но и клиентам, а также всей экономике в целом. Для противодействия этим угрозам, необходимо использовать современные инструменты, включая искусственный интеллект.

Цель данной дипломной работы заключается в исследовании и описании возможностей использования искусственного интеллекта для борьбы с мошенничеством в банковской сфере. В работе будет рассмотрен анализ существующих методов и технологий, применяемых в банковской сфере для обнаружения мошеннических операций. Также будет проведено исследование применения искусственного интеллекта в банковской сфере, его возможностей и преимуществ в борьбе с мошенничеством.

В работе будет проанализирована практическая реализация систем искусственного интеллекта в банковской сфере, а также рассмотрены примеры их успешного применения. Результаты исследования помогут выявить перспективы использования искусственного интеллекта в борьбе с мошенничеством и предложить пути оптимизации и совершенствования существующих методов.

В целом, дипломная работа посвящена актуальной проблеме защиты банковской сферы от мошенничества, и нацелена на исследование и разработку инновационных решений с использованием современных технологий искусственного интеллекта.

Ключевыми целями дипломной работы являются:

1. Анализ методов и технологий, используемых в банковской сфере для обнаружения мошеннических операций.
2. Исследование возможностей и преимуществ применения искусственного интеллекта в борьбе с мошенничеством в банковской сфере.
3. Анализ практической реализации систем искусственного интеллекта в банковской сфере, и рассмотрение примеров успешного применения.
4. Разработка и тестирование собственной системы искусственного интеллекта для обнаружения мошеннических операций в банковской сфере.
5. Определение перспектив применения искусственного интеллекта в борьбе с мошенничеством в банковской сфере.
6. Предложение рекомендаций по оптимизации и совершенствованию существующих методов искусственного интеллекта в борьбе с мошенничеством.

Система, которая должна предотвращать мошенничество в банковской сфере, должна отвечать ряду требований, включая:

1. Надежность: система должна быть высоконадежной и обеспечивать высокую степень защиты от кибератак и мошенничества.
2. Быстродействие: система должна быть быстрой и обрабатывать транзакции в режиме реального времени, чтобы оперативно обнаруживать мошеннические операции.
3. Гибкость: система должна быть гибкой и способной адаптироваться к изменениям в банковской сфере и новым видам мошенничества.
4. Масштабируемость: система должна быть масштабируемой и способной обрабатывать большие объемы данных, чтобы обнаруживать мошеннические операции в режиме реального времени.
5. Соответствие законодательству: система должна соответствовать законодательству и требованиям регуляторных органов в отношении защиты персональных данных и борьбы с мошенничеством в банковской сфере.

**1. ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ**

**1.1 Сущность, содержание и основные виды мошенничества**

В мире существует постоянная угроза мошенничества в банковском секторе. Мошенники постоянно ищут новые способы обмана людей и банковских учреждений. Это может происходить как через традиционные каналы, такие как фишинговые атаки и кражи личных данных клиентов, так и через новые технологии, такие как криптовалюты и смарт-контракты.

Такие мошеннические действия могут привести к серьезным последствиям, например, потеря денег клиентами банка, нарушение их личной информации и финансовых данных, ущерб репутации банка и ухудшение его финансовых показателей.

Банки предпринимают различные меры для борьбы с мошенничеством, такие как использование современных технологий защиты, повышение уровня обучения персонала и клиентов, введение двухфакторной аутентификации и многое другое. Также существуют различные организации и регуляторы, которые занимаются контролем и регулированием банковской деятельности в целом и борьбой с мошенничеством в частности.

Несмотря на все усилия, мошенничество в банковском секторе остается серьезной угрозой для клиентов и финансовых учреждений, поэтому важно оставаться бдительным и принимать меры предосторожности при работе с банками и финансовыми институтами.

Мошенничество в банковском секторе представляет собой незаконные действия, совершаемые с целью получения финансовой выгоды или доступа к конфиденциальной информации клиентов банка. Это может включать различные формы деятельности, такие как фишинг, кражу личных данных, кражу идентификационных данных, кибератаки и отмывание денег.

Один из наиболее распространенных методов мошенничества в банковском секторе - фишинг, когда злоумышленники отправляют поддельные электронные письма и создают фальшивые веб-сайты, чтобы получить доступ к личным данным клиентов, таким как номера банковских карт, логины и пароли. Они могут использовать эту информацию для взлома банковских аккаунтов или воровства личных данных.

Кража личных данных и идентификационных данных — это также распространенные методы мошенничества в банковском секторе. Злоумышленники могут использовать украденные личные данные для открытия фиктивных счетов, получения кредитов или осуществления других финансовых махинаций.

Кибератаки представляют серьезную угрозу для банковской безопасности, так как злоумышленники могут получить доступ к конфиденциальной информации клиентов, а также к счетам и финансовым ресурсам банка. Кибератаки могут включать в себя взломы сайтов банков, использование вредоносных программ и другие методы.

Отмывание денег — это процесс, при котором незаконно полученные деньги используются для приобретения легитимности через банковские счета или другие финансовые инструменты. Это может включать использование фиктивных счетов, перевод денег на другие счета и другие методы.

[**1.2. Искусственный интеллект и его применение в банковской сфере**](#_Toc102888867)

Искусственный интеллект (AI) — это область науки и технологии, которая занимается созданием программ и алгоритмов, которые позволяют компьютерам "думать" и "выполнять задачи", которые ранее были свойственны только человеческому интеллекту. Иными словами, искусственный интеллект относится к созданию компьютерных систем, которые способны выполнять задачи, которые требуют интеллектуальных способностей, таких как распознавание речи, обработка естественного языка, анализ данных, обучение, адаптация к новой информации и т.д.

Технически искусственный интеллект может включать в себя множество различных методов и технологий, таких как машинное обучение, глубокое обучение, нейронные сети, алгоритмы генетической оптимизации, различные формы логики, робототехника и многие другие. Все эти методы и технологии предназначены для того, чтобы обучать компьютерные системы находить закономерности в данных, выделять наиболее значимые признаки и принимать решения на основе полученных знаний.

В основе искусственного интеллекта лежит машинное обучение (Machine Learning), которое позволяет компьютерам обучаться на больших объемах данных, выявлять образцы и закономерности и делать предсказания на основе этих данных. Машинное обучение включает в себя алгоритмы классификации, регрессии, кластеризации, нейронные сети, глубокое обучение и т.д.

Искусственный интеллект может быть использован в различных областях, таких как медицина, финансы, транспорт, промышленность, реклама и т.д. В банковском секторе, искусственный интеллект используется для предотвращения мошенничества, прогнозирования рисков, управления портфелем, рекомендаций и т.д.

Искусственный интеллект имеет огромный потенциал для предотвращения мошенничества в банковской сфере. Ниже перечислены несколько преимуществ использования ИИ для предотвращения мошенничества в банковском секторе:

* Автоматизация процессов обнаружения мошенничества. С помощью ИИ можно автоматизировать процессы анализа больших объемов данных, чтобы выявлять потенциальные мошеннические операции. ИИ может выделять аномальные транзакции, сравнивать данные клиентов с ранее известными случаями мошенничества, а также использовать машинное обучение для создания точных моделей выявления мошенничества.
* Быстрое реагирование на мошеннические операции. ИИ может работать в режиме реального времени, что позволяет банкам быстро реагировать на мошеннические операции и принимать меры по предотвращению дополнительных потерь.
* Адаптивность: искусственный интеллект может обучаться на основе новых данных и улучшать свои алгоритмы для более эффективного предотвращения мошенничества.
* Сокращение затрат на предотвращение мошенничества. Использование ИИ может помочь банкам сократить затраты на предотвращение мошенничества, так как автоматизированные процессы могут быть более эффективными и точными, чем процессы, осуществляемые людьми.
* Защита конфиденциальности данных. Использование ИИ для предотвращения мошенничества может помочь банкам защитить конфиденциальность данных клиентов, так как ИИ может работать с большими объемами данных, не нарушая конфиденциальность.
* Улучшение качества обслуживания клиентов. Использование ИИ для предотвращения мошенничества может помочь банкам улучшить качество обслуживания клиентов, так как банки могут быстро и точно идентифицировать мошеннические операции и предотвращать их, не затрагивая удобство использования сервиса.

[**1.3. Проблемы и вызовы, связанные с применением искусственного интеллекта в борьбе с мошенничеством**](#_Toc102888868)

Хотя применение искусственного интеллекта в борьбе с мошенничеством может привести к значительному улучшению безопасности, но у него также есть свои проблемы и вызовы, которые могут ограничить его эффективность. Некоторые из таких вызовов включают в себя:

Недостаток качественных данных: для того, чтобы ИИ был эффективным в борьбе с мошенничеством, необходимы качественные данные. Однако, в борьбе с мошенничеством зачастую не всегда есть доступ к достаточно широкому диапазону данных, так как мошенники постоянно изменяют свои тактики и методы.

Сложность обучения модели: Обучение ИИ модели может быть сложным процессом, особенно если речь идет о более сложных задачах. Необходимо иметь квалифицированных специалистов, чтобы правильно настроить модели и обучить их на подходящих данных.

Ложноположительные и ложноотрицательные результаты: Использование ИИ может привести к ложноположительным и ложноотрицательным результатам. Например, ИИ может считать подозрительной легитимную транзакцию, которая попадает в категорию аномалии. Или, наоборот, ИИ может пропустить мошенническую транзакцию, которая считается нормальной, так как мошенник может использовать новые методы и тактики. Это может приводить к недовольству клиентов и потере доверия к банковской организации.

Необходимость постоянного обновления модели: Мошенники постоянно развивают свои методы, что требует от организаций постоянно обновлять свои ИИ модели, чтобы оставаться эффективными в борьбе с новыми мошенническими схемами.

Проблемы безопасности: использование ИИ может также повысить риски безопасности, так как мошенники могут использовать атаки на ИИ для искажения результатов и обойти систему. Кроме того, необходимо обеспечить безопасность данных и предотвратить утечки информации, которые могут использоваться мошенниками.

Этические и юридические вопросы: Использование ИИ в борьбе с мошенничеством также может вызвать этические и юридические вопросы. Например, сбор и обработка данных могут нарушать приватность клиентов. Кроме того, возможно, что ИИ может принимать решения, которые могут оказаться дискриминационными.

В целом, применение ИИ в борьбе с мошенничеством имеет множество преимуществ, однако, необходимо учитывать и эти вызовы и проблемы, чтобы эффективно использовать технологии ИИ в банковской сфере.