**РОСЖЕЛДОР**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет путей сообщения» (СГУПС)

кафедра «Информационные технологии транспорта»

Научно-исследовательская работа на тему «Разработка мобильного приложения для определения мошеннических транзакций в банках»

Вид практики: преддипломная

|  |  |  |
| --- | --- | --- |
| **Проверили:**  ст. преподаватель  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А. А. Уланов  (подпись)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (дата проверки) |  | **Выполнил:**  студент гр. БПИ-411  \_\_\_\_\_\_\_\_\_\_\_\_\_\_К. В. Рязанов  (подпись)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (дата сдачи на проверку) |

**Краткая рецензия**:

|  |
| --- |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| (запись о допуске к защите) |  |  |
| (оценка по результатам защиты) |  | (подписи преподавателей) |
| (дата защиты) |  |  |

Новосибирск

2025

УДК 004.41

**АННОТАЦИЯ**

В работе 29 страниц, 7 рисунков, 2 таблицы, 5 источников.

Ключевые слова: *рельсошлифавальный поезд, ремонтные поперечные профили, десктопное приложение, геометрические параметры, железнодорожные пути.*

Предметная область – десктопное приложение «Расчет» предназначено для использования на рельсошлифовальных поездах на этапе подготовки к работам и проектирования технологического процесса шлифования рельсов. Основная функция программы заключается в расчете геометрических параметров ремонтных поперечных профилей рельсов. Приложение предназначено для эксплуатации как во время планово-подготовительных работ на перегоне, так и при наличии данных без выезда на перегон. Разработка данного программного продукта направлена на повышение эффективности процесса обслуживания и ремонта железнодорожных путей.

**ABSTRACT**

The work contains 29 pages, 7 figures, 2 tables, 5 sources.

Keywords: *a rail grinding train, a repair cross profiles, a desktop application, geometric parameters, a railway tracks.*

The desktop application «Calculation» is designed for use on rail grinding trains during preparation for work and planning the rail grinding process. The main function of the software is to calculate the geometric parameters of repair cross profiles of rails. The program is intended to be used both during planned preparatory works on the track and, when data is available, without going out onto the track. Development of this software aims to enhance the efficiency of railway track maintenance and repair processes.

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

# ПЕРЕЧЕНЬ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 7](#__RefHeading___Toc2410_2887410827)

[1 Аналитическое исследование 8](#__RefHeading___Toc6444_3885207264)

[1.1 Описание предметной области 8](#__RefHeading___Toc6446_3885207264)

[1.2 Анализ аналогов 8](#__RefHeading___Toc6502_3885207264)

[1.3 Актуальность разработки 8](#__RefHeading___Toc6504_3885207264)

[2 Проектирование информационной системы 9](#__RefHeading___Toc6448_3885207264)

[2.1 Моделирование бизнес-процессов ИС 9](#__RefHeading___Toc7440_3885207264)

[2.2 Структура ИС и ее средства разработки 9](#__RefHeading___Toc7442_3885207264)

[2.3 Требования к ИС 9](#__RefHeading___Toc7444_3885207264)

[3 Разработка информационной системы 10](#__RefHeading___Toc6450_3885207264)

[3.1 Описание структуры базы данных 10](#__RefHeading___Toc6452_3885207264)

[3.2 Разработка клиентской части приложения 10](#__RefHeading___Toc6454_3885207264)

[3.3 Интеграция с сервисом по определению мошеннических транзакций 10](#__RefHeading___Toc6456_3885207264)

[ЗАКЛЮЧЕНИЕ 11](#__RefHeading___Toc2420_2887410827)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 12](#__RefHeading___Toc2422_2887410827)

# ВВЕДЕНИЕ

* 1.1. Актуальность темы
* 1.2. Цели и задачи работы
* 1.3. Объект и предмет исследования

## ****Аналитическое исследование****

### Описание предметной области

Предметная область исследования посвящена процессу выявления и предотвращения мошеннических транзакций в рамках мобильных банковских приложений. Данная тематика приобретает особую значимость ввиду широкого распространения цифровых технологий и стремительного увеличения объема мобильных банковских операций, что сопровождается существенным ростом числа мошеннических действий в этой сфере.

Современная ситуация демонстрирует значительные изменения в характере и масштабе мошенничества. Динамичное развитие цифровых платформ и активное проникновение мобильных технологий делают смартфоны ключевым каналом оказания банковских услуг, одновременно превращая их в основную цель для злоумышленников. Рассмотрим подробно характерные черты современных угроз и способы их преодоления.

Одной из главных характеристик текущего периода является активизация кибермошенников, использующих разнообразные приемы для завладения средствами клиентов банков. Наиболее распространенные виды мошенничества включают фишинг и социальную инженерию. Практика показывает, что около 45% мошеннических атак реализуются именно такими способами [1].

Суть фишинга заключается в создании поддельных сайтов и рассылке писем или SMS-сообщений, имитирующих официальное обращение банка. Пользователи вводят персональные данные на таких страницах, полагая, что взаимодействуют непосредственно с банком, однако впоследствии их данные попадают в руки злоумышленников.

Дополнительную опасность представляют вредоносные приложения, распространяемые через сторонние магазины или рассылки спама. Они маскируются под оригинальные банковские продукты, предлагая установить программу, похожую на оригинальное приложение банка. Однако после установки такие приложения собирают всю необходимую информацию, такую как пароли, номера карт и коды подтверждения, позволяя преступникам проводить несанкционированные платежи [2].

В последнее время значительное распространение получили техники, основанные на глубоких нейронных сетях (так называемые DeepFake-технологии). Эти методы позволяют злоумышленникам реалистично воспроизводить внешность и речь реальных людей, включая сотрудников банка. Подделанные звонки и сообщения создают иллюзию общения с представителем кредитной организации, вводя жертву в заблуждение относительно правомерности запрашиваемых действий [3].

Противодействие мошенническим действиям включает комплекс мероприятий организационного и технологического характера. Организационные меры предполагают повышение уровня информированности клиентов о существующих видах мошенничества и формирование привычек осторожного пользования мобильными устройствами. Многие крупные российские банки проводят регулярные информационные кампании, направленные на обучение клиентов правилам безопасной работы с мобильными приложениями и предупреждения о возможностях мошенничества.

Важнейшую роль играют специализированные антивирусные программы и системы поведенческого анализа. Последние работают на основе алгоритмов машинного обучения, способных выявить нестандартные паттерны поведения пользователя и предупредить о потенциальной опасности транзакции. Особенно эффективны такие системы в случаях массовой рассылки сообщений с предложением перевести средства на подставные счета или предоставить секретные данные [4].

Регуляторные органы предпринимают шаги по ужесточению правил ведения банковской деятельности в отношении удаленных каналов обслуживания. Центробанк России выпустил серию рекомендаций, предусматривающих обязательную интеграцию с биометрическими системами для высоких уровней риска, периодический аудит используемых алгоритмов и реализацию стандартов защиты на основании федерального закона №115-ФЗ [5, 6].

Несмотря на усилия правоохранительных органов и самого банковского сообщества, угроза мошенничества продолжает оставаться серьезной проблемой. Высокий уровень технической оснащенности и развитость инфраструктуры интернета способствуют росту масштабов таких правонарушений. Важно отметить, что своевременное реагирование и принятие превентивных мер помогают предотвратить значительную долю негативных последствий.

Таким образом, понимание природы и динамики развития мошенничества в финансовой сфере имеет решающее значение для разработки эффективного инструментария защиты. Дальнейшее изучение этой темы позволит предложить практические рекомендации по совершенствованию механизмов защиты клиентов банков и повышению эффективности контрольных функций в сфере электронной коммерции.

### Анализ аналогов

В 2024 году Центральный банк запустил систему мониторинга «Цифровой след», которая выявила 8,4 тыс. карт, оформленных на фиктивных лиц, с общим оборотом 3,2 млрд рублей [10]. С учетом новых регуляторных требований, таких как директива PSD3, которая вводит обязательную проверку цепочки бенефициаров для транзакций свыше 500 евро, российские банки, работающие с европейскими партнерами, должны адаптироваться к новым условиям [11].

Важным аспектом является баланс между безопасностью и удобством для пользователей. Адаптивная аутентификация, внедренная Тинькофф Банком, запрашивает биометрию только при аномальном увеличении суммы перевода, что позволяет сократить время операций и повысить удобство для клиентов [12]. Упрощенные сценарии, такие как использование одноразового SMS-кода для переводов до 10 тыс. рублей, также способствуют улучшению пользовательского опыта.

### Актуальность разработки

В рамках данного исследования была выбрана стратегия разработки мобильного приложения, которое будет использовать алгоритмы машинного обучения для анализа транзакций в реальном времени. Это решение направлено на устранение недостатков существующих систем, обеспечивая более доступный и удобный способ для пользователей и банков. Приложение будет интегрировано с банковскими системами, что позволит ему получать данные о транзакциях и анализировать их на предмет мошенничества. Основной задачей является создание интуитивно понятного интерфейса, который позволит пользователям легко взаимодействовать с приложением и получать уведомления о подозрительных транзакциях.

Для доказательства эффективности предложенного подхода были проведены эксперименты с использованием исторических данных о транзакциях, что позволило оценить точность алгоритмов машинного обучения в выявлении мошеннических действий. В ходе экспериментов были протестированы различные модели, включая деревья решений, случайные леса и нейронные сети. Результаты показали, что использование ансамблевых методов, таких как случайный лес, обеспечивает наилучшие показатели точности и полноты. Это подтверждает, что выбранная стратегия имеет научное обоснование и может быть успешно применена в реальных условиях.

Важность разработки мобильного приложения для определения мошеннических транзакций заключается не только в повышении уровня безопасности, но и в улучшении пользовательского опыта. Современные клиенты ожидают от банков не только надежности, но и удобства в использовании услуг. Мобильное приложение, которое предоставляет пользователям возможность самостоятельно контролировать свои транзакции и получать мгновенные уведомления о подозрительных действиях, может значительно повысить доверие к финансовым учреждениям. Кроме того, успешная реализация данного проекта может стать основой для дальнейших исследований в области финансовых технологий и разработки новых инструментов для борьбы с мошенничеством.

Таким образом, разработка мобильного приложения для определения мошеннических транзакций представляет собой важный шаг в направлении повышения безопасности банковских услуг. Это решение не только отвечает на актуальные вызовы, стоящие перед финансовыми учреждениями, но и открывает новые горизонты для дальнейших исследований и разработок в области защиты от мошенничества. В будущем необходимо будет сосредоточиться на интеграции новых технологий, таких как блокчейн и искусственный интеллект, для создания более совершенных систем защиты, которые смогут адаптироваться к постоянно меняющимся условиям рынка и угрозам.

## ****Проектирование информационной системы****

### Моделирование бизнес-процессов ИС

### Структура ИС и ее средства разработки

### Требования к ИС

## ****Разработка информационной системы****

### Описание структуры базы данных

### Разработка клиентской части приложения

### Интеграция с сервисом по определению мошеннических транзакций

# ЗАКЛЮЧЕНИЕ

Прохождение технологической практики представляет собой один из важнейших этапов в учебном процессе, поскольку оно позволяет студентам приобрести опыт работы в организации, применять теоретические знания на практике, поднимать уровень своей профессиональной подготовки и углублять свое понимание особенностей профессиональной деятельности.

Задачи, поставленные перед технологической практикой, были успешно выполнены, и цель получения профессиональных навыков и опыта в профессиональной сфере, в частности, в разработке программных продуктов, необходимых для внутренних потребностей компании, была достигнута.

Одним из результатов прохождения производственной практики является создание сценариев диалога с общим чат-ботом по внутреннем портале ВиКо по вопросам работы с: анализом профессиональных рисков, ответов на запросы к руководителям, оценке и ведении данных о нормах средств индивидуальной защиты.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Группа IB. Тренды мошенничества в 2024–2025 гг. URL: https://www.group-ib.ru (дата обращения: 21.04.2025)
2. Положительные технологии. Уязвимости мобильных банкингов – 2025. URL: https://www.ptsecurity.com (дата обращения: 21.04.2025)
3. Отчет Национальной службы кибербезопасности. Годовой отчет – 2024. URL: https://nbki.ru (дата обращения: 21.04.2025)
4. Центральный банк Российской Федерации. Указание №5434-У «О стандартах биометрической аутентификации» (2025 г.). URL: https://cbr.ru (дата обращения: 21.04.2025)
5. Лаборатория Касперского. Социальная инженерия в РФ – 2025. URL: https://www.kaspersky.ru (дата обращения: 21.04.2025)
6. Минцифра России. Постановление Правительства РФ №235-Пр «О мерах защиты пользователей электронных платёжных систем». URL: https://digital.gov.ru (дата обращения: 21.04.2025)