**(Слайд 1: Титульный слайд)**

Уважаемые члены комиссии, уважаемые присутствующие!

Тема моего научного доклада – «Разработка мобильного приложения для определения мошеннических транзакций в банках».

Работа выполнена в рамках преддипломной практики на кафедре «Информационные технологии транспорта» Сибирского государственного университета путей сообщения.

**(Слайд 2: Цель и задачи)**

Современный мобильный банкинг удобен, но попрежднему уязвим для мошенников.

Целью данной работы является разработка прототипа мобильного банка, который демонстрирует улучшенные механизмы информирования пользователя о рисках мошеннических транзакций, делая акцент на проактивность и удобство, что бы люди сами делали выбор что делать с возможными рисками.

Для достижения этой цели были поставлены следующие задачи:

Во-первых, проанализировать предметную область и существующие угрозы.

Во-вторых, исследовать аналогичные решения ведущих банков.

В-третьих, обосновать актуальность разработки и спроектировать архитектуру системы.

В-четвертых, разработать ключевые компоненты прототипа.

И, наконец, продемонстрировать его работу.

**(Слайд 3: Описание предметной области)**

Предметная область данной работы – выявление и предотвращение мошенничества в мобильном банкинге. Стремительный рост объема мобильных банковских операций, к сожалению, сопровождается существенным и продолжающимся ростом числа мошеннических действий в этой сфере как в России, так и в мире.

Основные угрозы сегодня – это фишинг и социальная инженерия, на долю которых, согласно прогнозам экспертов на 2024-2025 годы, приходится около 45% всех успешных атак.

Как показал опрос, проведенный ВТБ среди клиентов, свыше 80% россиян сталкивались с мошенниками, которые пытались украсть деньги с их банковского счёта.

Масштабы проблемы подтверждаются и данными ЦБ РФ: Это связанно с низкой киберграмотностью граждан. Именно низкая осведомлённость и неосторожность пользователей заняла первое место с показателем 29% из всех рисков, с которыми люди сталкиваются при использовании мобильных устройств для совершения транзакций.

Банки внедряют сложные системы защиты, включая поведенческий анализ и машинное обучение, но острота проблемы требует новых подходов, ориентированных на пользователя.

**(Слайд 4: Анализ аналогов)**

Проанализировав открытые дланные об антифрод-системы СберБанка, ВТБ, Т-Банка и платформу ЦБ РФ. Был выявлен список технологий которые они используют: сложные многослойные нейронные сети для анализа сотен параметров транзакции, многофакторная и адаптивная аутентификация для обеспечения безопасности данных.

Однако часто эти системы работают реактивно, блокируя операции постфактум, а многочисленные проверки могут вызывать раздражение у пользователей, что подтверждается опросом за ноябрь 2024 года проведенный Высшей школой экономики по его результатам 85 процентам пользователей не нравятся текущая политика уведомлений от банков.

**(Слайд 5: Актуальность разработки)**

Именно эти ограничения существующих систем подчеркивают актуальность нашей разработки.

Необходимо решение, которое будет не просто блокировать, а проактивно информировать пользователя о риске до завершения транзакции. Наш подход направлен на:

Повышение контроля пользователя через осознанное блокирование карты.

Улучшение пользовательского опыта за счет наглядной визуализации риска и ненавязчивых уведомлений.

**(Слайд 6: Бизнес-процессы)**

Для проектирования системы мы использовали UML-диаграммы.

Диаграммы вариантов использования определили акторов и их возможные действия.

Ключевым элементом стала диаграмма последовательности, которая моделирует поток взаимодействия между пользователем и всеми компонентами системы.

На данной диаграмме изображены 3 основный процесса в приложении:  
  
Возможность создания карты, для симуляции банковского приложениями

Совершение транзакции с ей последующей проверкой и отображением результатов этом проверки пользователю.

Блокировка карты с подозрительными транзакциями для предотвращения возможных рисков.

**(Слайд 7: Используемые в разработке технологии)**

Система спроектирована с использованием сервис-ориентированного подхода.

Это подход к созданию программного обеспечения, при котором приложение разбивается на независимые сервисы, которые легко масштабируются, изменяются и тестируются.

К таким компонентам в данной ИС относятся:

Серверная часть (Backend) реализована на ASP.NET Core 8 с использованием C#.

Клиентская часть (Frontend) – это нативное мобильное приложение для Android, разработанное на языке Kotlin.

В качестве системы управления базами данных выбрана PostgreSQL 16.

Разработка велась в средах Visual Studio 2022 и Android Studio.

Этот стек технологий обеспечивает необходимую производительность, кроссплатформенность серверной части, безопасность по возможностям настройки веб защиты встроенной в фреймворк ASP.net, удобство разработки внешнего вида прототипа и его тестирование в графическом редакторе и эмуляторе Android Studio.

**(Слайд 8: Демонстрация рабочего продукта)**

Сейчас я продемонстрирую работу прототипа.

На вход пользователь подает данные, например, создавая карту или инициируя перевод: выбирает карты, вводит сумму.

Приложение отправляет эти данные на сервер, который взаимодействует с антифрод-системой и получает оценку риска.

На выходе пользователь видит:

Уведомление, которое появляется сразу при попытке совершить операцию с высоким риском, давая возможность отреагировать.

В истории транзакций (показываем экран истории) каждая операция имеет визуальный индикатор риска.

На отдельной вкладке представлена обобщенная визуализация.

**(Слайд 9: Заключение)**

Подводя итоги преддипломной практики:

Был проведен анализ предметной области и аналогов

Спроектирована архитектура системы, выбран стек технологий, разработан и продемонстрирован прототип мобильного приложения.

Ключевое отличие предложенного решения – акцент на проактивном информировании пользователя и улучшении его взаимодействия с антифрод-системой по средствам вывода аналитических данных во временном промежутке.

Практика позволила закрепить навыки проектирования и разработки, а созданный прототип является основой для дальнейшей работы над выпускной квалификационной работой, где планируется полная реализация функционала в виде добавления возможности блокировки карты и комплексное тестирование всей системы.