Найдёнов А.А. ИД22-3

Разработка контейнера для обеспечения безопасности рекомендательной системы в финансовом секторе при угрозе неправомерных действий в каналах связи

Описание предметной области и пример работы рекомендательной системы

Рекомендательная система в финансовом секторе – это инструмент, который, используя алгоритмы машинного обучения и анализа данных, предлагает пользователям персонализированные советы и предложения, связанные с финансовыми продуктами и услугами. Система анализирует множество факторов, включая:

Историю транзакций пользователя: Какие платежи совершал пользователь, какие продукты и услуги он приобретал ранее.

Финансовое поведение: Как часто пользователь тратит деньги, какие категории товаров и услуг его интересуют, как он управляет своими сбережениями.

Демографические данные: Возраст, пол, местоположение, уровень дохода и другие социально-экономические характеристики.

Рыночные тенденции и анализ данных: Текущие процентные ставки, акции, курсы валют, инвестиционные возможности.

Профиль риска: Оценка склонности пользователя к риску при инвестировании.

На основе этого анализа система генерирует персональные рекомендации, такие как:

Инвестиционные возможности: Предложения по покупке акций, облигаций, паев инвестиционных фондов и других финансовых инструментов, соответствующие профилю риска и финансовым целям пользователя.

Кредитные продукты: Персональные предложения по кредитным картам, потребительским кредитам, ипотеке с учетом кредитной истории и финансовых потребностей пользователя.

Страховые продукты: Рекомендации по выбору страховых полисов (автомобильное страхование, страхование жизни, страхование имущества и т. д.), соответствующие потребностям пользователя.

Финансовое планирование: Советы по управлению бюджетом, оптимизации сбережений, планированию пенсионных накоплений.

Оптимизация расходов: Предложения по снижению расходов, например, путем выбора более выгодных тарифов на коммунальные услуги или банковские продукты.

Примерный сценарий работы пользователя

Авторизация и вход в систему: Пользователь входит в свой личный кабинет в мобильном приложении или на веб-сайте банка.
Просмотр главной страницы: На главной странице пользователь видит приветствие и краткий обзор своей финансовой ситуации (остаток на счетах, кредитный лимит,

инвестиционный портфель). Также на главной странице отображаются персональные рекомендации системы.
Изучение рекомендаций: Пользователь просматривает предложенные рекомендации:

Инвестиционная возможность: "Мы рекомендуем обратить внимание на акции компании XYZ, которые, по нашим прогнозам, покажут рост в ближайшие месяцы".

Кредитный продукт: "Вам одобрена кредитная карта с льготным периодом 120 дней".

Страховой продукт: "Мы предлагаем вам рассмотреть полис страхования имущества, который защитит ваш дом от непредвиденных обстоятельств".
Подробная информация: Пользователь кликает на интересующую его рекомендацию и получает более подробную информацию о предложении:
Инвестиции: Графики роста акций, прогнозы аналитиков, уровни риска.
Кредиты: Условия кредитования, процентная ставка, график погашения.
Страхование: Условия страхования, размер страховых выплат, список страховых случаев.
Принятие Решений: На основе полученной информации пользователь принимает решение.
Обратная связь: Пользователь может оставить отзыв о полученной рекомендации, указав, была ли она полезной, интересной и т.д. Это помогает системе улучшать качество рекомендаций в будущем.

Техническое задание на разработку контейнера для обеспечения безопасности рекомендательной системы в финансовом секторе при угрозе неправомерных действий в каналах связи

1. **Введение**
   Утечка персональных данных: Алгоритмы рекомендательных систем работают на основе персональных данных, и их утечка может привести к тому, что сведения будут проданы, куплены и использованы не по назначению2. Риск утечки персональных данных является одной из основных опасностей, связанных с рекомендательными системами. В связи с чем возникает необходимость разработки контейнера для обеспечения безопасности системы
2. **Основание для разработки:**
   Основанием для разработки является задание в рамках курса «Основы DevOps»
3. **Назначение разработки:**
   Контейнер предназначен для защиты от внесения изменений в работу сетевых протоколов злоумышленниками, которые могут добавлять или удалять данные из информационного потока. Цель таких действий — повлиять на работу системы или получить доступ к конфиденциальной информации. Разработка контейнера направлена на предотвращение нарушений конфиденциальности и целостности данных, которые могут возникнуть в результате несанкционированного доступа к сетевому трафику
4. **Требования к функциональным характеристикам**
   4.1. Требования к функциональным характеристикам

   Контейнер должен обеспечивать:

   - Защиту от сетевых атак через фильтрацию и блокировку подозрительного трафика.

- Логирование всех запросов в формате JSON для последующего анализа и аудита.
- Шифрование данных при передаче (TLS 1.2+).
- Интеграцию с системой рекомендаций через Docker-сети и reverse proxy.
- Мониторинг активности.
- Блокировку IP-адресов при превышении лимита запросов.
- Целостность данных (предотвращение модификации рекомендаций в канале связи).

Важные данные в контейнере:

- *IP-адреса клиентов (для анализа поведения).*
- *Запросы к системе (для обнаружения атак).*
- *Метаданные запросов (User-Agent, Referer, время, статусы).*

4.2. Требования к надежности

Контейнер должен:

- Обеспечивать автоматическое восстановление после сбоя.
- Поддерживать горячее обновление правил.
- Сохранять данные в случае перезапуска.
- Работать корректно в условиях сетевых задержек и временного отключения сервисов.

4.3 Условия эксплуатации

Использовать систему будут пользователи средней и низкой квалификации. Интерфейс системы должен быть максимально приближен к интерфейсам подобных систем. Вывод информации должен осуществляться в наиболее унифицированных формах.

4.4. Требования к составу и параметрам технических средств

Для разработки и тестирования системы необходимы:

Аппаратные требования:

- Хост:
    - ОС: Linux (Ubuntu 20.04+) / Windows 10+ / macOS 11+
    - RAM: 4 GB+
    - CPU: 2 ядра+
    - Диск: 20 GB свободного места

Программные требования:

- Docker Engine версия 20+

- Docker Compose версия 2.0+
- Linux kernel 5.10+
- Python 3.11+
- MySQL 8.0+
- Nginx 1.24+
- Fail2ban 1.1.0+

5. **Требования к программной документации (в соответствии с ГОСТ 19.101-77)**
    - Пояснительная записка (ГОСТ 19.404-79)
    - Руководство программиста (ГОСТ 19.504-79)
    - Описание программы (ГОСТ 19.402-78)
    - Текст программы (ГОСТ 19.401-78)
    - Описание применения (ГОСТ 19.502-78)
    - Программа и методы испытаний (ГОСТ 19.301-79)

6. **Порядок контроля и приемки**

    Приемка работы осуществляется по результатам приемо-сдаточных испытаний, проводимых в присутствии представителей заказчика в соответствии с программой и методикой испытаний на тестовых данных, подготовленных заказчиком.