DOI 10.37882/2223-2966.2025.04-2.15

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ

THE USE OF ARTIFICIAL INTELLIGENCE TO COUNTER FRAUD

O. Karelova
M. Makarov

Summary. The article is devoted to topical issues of the use of artificial intelligence in the fight against cyberbullying. The paper proposes a mathematical and linguistic model based on which a virtual interlocutor with artificial intelligence (chatbot) has been developed to increase the effectiveness of protection against a type of cyberfraud — telephone scam.

Keywords: fraud, artificial intelligence, social engineering, information security, risk reduction.

Карелова Оксана Леонидовна
Доктор физико-математических наук, профессор, Московский Государственный Лингвистический Университет; Президентская академия (Москва)
okarelova@yandex.ru
Макаров Мирон Павлович
Московский Государственный Лингвистический Университет
Miron.m4karov@yandex.ru

Аннотация. Статья посвящена актуальным вопросам использования искусственного интеллекта в борьбе с кибермошенничеством. В работе предложена математико-лингвистическая модель, на базе которой разработан виртуальный собеседник с искусственным интеллектом (чат-бот) для повышения эффективности защиты от разновидности кибермошенничества — телефонного мошенничества.

Ключевые слова: мошенничество, искусственный интеллект, социальная инженерия, информационная безопасность, риск.

В эпоху цифровизации финансовые преступления становятся всё более изощрёнными и масштабными. Кибермошенники постоянно совершенствуют свои методы, используя передовые технологии для обмана людей и организаций. По последним данным[1], ежегодный ущерб от киберпреступлений достигает астрономических сумм, а количество пострадавших продолжает расти в геометрической прогрессии.

Традиционные методы борьбы с мошенничеством уже не справляются с современными вызовами. Человеческий фактор, задержки в обработке информации и ограниченность ресурсов правоохранительных органов создают благоприятные условия для деятельности преступников. Именно поэтому критически важно разрабатывать и внедрять инновационные решения, способные оперативно выявлять и предотвращать мошеннические схемы.

Практические компьютерные программы становятся первым рубежом обороны в борьбе с киберпреступностью. Они способны анализировать огромные массивы данных в режиме реального времени, выявлять подозрительные паттерны поведения и принимать превентивные меры задолго до того, как ущерб станет необратимым. От банковских антифрод систем до специализированных решений для защиты персональных данных — программное обеспечение становится неотъемлемой частью современной системы безопасности.

В последние годы наблюдается тревожный рост телефонного мошенничества, и у этого явления есть несколько весомых причин.

1. Простой доступ к потенциальным жертвам

Мошенники получили возможность легко находить людей для своих афер благодаря:

- Доступным базам телефонных номеров
- Развитой IP-телефонии
- Возможности совершать звонки из любой точки мира
- Возможности оставаться анонимными при звонках

2. Минимальные риски для преступников

Телефонное мошенничество привлекает злоумышленников тем, что:

- Позволяет действовать скрытно
- Снижает риск быть пойманными
- Дает возможность быстро менять локации
- Усложняет процесс идентификации преступников

3. Технологическая поддержка мошенников

Современные технологии стали как благословением для общества, так и инструментом для преступников:

[1] Ущерб от IT-преступлений в 2024 году уже достиг 99 млрд рублей//Ведомости/ URL: https://www.vedomosti.ru/society/articles/2024/09/04/1059854-uscherb-ot-it-prestuplenii-dostig-99-mlrd-rublei (дата обращения 20.02.2025)

- Возможность подмены номеров
- Создание фальшивых документов
- Автоматизация обзвонов
- Имитация официальных служб

4. SIM-карты как инструмент мошенничества

Особую роль играет доступность «серых» SIM-карт в России:

- Возможность приобретения без регистрации
- Низкая стоимость
- Простота получения
- Быстрота активации

5. Психологическое воздействие

Звонки остаются одним из самых эффективных способов манипуляции:

- Прямой контакт с жертвой
- Возможность адаптации под конкретную ситуацию
- Создание чувства срочности
- Особое воздействие на уязвимые группы

6. Недостатки системы безопасности

Пробелы в системе защиты также способствуют росту мошенничества:

- Медленная реакция на подозрительные операции
- Недостаточная проверка транзакций
- Отсутствие мгновенной блокировки мошеннических схем
- Задержки в реагировании финансовых учреждений

Для реализации предиктивной защиты от мошеннических звонков предложен подход, основанный на том, что номер звонящего ищется не по уже сформированной базе мошеннических номеров, а по логике формирования случайных номеров и использованию серых сим-карт.

Предлагается реализация данного подхода по следующей схеме:

1. Анализ структуры номера:
- Выявление аномальных комбинаций цифр (например, последовательности 12345 или повторяющиеся цифры).
- Определение необычных префиксов операторов.
- Анализ географического расположения номера относительно звонящего.
2. Алгоритмы оценки:
- Проверка соответствия кода провайдера региону звонка.
- Анализ времени активности номера.
- Выявление паттернов в последовательности цифр.
- Оценка частоты смены номеров одним абонентом.

В статье приведена практическая реализация предложенного подхода по этой схеме в виде чат-бота.

В современных условиях борьбы с мошенничеством чат-боты демонстрируют беспрецедентную эффективность благодаря уникальному сочетанию возможностей искусственного интеллекта и автоматизации.

Во-первых, чат-боты способны круглосуточно обрабатывать огромное количество обращений, мгновенно анализируя сообщения на предмет подозрительной активности. В отличие от человеческих операторов, им не требуется отдых, а скорость обработки информации многократно выше. Во-вторых, современные чат-боты используют сложные алгоритмы машинного обучения, позволяющие распознавать новые схемы мошенничества по мере их появления. Они могут анализировать языковые паттерны, эмоциональные маркеры и поведенческие особенности собеседников, выявляя даже едва заметные признаки мошеннических действий. В-третьих, чат-боты могут одновременно вести диалог с множеством пользователей, что критически важно при массовых атаках мошенников. Они способны оперативно реагировать на стандартные сценарии мошенничества по заранее заданным алгоритмам, при этом передавая сложные случаи на рассмотрение специалистам.

Особую ценность представляет возможность интеграции чат-ботов в различные коммуникационные каналы — от мессенджеров до корпоративных систем. Это позволяет создать единую систему защиты, охватывающую все точки контакта с потенциальными жертвами мошенников. Кроме того, чат-боты могут выполнять превентивную функцию, информируя пользователей о новых схемах мошенничества и правилах кибербезопасности в ходе обычных диалогов. Такой подход превращает систему защиты в активный инструмент профилактики преступлений.

Модель работы чат-бота следующая:

1) Сбор информации от пользователя
2) Обработка и анализ
3) Расчет результатов
4) Вывод и рекомендации

Сбор информации

После запуска (инициализации) чат-бота и нажатия кнопки /start выводит сообщение: «Привет! Я помогу тебе определить, является ли сообщение подозрительным.\n» «Пожалуйста, отправь мне текст сообщения.»

Под текстом сообщения подразумевается текст СМС, сообщений из соцсетей, текст писем из электронной почты или примерное описание слов из звонка.

Текст пользователь может писать в любом регистре на русском языке с или без соблюдения правил пунктуации. В программе (коде) прописан обработчик текста, который приводит слова в определенный формат для дальнейшей обработки (Рис. 1).

Затем чат-бот запрашивает у пользователя выбор источника: звонок, почта, СМС, соцсети, веб-сайт (Рис. 2).

Далее идет запрос уровня доверия к источнику, например, в случае корпоративной почты — адрес с того же домена (i.ivanov@kasperskiy.ru или a.ivanov@kasperskiy.ru), уровень доверия запрашивается по сто бальной шкале (Рис. 3).

Обработка и анализ

Математическая модель данной программы следующая:

$$Result = Abs\ (100 — (S * 4 + K + D),$$

где result — число, обозначающее степень опасности, abs — модуль, S — количество совпадений слов, K — коэффициент источника, D — уровень доверия.

Для подсчета количества совпадений ключевых слов прописан следующий код (Рис. 4).

Совпадения считаются по базе ключевых слов, прописанных заранее. База ключевых слов пополняется актуальными элементами на постоянной основе.

Далее выбор источника сообщения переводится в коэффициент в соответствии с заранее выбранным коэффициентом риска, а также предлагается первое решение по проблеме пользователя (Рис. 5).

Выбор коэффициентов:

Звонок = 25, почта = 30, СМС = 25, Соцсети = 28, Веб-сайт = 29.

При выборе первого источника (звонок) далее предлагается ввести номер телефона, с которого был произведен звонок. Этот номер ищется по базе номеров (Рис. 6) уже известных как мошеннических, а также предположительно мошеннических согласно предложенному подходу. При совпадении — выводится сообщение пользователю с рекомендацией игнорировать звонок. Если номера нет в базе, то применяется алгоритм просчета вероятности того, является ли этот номер мошенническим. В ином случае выводится сообщение с рекомендацией связаться с человеком через другие каналы связи (Рис. 7).

```
# Функция обработки текста сообщения
def handle_message(update: Update, context: CallbackContext) -> int:
    text = update.message.text.lower()
```

Рис. 1. Обработчик введенного текста

```
update.message.reply_text("Какой был источник этого сообщения?")
update.message.reply_text("1 - Звонок\n2 - Почта\n3 - СМС\n4 - Соцсети\n5 - Веб-сайт")
```

Рис. 2. Виджет для выбора источника

```
# Обработчик уровня доверия
def trust_level(update: Update, context: CallbackContext) -> int:
    update.message.reply_text("Насколько по 100-балльной шкале Вы доверяете этому источнику? (от 0 до 100)")
    return TRUST_LEVEL
```

Рис. 3. Обработчик уровня доверия

```
# Подсчет количества совпадений ключевых слов
matches_count = sum(1 for keyword in KEYWORDS if keyword in text)
context.user_data['matches_count'] = matches_count
```

Рис. 4. Код для подсчета количества ключевых слов

```python
# Обработчик выбора источника
def choose_source(update: Update, context: CallbackContext) -> int:
    user_choice = int(update.message.text)

    if user_choice == 1:
        update.message.reply_text("Пожалуйста, напишите номер телефона без кода страны:")
        return PHONE_NUMBER

    elif user_choice == 2:
        update.message.reply_text("Игнорируйте данное сообщение и/или свяжитесь с человеком по другой линии связи.")
        return trust_level(update, context)

    elif user_choice == 3:
        update.message.reply_text("Игнорируйте данное сообщение и/или свяжитесь с человеком по другой линии связи.")
        return trust_level(update, context)

    elif user_choice == 4:
        update.message.reply_text("Игнорируйте данное сообщение.")
        return trust_level(update, context)

    elif user_choice == 5:
        update.message.reply_text(
            "Вы можете проверить сайт на мошенничество через данный ресурс: https://www.virustotal.com/gui/home/url")
        return trust_level(update, context)

    else:
        update.message.reply_text("Пожалуйста, выберите правильный вариант источника.")
        return SOURCE
```

Рис. 5. Обработчик выбора источника

```python
# Обработчик ввода номера телефона
def input_phone_number(update: Update, context: CallbackContext) -> int:
    phone_number = update.message.text
    if not re.match(r"^\d{10}$", number):  # Проверка формата номера (10 цифр)
        await update.message.reply_text(
            "Номер должен содержать только цифры и быть длиной 10 символов. Попробуйте ещё раз:")
        return PHONE_NUMBER_CHECK

    full_number = f"+7{number}"  # Предположим, что код страны +7
```

Рис. 6. Обработчик ввода номера телефона

```python
if full_number in phone_numbers_db:
    contact_info = phone_numbers_db[full_number]
    await update.message.reply_text(f"Данный номер известен как: {contact_info}")
else:
    await update.message.reply_text("Не удалось найти информацию об этом номере.")
    return PHONE_NUMBER_CHECK
```

Рис. 7. Результат анализа номера телефона

```python
# Обработчик результата
def calculate_result(update: Update, context: CallbackContext) -> int:
    try:
        trust_level = int(update.message.text)
        if not (0 <= trust_level <= 100):
            raise ValueError
    except ValueError:
        update.message.reply_text("Пожалуйста, укажите число от 0 до 100.")
        return TRUST_LEVEL
```

Рис. 8. Обработчик результата доверия к источнику

Далее анализиурется уровень доверия к источнику (Рис. 8).

Выводы и результаты

Собрав информацию от пользователя, обработав и проанализировав ее, выводится результат по алгоритму на основе математической модели, описанной выше (Рис. 9).

На основе численного результата выводятся следующие рекомендации (Рис. 10).

После вывода рекомендации прописано заключительное слово (Рис. 11).

Заключение

Разработанный чат-бот представляет собой инновационное решение в сфере защиты от мошенничества, объединяя в себе передовые технологии искусственного интеллекта и глубокого анализа данных. Его внедрение позволяет существенно повысить уровень безопасности пользователей благодаря:

Проактивной защите: Чат-бот не просто реагирует на уже известные схемы мошенничества, но и способен предвидеть новые угрозы на основе анализа поведения звонящих и характерных паттернов общения.

Повышению точности распознавания: Использование алгоритмов машинного обучения позволяет достигать высокой точности в определении мошеннических звонков, минимизируя количество ложных срабатываний.

Оперативности реагирования: Мгновенная обработка входящих звонков и определение потенциальной угрозы обеспечивает защиту пользователя в режиме реального времени.

Обучению и адаптации: Способность чат-бота к постоянному обучению на основе новых данных позволяет ему становиться всё более эффективным в выявлении мошеннических схем.

Комплексному подходу: Интеграция с существующими системами безопасности и возможность работы как самостоятельный инструмент защиты расширяет его функциональность.

```
matches_count = context.user_data.get('matches_count')
source = int(context.user_data.get('source'))
result = abs(100 - (matches_count * 4 + {
    1: 25,
    2: 30,
    3: 25,
    4: 28,
    5: 29
}.get(source, 0)) + trust_level)
```

Рис. 9. Алгоритм расчета результата

```
if result >= 74:
    update.message.reply_text("Это мошенники! Смените пароли, заново заведите двухфакторную аутентификацию.")
elif result >= 52:
    update.message.reply_text("Большая вероятность, что это мошенники. Будьте бдительны и осторожны!")
else:
    update.message.reply_text(
        "Есть небольшая вероятность, что это мошенники. Перепроверьте источник, действуйте на свой страх и риск!")

return ConversationHandler.END
```

Рис. 10. Вывод рекомендаций

```
# Функция завершения разговора
def cancel(update: Update, context: CallbackContext) -> int:
    update.message.reply_text("До свидания! Если у вас возникнут новые подозрения, обращайтесь снова.")
    return ConversationHandler.END
```

Рис. 11. Функция завершения диалога

Однако важно понимать, что чат-бот является частью комплексной системы защиты, и его эффективность максимальна при использовании в сочетании с другими методами борьбы с мошенничеством:

- Проверка по базам данных
- Анализ поведения звонящего
- Обучение пользователей
- Взаимодействие с правоохранительными органами
- Для достижения максимальной эффективности рекомендуется:
- Регулярно обновлять базы данных
- Настраивать параметры анализа под актуальные угрозы
- Обеспечивать техническую поддержку системы
- Собирать и анализировать обратную связь от пользователей

Внедрение такого чат-бота может стать значительным шагом в борьбе с мошенничеством, существенно повысив уровень защиты пользователей и снизив риски финансовых потерь. При этом важно продолжать развитие и совершенствование подобных систем, учитывая постоянно меняющиеся методы и тактики мошенников.

В перспективе развитие подобных технологий может привести к созданию ещё более совершенных систем защиты, способных не только предотвращать мошенничество, но и прогнозировать появление новых схем обмана, обеспечивая упреждающую защиту интересов пользователей.

ЛИТЕРАТУРА

1. Красовская Н.Р., Гуляев А.А. К вопросу о кибермошенничестве // Вестн. Удм. ун-та. Социология. Политология. Международные отношения. 2022. Т. 6, вып. 1. С. 133–138. https://doi.org/10.35634/2587-9030-2022-6-1-133-138 (дата обращения: 21.03.2025).
2. Старостенко Олег Александрович. Профилактика и предупреждение кибермошенничества // Наука. Образование. Современность / Science. Education. The present. 2020. №1-2. URL: https://cyberleninka.ru/article/n/profilaktika-i-preduprezhdenie-kibermoshennichestva (дата обращения: 21.02.2025).
3. Пикалов Павел Александрович, Бортников Сергей Петрович. Кибермошенничество с использованием искусственного интеллекта // АВБсП. 2024. №2. URL: https://cyberleninka.ru/article/n/kibermoshennichestvo-s-ispolzovaniem-iskusstvennogo-intellekta (дата обращения: 20.02.2025).
4. Кулев В.К., Папшева Е.В., Старинский А.Ю., Сугробова К.С. Телефонное мошенничество // НиКа. 2010. №. URL: https://cyberleninka.ru/article/n/telefonnoe-moshennichestvo (дата обращения: 21.02.2025).
5. Тюхтин Дмитрий А. Противодействие телефонному мошенничеству // Правовой альманах. 2025. №1 (41). URL: https://cyberleninka.ru/article/n/protivodeystvie-telefonnomu-moshennichestvu (дата обращения: 20.02.2025).
6. Демидова-петрова Елизавета Викторовна, Зотина Елена Владимировна. Телефонное мошенничество: современные угрозы и вызовы // Всероссийский криминологический журнал. 2024. №4. URL: https://cyberleninka.ru/article/n/telefonnoe-moshennichestvo-sovremennye-ugrozy-i-vyzovy (дата обращения: 20.02.2025).
7. Ущерб от IT-преступлений в 2024 году уже достиг 99 млрд рублей — Текст электронный // Ведомости. URL: https://www.vedomosti.ru/society/articles/2024/09/04/1059854-uscherb-ot-it-prestuplenii-dostig-99-mlrd-rublei (дата обращения 20.02.2025)
8. Защита от нежелательных спам-звонков и мошенников с услугой МТС «Защитник» — Текст электронный // МТС Медиа. URL: https://media.mts.ru/internet/201326-usluga-mts-zashchitnik/ (дата обращения 20.02.2025)
9. Правительство внесет в Думу три десятка мер по борьбе с телефонным мошенничеством — Текст электронный // Интерфакс. URL: https://www.interfax.ru/russia/1008795 (дата обращения 21.02.2025)
10. Россиянам рассказали, почему опасно пользоваться «серыми» SIM-картами — Текст электронный // Газета.ру. URL: https://www.gazeta.ru/social/news/2023/05/26/20524874.shtml (дата обращения 21.02.2025)

Журнал «Современная наука: актуальные проблемы теории и практики»