ТЕХНОЛОГИИ
ФЕДЕРАЛЬНЫЙ ПРОЕКТ

ФОНД СОДЕЙСТВИЯ ИННОВАЦИЯМ

СтС-628343

ФИШКА — AI-сервис защиты от мошенников

Асташев Никита Геннадьевич

Проблема

Масштаб проблемы:

1. В 2025 году объем похищенных мошенниками средств составил 29,3 млрд рублей, что на 6,4% выше показателя 2024 года (27,5 млрд рублей), говорится в обзоре Банка России.[1]

2. За 2025 год, по оценке «Сбера», кибермошенники похитили у россиян 275–295 млрд руб.[2]

Три ключевые проблемы:

1.Пользователь не всегда способен распознать мошенничество во время звонка: злоумышленники используют давление, срочность, авторитет банков, полиции и родственников, а также новые схемы с ИИ-голосами.

2.Определители номера и антиспам-приложения не анализируют содержание разговора, SMS-коды, ссылки и контекст угрозы одновременно.

3.Синтезированные ИИ-голоса: мошенники могут имитировать голос родственника, чтобы вызвать доверие и заставить человека действовать срочно.

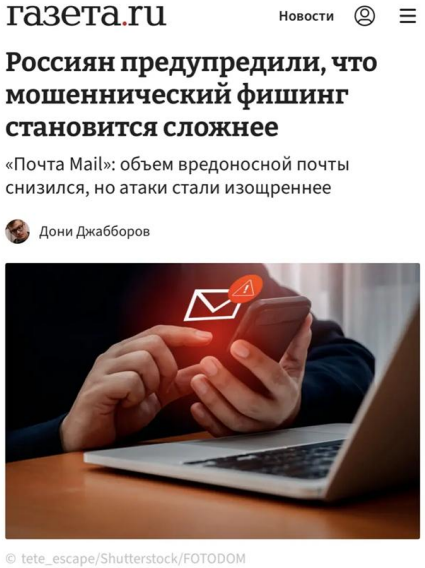

kommersant.ru

Коммерсантъ Вход

В МВД предупредили о распространении фишинговых ссылок на ложный «сайт СКР»

Преступники распространяют фишинговые ссылки в профильных чатах, в которых общаются жертвы мошенников. Пользователей чаще всего заманивают по ссылкам обещаниями компенсаций за украденные средства или якобы для перерасчета выплат участникам СВО. Об этом сообщили в УБК МВД.

«Через ботов распространяются ссылки на поддельные сайты и фальшивые каналы, оформленные под официальные ресурсы,— сообщили в полиции.— Злоумышленники копируют реальные новости и дополняют их "контактами для связи"».


газета.ru Новости

Россиян предупредили, что мошеннический фишинг становится сложнее

«Почта Mail»: объем вредоносной почты снизился, но атаки стали изощреннее

Дони Джабборов

© tete_escape/Shutterstock/FOTODOM

В первом квартале 2026 года количество заблокированных вредоносных писем снизилось на 5,6% по сравнению с 2025 годом и составило 6,7 млрд, а самыми популярными оказались письма под видом уведомлений от госсервисов с угрозой о штрафах и сообщениями о задолженностях. Об этом говорится в поступившем в «Газету.Ru» совместном исследовании «Почты Mail», «МегаФона» и «Лаборатории Касперского».

1. https://www.interfax.ru/business/1072685
2. https://www.rbc.ru/finances/29/01/2026/697b2a379a7947671694187e

О ПРОДУКТЕ

Функциональные модули ФИШКИ:

1.Номер — проверка по нескольким источникам и жалобам пользователей.

2. SMS — определение одноразовых кодов и опасных сообщений.

3. Ссылки — проверка фишинга через VirusTotal, Google Safe Browsing, URLhaus.

4. Email — проверка подозрительных адресов и доменов.

5. Разговор — анализ мошеннических фраз, давления, авторитета, просьб о кодах и переводах.

6. Тревога — автоматическое уведомление доверенных контактов при высоком риске

7. ИИ-голос —модуль выявления синтезированной речи и голосовой подмены.

Ключевой особенностью сервиса ФИШКА является разрабатываемое Android-приложение, которое позволит перехватывать звонки до ответа и автоматически расшифровывать разговоры без участия пользователя. Это превратит ФИШКУ из инструмента ручной проверки в полноценную систему пассивной защиты.

Технологический стек: Python 3.12, FastAPI, SQLite, Redis, Nginx, Ubuntu 24.04 LTS.

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

Этап 1 (апрель 2026) — Запуск MVP:

Развёрнут продакшн-сервер на VPS с доменом fishka-protect.ru и SSL-сертификатом.

Активированы все 7 модулей защиты. Настроен Telegram-бот @fishka_zashita_bot.

Результаты тестирования:

Проверка номера из мошеннической базы: Risk Score 96/100, система корректно определила угрозу.

Легитимный номер Yota: Risk Score 34/100 — вердикт ЧИСТО.

Фишинговая ссылка sberbank-online-secure.xyz: 1 из 95 антивирусов, Risk Score 100/100.

Сценарий мошеннического разговора: Risk Score 100/100, тревога доверенному контакту отправлена автоматически. Это подтверждает ключевую механику продукта — защиту в момент риска.

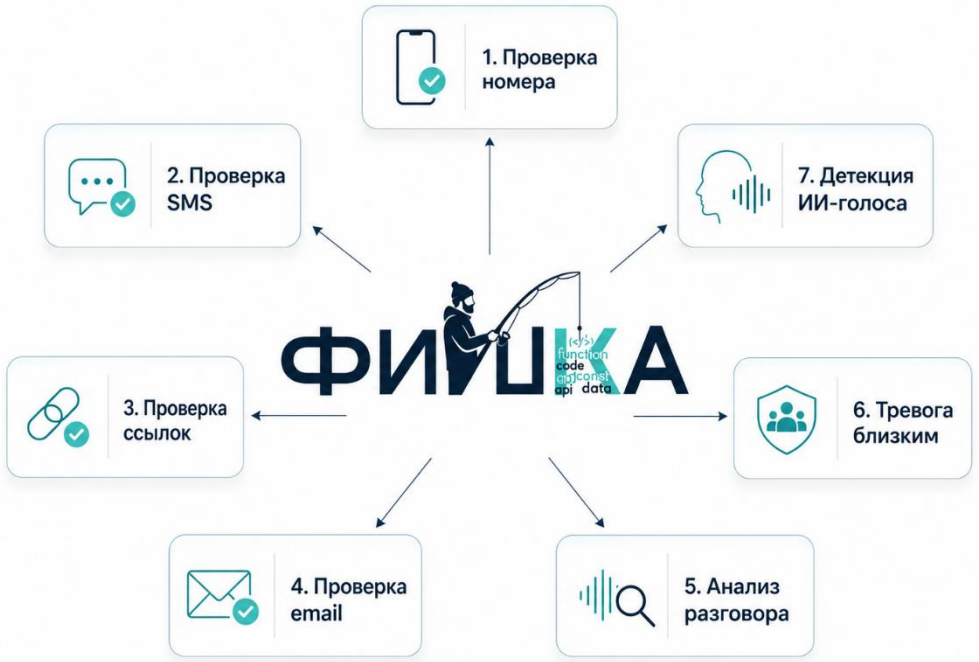
Redis кэш: повторный запрос возвращает результат мгновенно без обращения к API.

Telegram-бот: команды /start, /check, /stats, /connect функционируют корректно.

Проверены ключевые сценарии:

- подозрительный номер;
- безопасный номер;
- фишинговая ссылка;
- SMS с кодом;
- мошеннический разговор;
- автоматическая тревога родственнику/доверенному контакту.

ТЕХНОЛОГИЧНОСТЬ СТАРТАП-ПРОЕКТА



Сканируйте qr код или перейдите по ссылке **fishka-protect.ru**, чтобы протестировать возможности сервиса

Дополнительное технологическое преимущество — разрабатываемая интеграция методов детектирования синтезированных ИИ-голосов на основе нейронных сетей. Это позволит предупреждать пользователя о возможной имитации голоса родственника или представителя организации.

Уникальность ФИШКИ:

Ключевое отличие ФИШКИ — не просто определение номера, а анализ содержания угрозы: разговор, SMS-коды, ссылки, email, жалобы и поведенческие признаки объединяются в единый Risk Score.

MVP протестирован: продакшн-сервер fishka-protect.ru активен, Telegram-бот работает, все модули защиты функционируют.

АНАЛОГИ И КОНКУРЕНТЫ

Прямых конкурентов не выявлено:

ГИС Антифрод: для банков, закрыта.
ФИШКА: открытый сервис.

Сбер «Близкие рядом»: только финансы. ФИШКА: анализирует разговор.

Яндекс / GetContact: определитель.
ФИШКА: автоматическая тревога.

	ГИС Антифрод	Яндекс / GetContact	Сбер «Близкие рядом»	ФИШКА ✦
База номеров	Большая (гос.)	500+ млн номеров	Большая (банк)	Открытые API + своя пополняемая
Доверие бренда	Государственный	Высокое	Высокое	Стартап
Автоперехват звонков	✗	✓	✗	В разработке
Открытый доступ	✗	✓	✗	✓
Анализ разговора	✗	✗	✗	✓
Тревога близким	✗	✗	✗	✓
Проверка ссылок и SMS	✗	✗	✗	✓

Конкурентные преимущества:

Единственный продукт с анализом содержания разговора.

Многоисточниковая проверка: 3 базы для номеров + 3 для ссылок + 3 для email.

Реальный продакшн с работающим сервером и Telegram-ботом.

Минимальная инфраструктура: 364 руб/мес.

Технологический барьер: 200+ фраз мошенников на основе баз ЦБ РФ и МВД.

РЫНОК И ПОТРЕБИТЕЛЬ

Целевой рынок — Россия и СНГ:

Десятки миллионов семей в России сталкиваются с риском телефонного и цифрового мошенничества. Основной платящий сегмент — взрослые пользователи, которые хотят защитить себя, родителей и близких.

Рынок кибербезопасности для физических лиц в России:

2023 год: 85 млрд рублей.

2025 год: прогноз 130 млрд рублей (+53%).

2027 год: прогноз 200 млрд рублей.

Потери граждан от телефонного мошенничества (данные ЦБ РФ):

2022 год: 14,2 млрд рублей.

2023 год: 15,8 млрд рублей.

2024 год: 27,5 млрд рублей (+74% к 2023 году).

- **TAM:** рынок защиты физических лиц от цифрового мошенничества в России и СНГ.
- **SAM:** семьи, использующие смартфоны, Telegram и мобильный банкинг.
- **SOM:** первые 10 000–50 000 платных семейных подписок через RuStore, Telegram и партнёрства.

ПЛАН РЕАЛИЗАЦИИ ПРОЕКТА

Достигнуто (апрель 2026):

Продакшн-сервер fishka-protect.ru с HTTPS, firewall и защитой.

7 модулей защиты: номер, SMS, ссылки, email, разговор, тревога, история.

Telegram-бот с регистрацией, /check, /stats, /connect.

Q2 2026:

Ключевой особенностью сервиса ФИШКА является разрабатываемое Android-приложение, которое позволит перехватывать звонки до ответа и автоматически расшифровывать разговоры без участия пользователя. Это превратит ФИШКУ из инструмента ручной проверки в полноценную систему пассивной защиты.

Q3 2026:

Запуск платных тарифов. 1 000 платных пользователей. Партнёрства с банками.

Q4 2026:

10 000+ пользователей. Корпоративный API. Выход на рынки СНГ.

КВАЛИФИКАЦИЯ ЗАЯВИТЕЛЯ

Лидер команды / специалист по информационной безопасности
Координирует команду и также участвует в разработке backend-части сервиса. Отвечает за то, чтобы система эффективно выявляла фишинг, мошеннические звонки, SMS, ссылки и другие цифровые угрозы.
Ключевые навыки: backend-разработка, управление командой, информационная безопасность, анализ мошеннических схем, прототипирование, презентация проекта.
Финалист Акселератора Алтай-Азия 2025

Разработчик
Участвует в разработке backend-части антифишингового сервиса: пишет и тестирует код, помогает обрабатывать данные и внедрять механизмы выявления мошеннических угроз.
Ключевые навыки: backend-разработка, тестирование, анализ данных, основы информационной безопасности.
Финалист Акселератора Алтай-Азия 2024

Фронтенд-разработчик
Отвечает за интерфейс и пользовательскую часть сервиса: разрабатывает удобные экраны, помогает адаптировать продукт под мобильное приложение и делает взаимодействие с системой простым и понятным.
Имеет образование в сфере информационной безопасности, опыт разработки мобильных приложений, дизайна и участия в стартап-проектах.
Ключевые навыки: frontend-разработка, мобильные приложения, UI/UX-дизайн, информационная безопасность, стартап-проекты.
Участник ТОП-50 программы «Стартап как диплом» 2025г.
Финалистка Акселератора Алтай-Азия 2024

Планируемое расширение команды
Для развития проекта планируется привлечение дополнительных специалистов: маркетолога, аналитика, продуктового менеджера. Это поможет усилить продвижение сервиса, глубже изучать целевую аудиторию, анализировать мошеннические сценарии и быстрее выводить продукт на рынок.

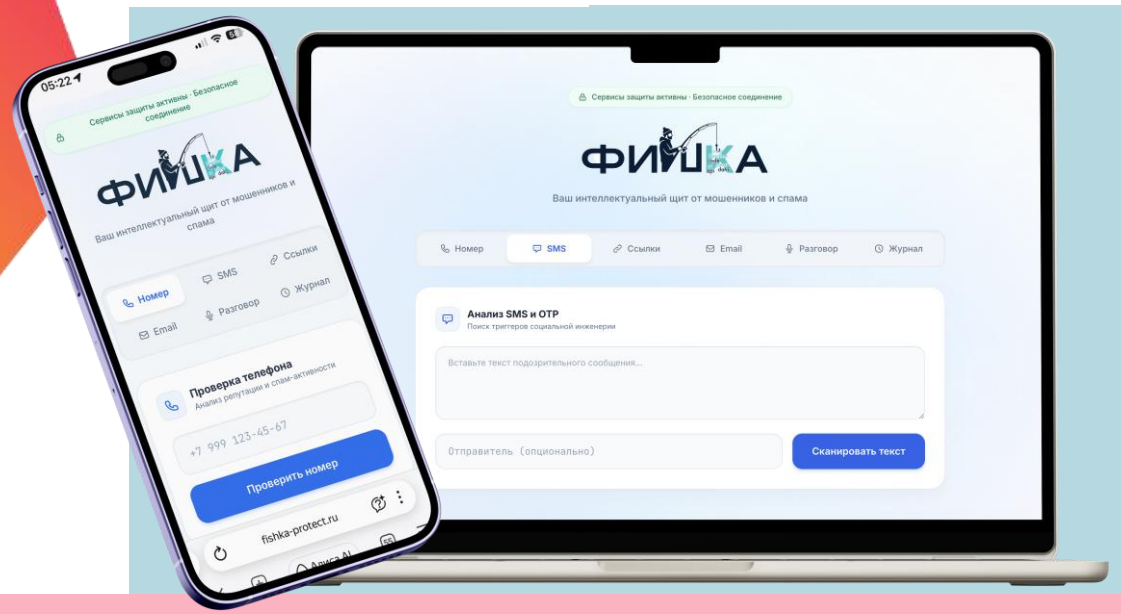
ТЕХНОЛОГИИ
ФЕДЕРАЛЬНЫЙ ПРОЕКТ

ФОНД СОДЕЙСТВИЯ ИННОВАЦИЯМ

Спасибо за внимание!

СтС-628343
Асташев Никита Геннадьевич

89293913080
nikita-astashev@mail.ru



ПЛАТФОРМА УНИВЕРСИТЕТСКОГО ТЕХНОЛОГИЧЕСКОГО ПРЕДПРИНИМАТЕЛЬСТВА