Яндекс

Антифишинг в Яндекс Браузере

Александр Ульянов, руководитель группы

Фишинговый сайт

- фальшивый ресурс, маскирующийся под легитимный, чтобы обманом получить данные или деньги пользователя.

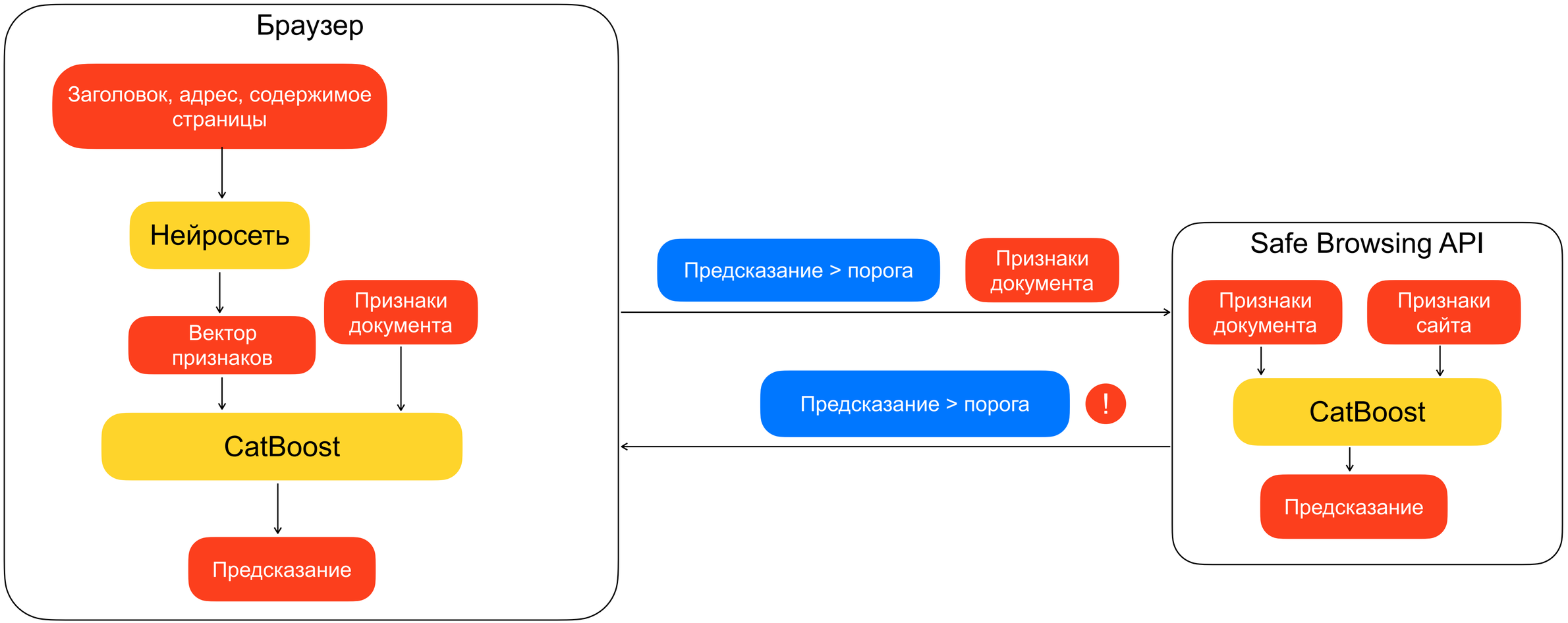
Популярные категории фишинга

- Инвестиции
- Голосования
- Авторизация в мессенджерах
- Оплата на онлайн-сервисах и маркетплейсах
- Личные кабинеты банков
- Лотереи

Использование машинного обучения для борьбы с фишингом

- Высокие точность и полнота
- Анализ большого объема данных
- Скорость выявления
- Выявление сложных закономерностей

Схема работы метода в Браузере



Сбор данных

- Поиск фишинговых сайтов

1. Жалобы пользователей
2. Обмен вердиктами с партнерами
3. Разметка обученными специалистами

- Автоматическое аннотирование

1. Получение содержимого сайтов
2. Использование активности пользователей
3. Вычисление признаков

Сложности сбора данных

Фишинговый сайт активен короткое время, за которое нужно его обнаружить и собрать нужные для обучения данные.

Необходимо получить данные идентичные показанным пользователю.

Обучение моделей

› Нейросеть

1. Модель на базе архитектуры DSSM
2. Используется адрес, заголовок и содержимое страницы
3. Модель преобразует текст в вектор признаков

› Градиентный бустинг (CatBoost)

1. Вектор признаков DSSM
2. Признаки документа
3. Признаки сайта

Признаки документа

- Наличие ключевых фишинговых фраз
- Наличие внешних ссылок, скриптов, картинок с других доменов
- Формы ввода паролей, данных карты и проверка ввода
- Использование в имени сайта названий известных компаний

Признаки сайта

- Посещения из поисковой системы
- Количество посетителей в Браузере
- Прямые заходы через адресную строку
- Возвращаемость пользователей на сайт
- Проведенное время на сайте
- Уникальность текста
- Наличие исходящего трафика с сайта
- Отказ скачивания сайта поисковым роботами

Асинхронный контур

- Применение сложных моделей
- Обогащение данных
- Интеграция всех данных

Фишинговые сайты избегают обнаружения

Качество метода обнаружения

- Точность метода по результатам внутреннего тестирования: 99.9%
- Метод выявляет более 1500 фишинговых сайтов ежедневно.

- По данным независимого исследования ГК Softline, настольная версия Яндекс Браузера обнаружила 69 из 100 новых фишинговых сайтов.

Яндекс

Спасибо

Александр Ульянов

руководитель группы

 ulyanov@yandex-team.ru