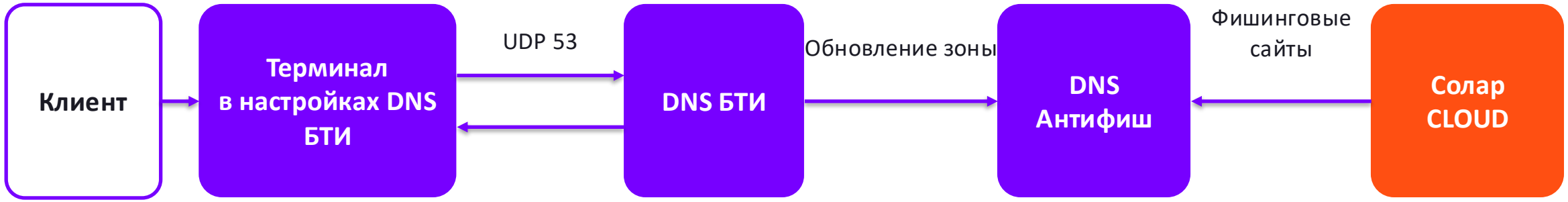
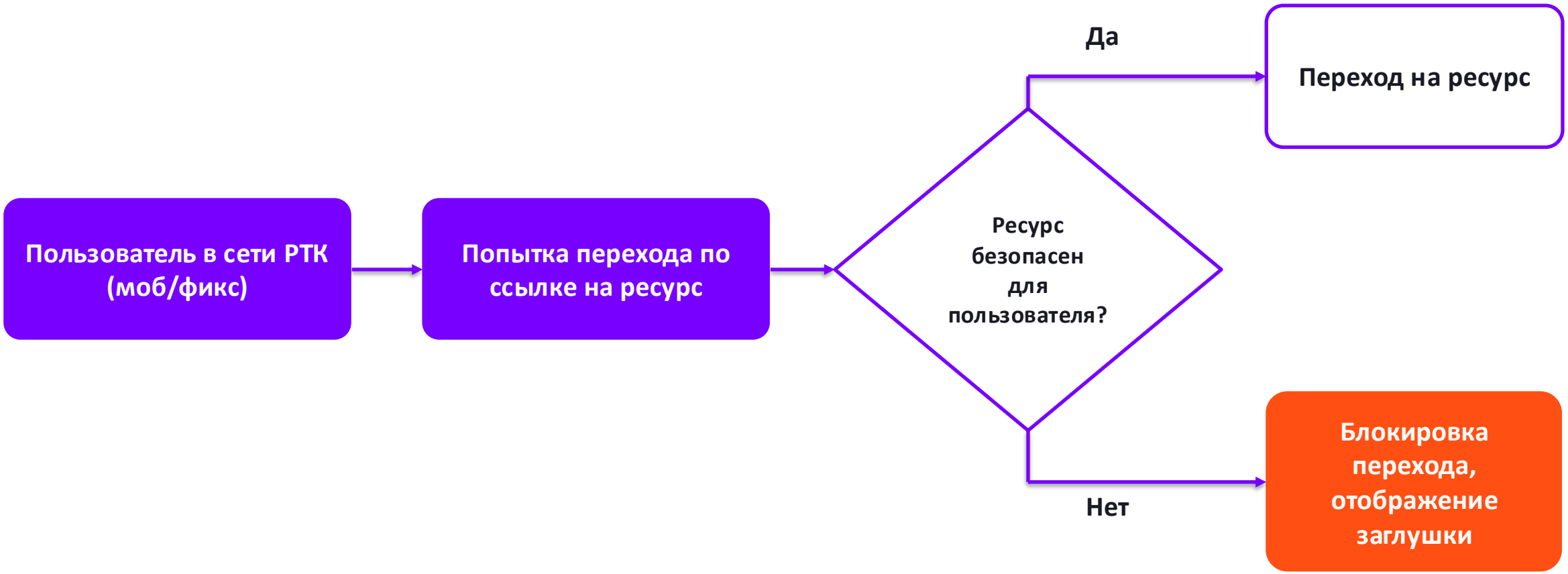
Антифишинг: реализация сервиса

Архитектура решения



На терминал клиента не устанавливается ПО. Терминал отправляет DNS-запросы на серверы DNS РТК, которые выдаются автоматически при подключении к интернету.

CJM сценария блокировки перехода



Что видит клиент при блокировке перехода

1

Понятная заглушка

Клиент получает объяснение, почему переход на ресурс был заблокирован

2

Перечень рисков

Вредоносное ПО, фишинг, незаконный сбор данных и другие угрозы

3

Рекомендация

Воздержаться от посещения ресурса — безопасность в интернете в приоритете

Уважаемый абонент!

Мы заблокировали переход на данный ресурс, так как он представляет угрозу для Вашей безопасности в интернете.

Возможные риски включают в себя:

- вредоносное ПО (вирусы, трояны и т. д.)
- фишинговые атаки (попытки мошенничества)
- незаконный сбор личной информации
- продажа или распространение запрещённых веществ
- пропаганда расизма, терроризма

Для Вашей безопасности рекомендуем воздержаться от посещения данного web-ресурса.

Результаты проекта и экономический эффект

5 млн+

попыток перехода на фишинговые и вредоносные ресурсы предотвращено с декабря 2025 (400 тыс. — за первый месяц)

99,95%

точность блокировки

15–18 с

от активации системы до определения угрозы с вероятностью 99,9%

≈10 ×

Операционная эффективность

Предзаписанные алгоритмы вместо прямого обращения к ИИ-агентам снижают стоимость обработки данных примерно в 10 раз: миллионы событий в реальном времени без роста затрат на инфраструктуру

0 ₽

Социальный эффект

Сервис бесплатен для абонентов и работает автоматически. Меньше успешных фишинговых атак — меньше потерь граждан и ниже нагрузка на банки и правоохранительную систему

Финансовые показатели (выручка, ROI) не раскрываются: сервис — инфраструктурный элемент, а не коммерческий продукт с прямой монетизацией.