# Adspect Documentation

Adspect

сент. 15, 2020

Содержание:

Глава 1

# Обзор

Adspect — это простой в использовании облачный сервис, предназначенный для защиты онлайн-рекламных кампаний (CPA-офферов, лэндингов) от нежелательного трафика. Под нежелательным трафиком мы понимаем:

- скликивание (кликфрод), повсеместно распространенное в медийных рекламных сетях и popunder-сетях;
- модераторов рекламных сетей;
- роботов spy-сервисов («spy services» — сервисы для отслеживания чужих рекламных кампаний);
- роботов для веб-скрейпинга;
- роботов для подбора паролей;
- роботов антивирусных компаний;
- и другие разновидности нецелевых или откровенно враждебных посетителей.

Мы работаем со всеми источниками трафика, как существующими, так и теми, которые только появятся в будущем — наши алгоритмы фильтрации трафика абсолютно универсальны и одинаково эффективно обрабатывают любой трафик, откуда бы он ни поступал. Мы работаем с ведущими рекламными сетями, в том числе:

- Google Ads
- Microsoft Advertising (Bing Ads)
- Facebook
- Instagram
- VK
- Яндекс.Директ и РСЯ
- myTarget
- ZeroPark
- ExoClick

- Taboola
- MGID
- PropellerAds
- TrafficStars
- и сотнями других

Мы защищаем ваши лэндинги и офферы от различных антивирусных, ИБ и скоринговых компаний, в том числе:

- GeoEdge
- Adscore
- Google Safe Browsing
- Kaspersky Labs
- Avast
- Forcepoint
- и многих других

Дополнительная информация по основным вопросам представлена в нашем FAQ.

Мы поддерживаем несколько типов интеграции, которые отличаются техническими деталями, но все предоставляют одинаково высокий уровень защиты трафика:

- PHP-интеграция при помощи отдельного файла `index.php`;
- JavaScript-интеграция при помощи HTML-тега `<script>`:
  - Пассивный режим без клоакинга, как Google Analytics — подходит для сбора статистики по ботам;
  - Клоакинг при помощи JavaScript-редиректа на целевую страницу методом `location.replace()`;
  - Клоакинг при помощи наложения iframe на белую страницу без редиректа.

## 1.1 PHP-интеграция

В PHP-интеграции разделение трафика осуществляется при помощи специального файла, именуемого здесь и далее `index.php`, который вы размещаете в папке лэндинга или в любом другом месте, доступном по протоколу HTTP. Этот файл выступает в роли точки входа для вашего трафика и работает в паре с нашими серверами, которые уже непосредственно выполняют фильтрацию. В зависимости от принятого нашими фильтрами решения, посетитель может быть направлен на ваш контент (оффер, лэндинг) или на так называемую «белую страницу» — страницу, которая не содержит никакого чувствительного к несанкционированному доступу содержимого. Другими словами, Adspect выступает в роли промежуточного этапа на пути прохождения трафика, осуществляя отсев нежелательных посетителей от целевых в реальном времени.

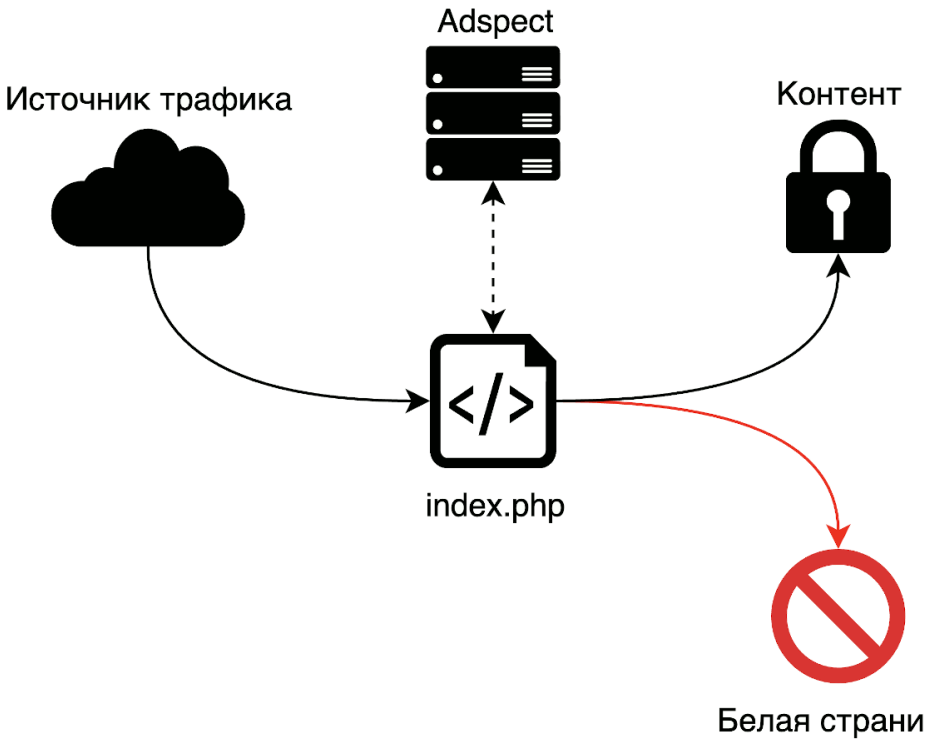


Схема прохождения трафика

Несколько одинаковых файлов `index.php` могут использоваться параллельно для защиты нескольких офферов или лэндингов, при этом не мешая друг другу.

## 1.2 JavaScript-интеграция

JavaScript-интеграция предназначена в первую очередь для использования со сторонними сервисами, такими как Shopify, Tilda и OpenCart, где вы не можете загрузить наш файл `index.php` для PHP-интеграции. Она также позволяет вам использовать более защищенную и аутентичную с точки зрения рекламных сетей схему клоакинга, в которой посетитель сразу попадает на белую страницу, а переход на целевой контент происходит при помощи JavaScript после одобрения нашей системы. Такой режим особенно желателен при работе с Facebook и Google Ads.

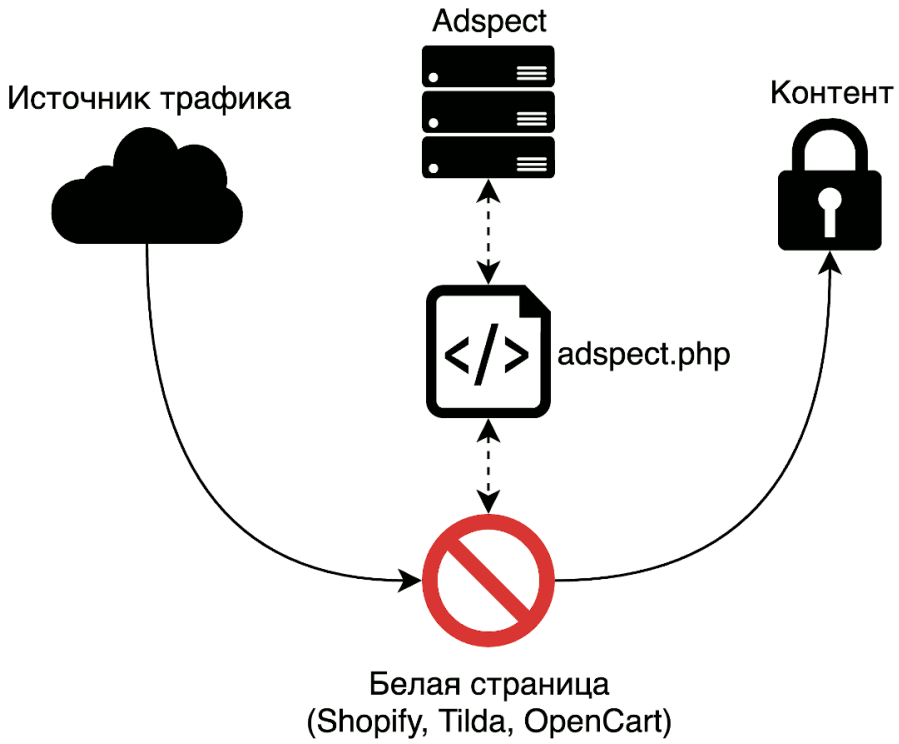


Схема прохождения трафика

Вам также потребуется загрузить и разместить на сервере наш PHP-скрипт `ajax.php`, но его конкретное расположение не имеет значения, так как файл будет подключен к белой странице через HTML-тег `<script>`. Когда посетитель попадает на белую страницу, тег `<script>` обращается к удаленному файлу `ajax.php`, который отдает наш JavaScript-код для фильтрации. Дальнейшее поведение зависит от режима работы, выбранного при интеграции:

- В пассивном режиме обновляется статистика Adspect, но никаких действий не предпринимается — посетитель останется на белой странице. Этот режим похож на Google Analytics и предназначен для пассивного сбора аналитической информации по ботам в трафике в тех случаях, когда клоакинг не требуется.
- В режиме JavaScript-редиректа благонадежные по мнению наших фильтров посетители будут перенаправлены на страницу контента при помощи JavaScript-редиректа методом `location.replace()`. Это означает, что **URL в адресной строке изменится**.
- В режиме отображения в iframe целевые посетители увидят контент-страницу в iframe без редиректа, то есть iframe будет наложен поверх белой страницы.

## 1.3 index.php и ajax.php

`index.php` — это PHP-скрипт, который является связующим звеном между вашим хостом и нашими бэкенд-серверами. Имя файла `index.php` является лишь принятым обозначением, которое мы используем в Adspect, однако вы можете переименовывать эти файлы так, как вам угодно. Так как скрипт `index.php` написан на PHP, то это автоматически означает необходимость в хостинге с поддержкой PHP или в трекере, поддерживающем загрузку PHP-лэндингов.

Сам скрипт специально написан таким образом, чтобы быть совместимым с практически любыми хостинг-провайдерами, начиная от виртуальных хостингов и VPS и заканчивая выделенными серверами и Amazon AWS. Поддерживаются как Windows, так и Unix-подобные операционные системы, в пределах их поддержки самим PHP. PHP 7 рекомендуется, PHP 5 также поддерживается.

Единственным требованием к PHP является поддержка cURL. Вы можете проверить, поддерживается ли cURL вашей сборкой PHP, используя информацию из phpinfo; cURL поддерживается подавляющим большинством работающих ныне сборок PHP.

Файл `ajax.php` является лишь измененной версией файла `index.php`, поэтому все сказанное выше также применимо.

## 1.4 Хостинг

Мы рекомендуем использовать хостинг от Inferno Solutions из-за качественного обслуживания, ориентированности на русскоязычных клиентов и отсутствия необходимости предъявлять документы или иные личные данные (нет KYC).

Предлагаем вам воспользоваться нашими скидочными купонами:

- **ADSPECT25VPS** — скидка 25% на первый платеж для всех VPS за период 1, 3, 6 месяцев;
- **ADSPECT25SSDVPS** — скидка 25% на первый платеж для всех SSD VPS за 1, 3, 6 месяцев;
- **ADSPECT25SSDVPSRU** — скидка 25% на первый платеж для всех SSD VPS в России;
- **ADSPECT15SSDVPSPL** — скидка 15% на первый платеж для всех SSD VPS в Польше;
- **ADSPECT15DEDI** — скидка $15 на первый платеж для серверов RU-xx и NL3-xx.

## 1.5 Порядок работы

Типичный порядок работы с Adspect для защиты рекламных кампаний в партнерском маркетинге выглядит следующим образом:

1. *Создаете поток* в Adspect;
2. Выбираете подходящий вам тип интеграции и следуете соответствующим инструкциям на странице интеграции;
3. Переключаете поток в режим «Контент» и проверяете, что контент-страница отображается корректно;
4. Переключаете поток в режим «Белая страница» и проверяете, что белая страница отображается корректно;
5. Переключаете поток в режим «Фильтр» и проверяете, что нет никаких других ошибок при обработке клика;
6. Переключаете поток в режим «Модерация»;
7. Создаете рекламную кампанию, используя в качестве рекламной ссылки ссылку на файл `index.php` при PHP-интеграции или на белую страницу, в которую вы встроили наш тег `<script>`, при JavaScript-интеграции;
8. Ожидаете одобрения вашей кампании модерацией рекламной сети и переключаете поток в режим «Фильтр»;
9. Льете трафик и анализируете его показатели в разделе *«Статистика»*.

Глава 2

# Фильтрация трафика

Существует несколько подходов к обнаружению и фильтрации нежелательных посетителей в рекламном трафике. В этой главе мы рассмотрим три основных технологии автоматической фильтрации и покажем, что делает Adspect уникальным и инновационным продуктом на рынке.

## 2.1 Черные списки

Это наиболее распространенный и в то же время примитивный и наивный подход. Обычно для анализа выбирается узкий набор атрибутов посетителя (IP-адрес, заголовки HTTP-запроса и т.п.) и сверяется с заранее составленным «черным» списком этих атрибутов. Совпадение означает сигнал к блокировке. Несмотря на популярность, у этого подхода есть два существенных недостатка:

1. Черные списки никогда не являются исчерпывающими, что делает процесс их обхода тривиальным. Для обхода черных списков IP-адресов достаточно менять IP-адреса, каждый раз выбирая для проверки новый из длинного списка, как это часто и делается с помощью прокси-сервисов. Невозможно занести в черный список все, всегда останутся бреши, через которые недоброжелатели получат доступ к защищаемому контенту. Существуют целые компании, бизнес которых построен на предоставлении в аренду огромных пулов резидентских IP-адресов (т.е. выданных провайдерам домашнего Интернета), постоянно пополняемых, что делает поддержание актуального черного списка таких IP-адресов невероятно сложной, если вообще выполнимой задачей.
2. Черные списки могут быть слишком широкими в охвате, что приводит к ложноположительным срабатываниям. Это особенно актуально для черных списков адресов IPv4. Сравнительно небольшое 32-битное адресное пространство IPv4 уже исчерпано, вынуждая Интернет-провайдеров и сотовых операторов использовать NAT для объединения целых абонентских сетей за единым общим IP-адресом. Попадание одного такого адреса в крупном мегаполисе в черный список, например по подозрению в использовании в качестве прокси (да, прокси за NAT существуют), будет означать одновременную блокировку тысяч хороших, благонадежных потенциальных посетителей.

Черные списки — это самый распространенный и зачастую единственный подход, используемый сервисами клоакинга в сфере партнерского маркетинга. Пусть и оправданный в некоторых случаях, этот подход слишком грубый и ненадежный, чтобы использовать его сам по себе. Ложноотрицательные результаты такой фильтрации — наиболее частая причина «пробива клоаки». Adspect имеет массивные

встроенные черные списки IP-адресов заведомо неблагонадежных источников трафика, совокупный объем которых насчитывает порядка одного миллиарда адресов.

## 2.2 Сбор и анализ отпечатков

Сбор отпечатков, по аналогии с отпечатками пальцев, — это процесс сбора «машинных отпечатков» посетителей, которые их идентифицируют. Но, в отличие от совершенно уникальных отпечатков пальцев, машинные отпечатки не уникальны. В зависимости от алгоритма, они могут включать в себя разное число составляющих фактов. Некоторые факты встречаются очень часто, например строка user agent популярного браузера. Другие же факты, встречающиеся реже, примечательны тем, что встречаются только у всех тех нежелательных видов трафика, от которых мы защищаем своих клиентов. И мы в Adspect отлично знаем, что это за факты.

Анализ машинных отпечатков — это намного более продвинутая технология, которую используют крупные, ориентированные на бизнес-клиентов игроки на рынке защиты информации. Их услугами пользуются VAS-провайдеры (VAS — «value-added services», мобильный контент) для защиты wap-click-офферов от скликивания. Adspect первыми применили технологию сбора и анализа отпечатков в adtech-индустрии для защиты рекламных кампаний частных рекламодателей.

У нас имеется богатый опыт в анализе JavaScript-отпечатков — машинных отпечатков, составленных из многочисленных деталей среды исполнения JavaScript в браузерах посетителей. Собираемые нами отпечатки состоят в среднем из 1600–2200 различных фактов, которые показывают нам очень детальную картину внутреннего устройства программного обеспечения посетителей. Мы проверяем эти отпечатки десятками высокоточных тестов и безошибочно определяем нежелательный трафик. Мы считаем своей миссией принести сложные и дорогостоящие технологии из мира корпоративной защиты данных в мир партнерского маркетинга.

## 2.3 Машинное обучение

Машинное обучение (ML) — это широкий термин, в общем случае обозначающий алгоритмы обучения компьютеров для того, чтобы в дальнейшем использовать полученные ими знания для выполнения конкретной задачи. В плане защиты рекламного трафика машинное обучение может использоваться для оценки каждого отдельного клика с целью понять, целевой это посетитель или кто-то нежелательный. В научной среде это называется задачей классификации. И при условии наличия достаточного объема данных для обучения эта задача решается с очень высокой точностью.

Машинное обучение оказалось идеальным инструментом анализа отпечатков с их огромным набором составляющих их фактов. Adspect использует собственную технологию машинного обучения VLA™, которая постоянно обучается и точно распознает нежелательных посетителей далеко за рамками тех проверок, которые мы изначально в нее заложили. Более подробное описание технологии вы можете найти в *главе о VLA*.

Машинное обучение пока остается «высшей математикой», которую применяют лишь немногие из лидеров рынка корпоративных антифрод-систем. Adspect является первой компанией, применившей машинное обучение для решения проблем безопасности в сфере партнерского маркетинга и рекламных технологий.

## 2.4 Наш подход

Adspect использует все три описанных подхода совместно, не полагаясь целиком на какой-то один из них. Мы не держим все яйца в одной корзине. Это позволяет нам принимать точные решения с

наименьшими ложноположительными и ложноотрицательными результатами. Мы твердо уверены в том, что детальные машинные отпечатки и их анализ алгоритмами машинного обучения будут играть ключевую роль в новых adtech-проектах, направленных на защиту рекламного трафика, благодаря огромному потенциалу обеих технологий, особенно когда они применяются совместно.

# Глава 3

## VLA™

VLA™ — это аббревиатура от «Virtual Learning Appliance». Это торговое название нашей технологии машинного обучения, лежащей в основе наиболее продвинутых фильтров трафика в Adspect. Если говорить упрощенно, то это математическая машина, т.н. модель, которая проверяет входящий трафик и сама находит подозрительные повторяющиеся последовательности среди тысяч фактов в машинных отпечатках посетителей. По этим признакам она определяет модераторов, кликфрод и прочую злонамеренную активность. VLA находится в постоянном цикле самообучения, развиваясь и адаптируясь к новым угрозам по мере их появления. VLA является нашим самым мощным оружием в гонке вооружений партнерского маркетинга, так как может распознавать цели далеко за рамками тех проверок, которые мы изначально заложили. То, что человек-аналитик может упустить, никогда не ускользнет от математически точного анализа запрограммированной машины.

Принцип работы машинного обучения можно проиллюстрировать следующей аналогией. Представьте полицейского в аэропорту, которого проинструктировали задерживать всех пассажиров с определенной татуировкой, так как известно, что носящие эту татуировку принадлежат к опасной банде. За последний месяц полицейский задержал десять человек с татуировкой и заметил, что все они также были одеты в футболки с таким же символом. Он сделал выводы и теперь будет также останавливать других пассажиров в таких футболках вне зависимости от того, есть у них татуировка или нет.

В то время, как наши обычные проверки отпечатков дают очень близкую к 100% точность определения нежелательных посетителей, VLA является по своей природе вероятностной системой. Реальная ценность VLA в том, что стандартные проверки охватывают лишь заранее известные нам типы угроз, но VLA обнаруживает новые, ранее не известные нам образцы. Система получает на вход отпечаток, анализирует каждый факт в его составе и выдает процент уверенности в его опасности, как будто говоря: «я на 97% уверена в том, что это отпечаток опасного посетителя, и тебе лучше отфильтровать его!»

Остается лишь определить, какой процент уверенности является достаточно высоким, чтобы фильтровать. В этом вопросе решение принимаете вы. В настройках каждого потока есть параметр «Точность VLA», который предназначен как раз для этого: вы выбираете минимально необходимую уверенность VLA, при которой посетитель будет отфильтрован на белую страницу. Например, если вы указали точность в 95%, то VLA отфильтрует всех тех посетителей, в чьей опасности она уверена на 95% и более. Те же, в ком VLA сомневается меньше, будут пропущены на контент (при отсутствии других признаков опасности). Этот единственный параметр точности позволяет вам тонко настроить систему

в соответствии с вашим личным пониманием того, что значит «достаточная уверенность». Наши тесты показали, что 95% — хорошее начальное значение для точности VLA.

Глава 4

# Примеры использования

У Adspect есть несколько четко обозначенных способов применения, которые зарекомендовали себя как полезные и надежные. Здесь мы прежде всего говорим о двух взаимосвязанных, но тем не менее различных функциях Adspect: клоакинг и фильтрация ботов. Остановимся подробнее на каждой.

## 4.1 Клоакинг

Клоакинг — это практика сокрытия настоящего контента, будь то лэндинг или CPA-оффер, от тех, для кого этот контент не предназначен, по единоличному усмотрению владельца контента. Мы в Adspect твердо верим, что если вы не желаете показывать ваш контент кому-либо, то вы должны иметь возможность ограничить доступ, вне зависимости от ваших причин. И мы даем вам инструмент для этого. В частности, это означает сокрытие ваших лэндингов от модераторов рекламных сетей, spy-сервисов и роботов антивирусных компаний. Эти посетители никогда не принесут вам конверсий и денег.

## 4.2 Обнаружение ботовых площадок

Популярные форматы онлайн-рекламы, такие как баннеры, тизеры, нативная реклама и popunder, все наводнены ботами для накрутки кликов — кликфродом. Технологии, на которых строятся эти форматы (HTTP, HTML и JavaScript), позволяют относительно легко и дешево генерировать автоматические клики — достаточно выбрать любой из программируемых headless-браузеров. Неудивительно, что эти браузеры, изначально предназначенные для автоматизации тестирования веб-приложений, активно используются мошенниками для накрутки кликов в рекламных сетях, вынуждая рекламодателей платить за то, что никогда не принесет им доход.

Adspect с легкостью обнаруживает их всех. Все, что вам нужно сделать, — это указать параметр для «Sub ID» в настройках потока, как описано в главе о потоках. Если вы передадите нам идентификатор паблишера, сайта или площадки (будем называть их *источниками* здесь и далее) через параметр ссылки, то вы сможете выгружать отчеты с разбивкой по отдельным источникам, содержащие точную статистику о ботах в их трафике. Самая правая колонка отчета, «Качество», удобна для оценки и сравнения различных источников и показывает процент целевого трафика в общей массе трафика

с каждого конкретного источника. Просто выберите разбивку по «Sub ID» в поле слева от выбора часового пояса.

Проведя черту, скажем, в минимум 80% целевого трафика, вы легко сможете найти источники, удовлетворяющие этому требованию — кликните на заголовок колонки «Качество», чтобы отсортировать ее по возрастанию или убыванию. Источники с качеством выше 80% будут вашим белым списком площадок; наоборот, если вы хотите использовать черный список, то им будут источники с качеством ниже 80%. Этот простой метод поможет вам избежать больших и бессмысленных трат на составление черных и белых списков в медийной рекламе и popunder-е, как при отсеве по CR (conversion rate). Сначала офильтруйте ботовые площадки, а затем уже переходите к фильтрации по конверсиям.

## 4.3 Сокрытие источников трафика

Многие партнерские сети имеют внутренние отделы медиабаинга («media buying» — закупка рекламы), которые могут обнаружить ваши источники трафика и использовать эту информацию для кражи ваших рекламных кампаний. Поэтому источники трафика следует скрывать от партнерских сетей и любых других третьих лиц. Adspect делает это для вас, отрезая HTTP-заголовок Referer от проходящих через систему кликов, что делает невозможным тривиальное обнаружение ваших источников трафика путем анализа журналов веб-серверов в цепочке редиректов.

Глава 5

# Настройка потоков

Управление трафиком в Adspect организовано в контексте потоков. Поток — это канал прохождения трафика, которым можно управлять как единым целым, подобно кампании в рекламной сети или схеме в TDS.

Потоки управляются в разделе «Потоки» вашего личного кабинета и создаются по кнопке «Создать поток». У каждого потока есть связанные с ним файлы `index.php` и `ajax.php`, в которых закодирован ID потока. Однако вы можете изменить целевой поток для любого перехода, указав полный ID потока в параметре ссылки `__sid`:

```
https://example.com/index.php?__sid=1ea85c7c-b977-6804-8e69-00162501c2b4
```

Кликните на короткий ID потока в списке потоков, чтобы скопировать полный ID потока в буфер обмена.

Далее мы рассмотрим назначение каждой настройки в потоке.

## 5.1 Название

Название потока — это просто любое читабельное имя, которое позволит вам быстро отличить один поток от другого. Мы рекомедуем называть потоки по именам рекламных сетей и кампаний в них для сохранения ясности связей между источниками трафика и соответствующими потоками в Adspect. Мы также рекомендуем создавать отдельный поток для каждой страны, для простоты получения статистики с разбивкой по странам.

## 5.2 Режим

Это режим работы потока, главный рычаг управления. Всего есть четыре режима:

- «Фильтр» — основной режим работы любого потока, в котором мы осуществляем фильтрацию хороших посетителей от опасных в реальном времени. Все технологии фильтрации Adspect, в том числе *VLA™* , работают именно в этом режиме.

- «Модерация» — этот режим предназначен для тех моментов, когда рекламные кампании находятся на проверке у модераторов рекламных сетей. Каждому посетителю будет показана белая страница. В этом режиме доступны дополнительные функции, настройка которых будет описана ниже в этой главе.
- «Контент» — вспомогательный режим, в котором всем посетителям показывается страница с основным контентом. Режим может быть удобен для тестирования доступности контент-страницы.
- «Белая страница» — вспомогательный режим, в котором всем посетителям показывается «белая» страница. Режим может быть удобен для тестирования доступности белой страницы. Рекомендуем переводить в этот режим потоки при остановке их кампаний, так как система модерации многих рекламных сетей работает даже тогда, когда ваши кампании остановлены.

«Модерация» является режимом по умолчанию для вновь созданных потоков. Вам *следует* использовать этот режим при прохождении модерации в рекламных сетях. После того, как кампания одобрена, переключите поток в режим «Фильтр» прежде, чем сеть начнет поставлять трафик.

## 5.3 Контент

Контент — это ваш настоящий лэндинг или CPA-оффер, который вы собираетесь рекламировать. Словом, это то, что должно принести вам прибыль. Вы можете указать до 254 контент-страниц для сплит-тестирования. Трафик будет распределяться между ними в соответствии с правилами выбранного ротатора (см. «Ротатор» ниже).

Есть два типа значений, которые здесь можно указать: имя файла лэндинг-страницы или внешний URL. Имя файла страницы это наиболее предпочтительный способ отображения контента. Это имя HTML- или PHP-файла вашего настоящего лэндинга, который *должен* располагаться в той же папке, что и файл `index.php`, то есть в корневой папке вашего лэндинга. Несоблюдение этого правила поломает отображение вашего лэндинга в браузерах посетителей.

Имя файла не должно быть легко угадываемым, иначе целеустремленные модераторы или конкуренты могут его угадать, со всеми вытекающими последствиями. Выберите случайное длинное имя.

*Не называйте* файл страницы контента `index.html` или `index.htm`! Не считая того, что это легко угадываемые имена и позволяют легко «пробить клоаку», они также могут конфликтовать с вашей конфигурацией веб-сервера и привести к непредвиденным проблемам.

В сумме получается следующее: если у вас есть папка с лэндингом, основная страница которого называется `index.php` (как это часто бывает), то сначала переименуйте файл `index.php` во что-то трудно угадываемое, например `re3NBX1XtH.php`, а после создания потока скачайте наш файл `index.php` в ту же папку. Этот файл `index.php` переключит клик на целевой `re3NBX1XtH.php`, если посетитель будет расценен как благонадежный.

Вы также можете указать URL конечной страницы, например прямую ссылку на оффер из партнерской программы. Это может быть оптимально для некоторых кампаний, однако помните, что внешний URL означает лишний HTTP-редирект, со всеми вытекающими последствиями — потенциальным увеличением технических потерь трафика из-за увеличения времени обработки клика, особенно на низкокачественных рекламных форматах вроде popunder-а.

Также поддерживаются различные не-HTTP URL-ы, при помощи которых вы можете выполнять специализированные задачи на устройствах ваших посетителей. Несколько распространенных примеров:

- `mailto:user@example.com` откроет почтовую программу для составления e-mail на указанный адрес;
- `tel:+08001234567` наберет указанный номер на мобильных устройствах и некоторых десктопах с ПО для телефонии;

- `market://details?id=app` откроет страницу мобильного приложения в Google Play.

Эта функциональность особенно полезна для работы с т.н. deep-ссылками, которые ведут на контент внутри мобильных приложений.

### 5.3.1 «Парам»

«Парам» — это сокращение от «проброс URL-параметров». Если проброс параметров включен, то все параметры из входящей ссылки будут добавлены к ссылке или имени файла контент-страницы.

Допустим, ваша страница указана в виде ссылки:

```
https://example.com/?utm_campaign=sweeps
```

Посетитель переходит на файл `index.php` потока по ссылке:

```
https://tracker.test/lander/index.php?utm_medium=ppc&utm_source=search
```

Если посетитель будет посчитан благонадежным, то он будет перенаправлен на контент-страницу с объединением параметров из обеих ссылок выше:

```
https://example.com/?utm_campaign=sweeps&utm_medium=ppc&utm_content=search
```

### 5.3.2 Вес

Каждая контент-страница имеет свой абстрактный вес, который по умолчанию равен 10. Этот параметр учитывается при сплит-тестировании нескольких контент-страниц. Конкретное влияние этого параметра на распределение трафика зависит от выбранного ротатора (см. «Ротатор» ниже).

### 5.3.3 «Вкл»

Настройка «вкл» позволяет вам включать и выключать отдельные контент-страницы.

### 5.3.4 URL-макросы

Adspect поддерживает макросы для использования в полях «Контент» и «Белая страница» (а также в URL-правилах, как будет описано далее в этой главе):

- `{ip}` — IP-адрес посетителя;
- `{asn}` — номер автономной системы посетителя;
- `{agent}` — строка user agent посетителя;
- `{clickid}` — уникальный идентификатор клика (внешний из параметра ссылки, либо сгенерированный Adspect);
- `{country}` — ISO 3166-1 alpha-2 код страны посетителя;
- `{os}` — операционная система посетителя и ее версия в случае Windows и Android;
- `{browser}` — название браузера посетителя;
- `{epoch}` — Unix-время перехода;
- `{tags}` — теги обработки перехода, если есть.

При отображении страниц без редиректа вы также можете добавить параметры ссылки с макросами после имени файла для отображения, и они будут переданы в PHP, где будут доступны через суперглобальную переменную `$_GET`.

Пример использования в ссылке для редиректа:

```
https://example.com/offer?clickid={clickid}&geo={country}&os={os}
```

Пример использования при отображении без редиректа:

```
page.php?clickid={clickid}&geo={country}&os={os}
```

```
<!-- В коде файла page.php -->
<a href="https://example.com/offer?clickid=<?= $_GET['clickid'] ?>">Offer</a>
```

## 5.4 Ротатор

Ротатор определяет алгоритм ротации контент-страниц, т.е. то, как система выбирает, какую контент-страницу показать каждому конкретному посетителю. Если указана только одна контент-страница, то выбор ротатора ни на что не влияет. На данный момент Adspect поддерживает два ротатора: «сплит» и «таймер».

### 5.4.1 Ротатор «сплит»

Это ротатор по умолчанию, который распределяет трафик между включенными контент-страницами в соответствии с их весами: чем больше вес страницы, тем пропорционально больше трафика она получит.

Например, если у вас есть три контент-страницы с весами 10, 15 и 25, то первая страница получит 20 % от всего целевого трафика, вторая страница получит 30 %, а третья — 50 %.

Так как этот ротатор имеет в основе генератор псевдослучайных чисел (PRNG), при небольшом числе входящих кликов могут быть «перекосы» в распределении трафика относительно заданных весов. Однако, математические свойства PRNG гарантируют, что на дистанции распределение трафика максимально точно достигнет заданных весов.

### 5.4.2 Ротатор «таймер»

Этот ротатор переключается между контент-страницами, используя вес как число секунд, на которое активируется та или иная страница.

Например, если у вас указаны три страницы с весами 60, 120 и 180, то первая страница будет показываться посетителям в течение одной минуты, затем ротатор будет 2 минуты показывать вторую страницу, затем переключится на третью и будет отображать ее 3 минуты, а затем снова вернется к первой, и так далее.

Этот ротатор удобен для автоматической смены доменов по времени.

## 5.5 Белая страница

Это безопасная страница, которую можно показывать модераторам, роботам, скрейперам и т.п. Она не должна содержать никакой чувствительный контент, который может поставить вашу рекламную

кампанию под угрозу, например из-за нарушения правил рекламной сети. Все, описанное выше для страницы контента, также относится и к белой странице: вы можете использовать URL или имя файла для отображения. В случае с файлом, если ваша контент-страница также настроена как файл, вам фактически потребуется совместить два лэндинга в одной папке, с разными именами HTML- или PHP-файлов.

Мы настоятельно рекомендуем использовать полноценный собственный лэндинг в качестве белой страницы. Это связано с тем, что некоторые рекламные сети с подозрением относятся к любым редиректам, подвергая содержащие их кампании более тщательной проверке, а некоторые и вовсе запрещают редиректы.

## 5.6 Пробрасывать URL-параметры на белую страницу

Если проброс параметров включен, то все параметры из входящей ссылки будут добавлены к ссылке или имени файла белой страницы. Эта настройка работает по тому же принципу, что настройка «парам» для контент-страниц.

## 5.7 VLA™

VLA™ является аббревиатурой от «Virtual Learning Appliance». Это торговое название собственной системы машинного обучения в основе технологии фильтрации трафика Adspect. Вы можете ознакомиться с системой более детально в *главе о VLA*. 95% является оптимальным начальным значением для точности VLA.

## 5.8 Sub ID

Sub ID — это параметр ссылки, по которому можно делать разбивку в статистике, выбрав критерий группировки «Sub ID». Статистика подробно описана в *отдельной главе* данного руководства.

Принцип работы проще всего показать на примере. Возьмем рекламную сеть, у которой есть понятие зон — номеров площадок, на которых показываются рекламные объявления. Номер зоны, с которой пришел клик, помещается в трекинговую ссылку для передачи в трекер при помощи макроса, например `{zoneid}`:

```
https://tracker.test/lander/index.php?subid={zoneid}
```

Для каждого клика рекламная сеть заменит этот макрос `{zoneid}` фактическим номером зоны, из которой пришел клик, а далее трекер извлечет его из кликовой ссылки для сбора статистики. В данном примере `subid` является параметром ссылки, в котором содержится номер зоны. Если вы укажете `subid` в поле «Sub ID» в потоке, то сможете получать статистику по каждой отдельной зоне в потоке. Это может быть очень полезным для сбора черных списков зон с высокой плотностью ботов.

В качестве sub ID можно использовать и другие атрибуты: страну, платформу (десктоп/мобайл), версию ОС, вообще любой параметр ссылки. Вы можете комбинировать несколько макросов для получения составного параметра для sub ID, например:

```
https://tracker.test/lander/index.php?subid={zoneid}-{platform}
```

В этом примере каждый субаккаунт будет парой из зоны и платформы устройства посетителя.

## 5.9 Click ID

Настройка Click ID работает по тому же принципу, что и Sub ID, но используется для уникальной идентификации отдельных кликов с помощью параметра, генерируемого рекламной сетью или трекером. Если параметр указан, то его значения извлекаются из ссылки при прохождении клика через Adspect и записываются в статистику вместе с другими показателями. Это позволяет находить отдельные клики в сырых покликовых отчетах, которые можно выгрузить в формате CSV. Одним из способов применения может быть сбор доказательной базы для выявления кликфрода в трафике.

Если параметр не указан, то Adspect сам сгенерирует индентификатор перехода для использования в *трекере*. В зависимости от того, как именно осуществляется отображение контента/белой страницы, идентификаторы переходов могут быть помещены в целевые ссылки при помощи макроса `{clickid}`, либо встроены где угодно в файлы лендингов при помощи PHP-переменной `$_SERVER["ADSPECT_CLICK_ID"]`.

## 5.10 Режим паранойи

Режим паранойи подключает дополнительные строгие проверки JavaScript-отпечатков, а также обширные черные списки IP-адресов совокупным объемом 2 миллиарда адресов IPv4. Эти меры считаются «параноидальными» в том смысле, что несут в себе более высокие риски ложноположительных срабатываний, но в то же время они предоставляют более высокий уровень защиты от модераторов.

**Мы рекомендуем включить этот режим при работе с Facebook и Google Ads.**

## 5.11 Разрешить трафик из мобильных приложений

Эта настройка говорит нам пропускать трафик из мобильных приложений в общем порядке, не считая его априори фродовым. Ярким примером такого трафика являются переходы, сделанные из браузера WebView на платформе Android. Этот трафик является естественным для некоторых нишевых рекламных форматов, но в традиционных форматах рекламы он очень часто оказывается накруткой (автоматическими кликами, выполняемыми зараженными вирусами мобильными устройствами) и поэтому должен быть отфильтрован. Включайте настройку только в том случае, если ваш рекламный формат так или иначе основан на мобильных приложениях.

## 5.12 Страны, операционные системы, браузеры, языки и часовые пояса

Эти настройки ручного таргетинга позволяют вам ограничить круг потенциальных посетителей контента только указанными странами, операционными системами, браузерами, языками браузера и часовыми поясами. Обычно следует указывать те же таргетинги, что и в рекламной кампании. Если та или иная настройка не задана (список пуст), то проверка по ней не производится.

Настройка часовых поясов ограничена полночасовыми смещениями относительно UTC. Если часовой пояс посетителя смещен относительно UTC на неполное число часов (например, Индия UTC+5.5), то смещение округляется до ближайшего полного часа (в примере с Индией до UTC+5).

## 5.13 Проверять соответствие часового пояса браузера и местоположения

Если эта настройка включена, то Adspect будет отфильтровывать всех посетителей, у которых часовой пояс браузера не совпадает с часовым поясом их фактического местоположения, определенного при помощи нашей геолокации. Эта проверка немного повышает вероятность ложноположительных срабатываний, однако значительно улучшает защиту от модераторов и ботов, использующих VPN- и прокси-сервисы. При включенной проверке описанный выше ручной список часовых поясов игнорируется. Мы рекомендуем включить эту настройку.

## 5.14 URL-правила

Эта секция позволяет вам создать до 30 собственных правил проверки и изменения URL-параметров. Каждое правило описывается следующими составными частями:

- Параметр — имя параметра в ссылке, который будет проверяться или изменяться;
- Оператор — конкретная проверка или операция, которая будет произведена;
- Аргумент — аргумент оператора, если он применим (поддерживаются макросы);
- Переключатель «Вкл» — позволяет включать и выключать отдельные правила.

Поддерживаются следующие операторы:

- `EXISTS` — проверяет, что параметр существует (аргумент игнорируется);
- `! EXISTS` — проверяет, что параметр не существует (аргумент игнорируется);
- `REGEX` — проверяет параметр на совпадение с Perl-совместимым регулярным выражением (PCRE) в аргументе (с учетом регистра);
- `REGEX (no case)` — проверяет параметр на совпадение с регулярным выражением в аргументе (без учета регистра);
- `! REGEX` — проверяет параметр на несовпадение с регулярным выражением в аргументе (с учетом регистра);
- `! REGEX (no case)` — проверяет параметр на несовпадение с регулярным выражением в аргументе (без учета регистра);
- =, , >, , <, — сравнивают параметр с аргументом; целочисленные и вещественные значения сравниваются как числа, строки сравниваются в соответствии с лексикографическим порядком;
- `ASSIGN` — назначает параметру значение из аргумента;
- `RENAME` — переименовывает параметр в аргумент;
- `DELETE` — удаляет параметр из ссылки (аргумент игнорируется);

Правила выполняются в следующем порядке:

1. Проверки: правила `EXISTS` и `REGEX`, =, , >, , <, — не пройденная проверка отправляет на белую страницу;
2. Правила `ASSIGN`;
3. Правила `RENAME`;
4. Правила `DELETE`.

В аргументах правил поддерживаются все те же макросы, доступные для использования в полях «Контент» и «Белая страница».

## 5.15 Фильтр user agent

Эта настройка позволяет вам указать собственное Perl-совместимое регулярное выражение (PCRE) для фильтрации посетителей по их строке user agent. Сравнение производится с учетом регистра символов. По умолчанию поиск вхождения производится в любой части строки user agent; вы можете использовать якоря ^ и $ для привязки шаблона к началу или концу строки (см. примеры ниже).

Синтаксис PCRE очень богатый и мощный и находится за рамками данной документации. Отдельные выражения могут быть объединены с помощью различных синтаксических конструкций, что позволяет создавать сколь угодно сложные шаблоны, однако обратите внимание, что в текущей реализации длина регулярного выражения не может превышать 1023 символа.

Несколько примеров:

```
Firefox|Nexus|Miui
```

Это выражение совпадет с любым user agent, который содержит слова «Firefox», «Nexus» или «Miui». Его можно использовать для фильтрации посетителей с Mozilla Firefox, Google Nexus и встроенного браузера Xiaomi.

```
^Mozilla/4[.]0
```

Это выражение совпадет с любым user agent, который начинается с «Mozilla/4.0». Оно отфильтрует всех подозрительных посетителей, которые якобы используют очень старые браузеры, но тем не менее поддерживают современные конструкции JavaScript (подразумевается тем, что посетитель смог сформировать машинный отпечаток.)

```
^Mozilla/5[.]0$
```

Это выражение отфильтрует тех посетителей, чей user agent строго совпадает с «Mozilla/5.0», то есть не содержит сведений о конкретном бразуре, HTML-движке и платформе, что очень необычно и подозрительно.

Все выражения выше могут быть объединены в одно с использованием логического «или» (т.е. совпадет первое *или* второе *или* третье) следующим образом:

```
Firefox|Nexus|Miui|^Mozilla/4[.]0|^Mozilla/5[.]0$
```

**Будьте осторожны! Неправильно сформированное регулярное выражение может привести к ошибочным срабатываниям и фильтрации больших объемов хорошего трафика. Используйте эту настройку только если вы точно знаете что делаете.**

## 5.16 Фильтр referer

Эта настройка работает по тому же принципу, что описанный выше фильтр user agent, но в отношении HTTP referer. Adspect отфильтрует всех посетителей, чей referer совпадет с указанным Perl-совместимым регулярным выражением. Сравнение производится с учетом регистра символов.

Распространенным сценарием использования является фильтрация пустых referer-ов:

```
^$
```

**Будьте осторожны! Неправильно сформированное регулярное выражение может привести к ошибочным срабатываниям и фильтрации больших объемов хорошего трафика. Используйте эту настройку только если вы точно знаете что делаете.**

## 5.17 Черный список IP/ASN

Это черный список IP-адресов, диапазонов IP-адресов и/или номеров автономных систем (ASN), которым будет всегда показываться белая страница. Поддерживаются адреса IPv4 и IPv6, CIDR-нотация и произвольные диапазоны. Примеры:

- 192.0.2.1
- 192.0.2.0/24
- 192.0.2.0–192.0.2.255
- 2001:db8::1
- 2001:db8::/112
- 2001:db8::-2001:db8::ffff

Отдельные элементы должны разделяться переносами строки или пробелами. Обратите внимание, что система автоматически объединяет соседние или пересекающиеся диапазоны для оптимизации их хранения в памяти и для ускорения поиска.

## 5.18 Заносить все IP-адреса в черный список в режиме «Модерация»

Если эта настройка включена, то Adspect будет автоматически заносить IP-адреса всех посетителей в потоке в черный список, если поток работает в режиме «Модерация». Так как этот режим предназначен именно для прохождения модерации, то будет справедливо считать всех посетителей модераторами, а следовательно запоминать и блокировать в дальнейшем. Мы рекомендуем вам всегда включать эту опцию, но будьте внимательны и не пропустите момент, когда вашу кампанию одобрят, — вам нужно успеть переключить поток в режим «Фильтр» прежде, чем польется трафик, иначе в черный список попадут IP-адреса обычных посетителей.

Глава 6

# Трекер

Трекер — это незаменимый инструмент в цифровой рекламе в целом и в партнерском маркетинге в частности. Его главная задача состоит в регистрации конверсий (лидов, заказов, продаж) и отслеживании их до конкретных посетителей, ранее пришедших на сайт или оффер. Это позволяет маркетологам собирать статистику по конверсиям и анализировать ее в различных разрезах, выстраивая так называемые воронки продаж.

Adspect имеет встроенный в ядро системы трекер, легкий, но в то же время эффективный и полнофункциональный. В разделе *Статистика* личного кабинета вы можете строить и анализировать различные воронки, используя любые комбинации доступных группировок и фильтров. В числе прочего, статистика Adspect считает и отображает такие важнейшие маркетинговые показатели, как конверсии, расход, доход, CR (коэффициент конверсии), ROI (возврат инвестиций), CPA (цену лида) и EPC (доходность перехода) / EPM (доходность тысячи переходов). Эти метрики особенно полезны в комбинации с группировкой по отдельным площадкам в источнике трафика, как описано в параграфе о настройке Sub ID.

## 6.1 Postback

Для того, чтобы использовать трекер, вам понадобится настроить postback — «отстук» информации о конверсиях на postback URL, который вы можете найти в вашем профиле. Мы принимаем postback любым из доступных HTTP-методов: `GET`, `POST`, `PUT` и др. Postback URL принимает три параметра:

1. `aid` — ID аккаунта в Adspect, который заранее указан в ссылке и обычно не меняется;
2. `cid` — уникальный идентификатор перехода, с которого произошла конверсия;
3. `sum` (необязательно) — сумма выплаты за конверсию при работе по моделям CPA и revenue share.

Большинство партнерских программ и сетей поддерживают postback и предоставляют различные макросы, которые можно использовать для заполнения переменных частей postback-ссылки (параметры `cid` и `sum`). Если вам нужно делать postback самостоятельно, то вы можете разместить пиксель конверсии где-нибудь, например на странице «Спасибо за заказ». Код пикселя может выглядеть следующим образом (положим, что ID перехода передается в параметре ссылки `clickid`):

```
<script>
(function () {
  const cid = new URLSearchParams(location.search).get("clickid");
  const url = "https://rpc.adspect.net/v1/postback?aid=1ea704aa-d0d3-6262-bf65-ac1f6b95a853&cid="␣
↪+ cid;
  fetch(url, {mode: "no-cors"});
})();
</script>
```

При успешной регистрации конверсии запрос будет завершен HTTP-кодом ответа 200 и текстом `OK`.

## 6.2 ID переходов

Чтобы конверсия была зарегистрирована и обработана, Adspect необходимо иметь данные о предшествующем ей переходе в базе данных статистики, то есть ранее должен быть зарегистрирован переход с тем же ID перехода. Вы можете использовать внешние ID переходов, например генерируемые рекламной сетью, для чего следует указать имя параметра ссылки, содержащего ID перехода, в поле Click ID в настройках потока. Вы также можете оставить поле Click ID пустым, и тогда Adspect будет самостоятельно генерировать ID переходов. Postback-ссылка принимает без ошибок ранее не встречавшиеся ID переходов, однако такие конверсии будут отброшены на более поздних стадиях обработки.

Глава 7

# Статистика

Наша статистика является точным и ценным источником аналитической информации о качестве трафика в ваших рекламных кампаниях. Вы можете использовать наши отчеты для сравнительного анализа отдельных источников, площадок, спотов и т.п. Отчетность доступна в двух форматах: сырая и агрегированная.

Обратите внимание, что статистика не отображается в реальном времени, а обновляется раз в минуту.

## 7.1 Сырые отчеты

Сырые отчеты являются покликовыми, то есть содержат информацию о каждом переходе, который был обработан нашей системой. Их можно скачать в формате CSV при помощи кнопки «CSV-файл». В выпадающем меню будут две опции: скачать полный отчет или только по тем переходам, для которых сработал один или несколько фильтров. Охват отчета будет ограничен выбранным диапазоном дат. Далее скачанный файл может быть импортирован в Microsoft Excel или другое ПО для работы с таблицами.

Пожалуйста, не выбирайте слишком широкие диапазоны дат, так как это приводит к формированию очень больших CSV-файлов и повышенной нагрузке на наши серверы. Мы ограничиваем количество строк, которые выгружаются для отчета; этот лимит пересматривается время от времени по усмотрению наших системных администраторов.

## 7.2 Колонки сырого отчета

Сырые отчеты могут содержать одну или две строки на каждый переход. Первая строка соответствует отдаче посетителю скрипта для сбора машинного отпечатка браузера. Вторая строка, если она есть, соответствует сканированию отпечатка и принятию решения — пропустить или отфильтровать. Второй строки может не быть, если посетитель по тем или иным причинам не смог сформировать или отправить нам отпечаток.

Сырые отчеты состоят из следующих колонок:

- `timestamp` — дата и время события;
- `ip_address` — IP-адрес посетителя в формате IPv6 (для адресов IPv4 используется стандартное преобразование IPv4-to-IPv6 mapping);
- `stream_id` — ID потока, в котором произошло событие;
- `country_code` – ISO 3166-1 alpha-2 код страны посетителя;
- `os` – название и версия операционной системы посетителя;
- `browser` – название браузера посетителя;
- `cost` – цена перехода, если передана через параметр ссылки;
- `sub_id` — sub ID перехода, если передан через параметр ссылки;
- `click_id` — click ID (уникальный идентификатор перехода), если передан через параметр ссылки;
- `mode` – режим потока в момент события;
- `sequence` — этап обработки перехода: 0 — сбор отпечатка, 1 — сканирование отпечатка;
- `target` — страница, показанная посетителю: 0 обозначает белую страницу, 1 и выше — контент;
- `tags` — список мнемонических тегов, обозначающих конкретные фильтры или иные причины для принятия решения (в основном для внутреннего использования).

### 7.2.1 Теги

Конкретный смысл многих тегов является коммерческой тайной — мы не раскрываем наши алгоритмы фильтрации. Однако, ниже мы приведем расшифровку некоторых из них, которые могут быть использованы в качестве доказательства наличия ботов в трафике (например, при требовании денежных компенсаций у рекламных сетей) или для отладки:

- `REVIEW`, `MONEY`, `WHITE` – решение принято клиентом путем установки режима потока: «Модерация», «Контент» и «Белая страница» соответственно;
- `IP`, `IP...` – IP-адрес находится в наших черных списках: прокси-сервисы, VPN- и хостинг-провайдеры, антивирусные, скоринговые и ИБ-компании, модераторы и т.п.;
- `BL` – IP-адрес находится в черном списке IP/ASN потока;
- `BOT` – посетители, чей user agent явно указывает на то, что они боты, известные эмуляторы устройств или системы виртуализации;
- `PARANOID` – посетители, заблокированные режимом паранойи;
- `GEO`, `OS`, `BROWSER`, `LANG`, `TZ`, `IPTZ` – посетители, заблокированные ручными фильтрами потока;
- `RULE` – посетители, заблокированные пользовательским URL-правилом;
- `UARE` – посетители, отфильтрованные регулярным выражением потока для user agent;
- `REF` – посетители, отфильтрованные регулярным выражением потока для referer.

## 7.3 Агрегированные отчеты

Агрегированные отчеты создаются путем разбивки сырых отчетов на группы с последующим агрегированием (или суммированием) показателей в рамках каждой группы. Группировка выбирается в поле слева от выбора часового пояса и по умолчанию имеет значение «Поток», то есть статистика будет считаться отдельно для каждого потока. Есть и другие возможные значения: «Дата» для подсчета

показателей за каждую дату и «Sub ID» для разбивки статистики по отдельным субаккаунтам (в этом параграфе описаны принципы работы субаккаунтов).

Группировка может быть вложенной, например «Дата» + «Поток» — в этом случае статистика будет разбита сначала по датам, а затем по потокам за каждую дату. Так вы можете комбинировать критерии группировки, чтобы строить различные воронки.

После выбора параметров отчета нажмите на кнопку «Отчет», чтобы его сформировать. Данные будут отображены в виде сортируемой таблицы под панелью параметров.

Помимо работы с отчетом в нашем веб-интерфейсе, вы также можете выгрузить текущий отчет в формате CSV с помощью серой кнопки «CSV» в левом нижнем углу окна отчета.

## 7.4 Колонки агрегированного отчета

Каждый агрегированный отчет в левой части состоит из колонок, по которым осуществлялась группировка, за которыми идут колонки статистики. Некоторые из них могут содержать значение в процентах, отображенное серым цветом, — это процент от общего числа переходов, выводимый для удобства.

Список статистических колонок с пояснениями:

- Переходы — общее число переходов на файл `index.php`; от него считаются проценты в других колонках.
- Уники — приблизительное число уникальных посетителей с точки зрения уникальности их IP-адресов.
- FP — число посетителей, которые при обработке сформировали и успешно отправили нам JavaScript-отпечаток для анализа. Это число может быть меньше, чем число кликов, по разным причинам, но как правило разницу составляют «тупые» клик-боты, которые не в состоянии выполнять JavaScript.
- На контент — число посетителей, которым была показана контент-страница. Это хороший показатель для оценки объемов чистого целевого трафика. Обратите внимание, что сюда же попадут все посетители при работе потоков в режиме «Контент».
- На белую — число посетителей, которым была (или была бы) показана белая страница. Этот показатель рассчитывается как общие переходы минус переходы на контент, то есть включает в себя упомянутых выше «тупых» ботов, которые бы попали на белую страницу, если бы могли выполнять JavaScript (впрочем, проблему JavaScript мы решаем другим способом через «meta refresh»).
- GIVT — «general invalid traffic» — это технические потери, число посетителей, которые не смогли сформировать и отправить отпечаток. Как упоминалось ранее, это как правило «тупые» боты с ограниченной поддержкой JavaScript. Другая распространенная причина технических потерь — сетевой лаг, особенно наглядный при работе с трафиком с плохим Интернет-соединением: посетители успевают закрыть окно или вкладку прежде, чем отпечаток будет отправлен и обработан. На данный момент в эту же колонку попадут все переходы, которые произошли, когда поток находился в режиме «Контент», «Белая страница» или «Модерация» при отключенном сборе отпечатков, так как во всех этих режимах не происходит обработки отпечатков. Мы планируем изменить эту логику подсчета GIVT в будущем для отражения более объективных данных по техническим потерям.
- SIVT — «sophisticated invalid traffic» — число отпечатков, которые были осознанно отфильровано алгоритмами Adspect. Это может быть грубой метрикой современного продвинутого кликфрода в вашем трафике. Сюда же входят модераторы и переходы, заблокированные ручными фильтрами потока.

- Расход — это суммарный расход средств на трафик, посчитанный как сумма цен каждого перехода, если они были переданы через соответствующий параметр ссылки.
- Расход (боты) — расход средств на трафик, который был направлен на белую страницу. Если настроена передача цены перехода через параметр ссылки, то эта метрика точно отражает потери бюджета на фильтрации.
- Качество — это процент показов контент-страницы от общего числа кликов. Это наилучший показатель для оценки качества трафика в целом и может быть использован для сравнения различных источников, площадок, спотов и т.п. Особую ценность представляет сбор черных или белых списков площадок по плотности ботов в них; методика описана в отдельной главе.
- Конверсии — общее число конверсий, полученных через механизм postback.
- CR — коэффициент конверсии, считаемый как конверсии : клики.
- Доход — общая выручка воронки, посчитанная через механизм postback.
- Прибыль — прибыль или убыток, считаемые как доход  расход.
- ROI — возврат инвестиций, считаемый как прибыль : расход.
- CPC / CPM — средняя цена клика, считаемая как расход : клики, и стоимость тысячи кликов, считаемая как CPC  1000.
- CPA — средняя цена лида, считаемая как расход : конверсии.
- EPL — средний доход с лида, считаемый как доход : конверсии.
- eCPM — Средний доход с тысячи кликов, считаемый как доход / клики  1000.

Также в нижнем левом углу окна отчета находится кнопка «CSV», которая позволяет скачать текущий агрегированный отчет в виде CSV-файла для дальнейшего импорта, анализа или печати.

Глава 8

# Рекомендации

Ниже мы приводим список общих рекомендаций по работе, универсальных для большинства наших клиентов. Мы настоятельно рекомендуем придерживаться их для достижения наилучших результатов с Adspect.

## 8.1 Доменные имена и хостинг

1. **Не используйте** доменные имена в дешевых зонах, таких как `.site`, `.club`, `.world` и т.п., потому что они привлекают повышенное внимание проверяющих, а также антивирусных и скоринговых компаний. Фактически такие доменные имена находятся «на карандаше» с самого момента их регистрации. Используйте только доменные зоны `.org`, `.net` и `.com`, в порядке предпочтительности.

   **Совет:** вы можете проверить статус домена в Facebook при помощи инструментов разработчика.

2. **Не используйте** доменные имена, содержащие сомнительные или стоп-слова: «sex», «xxx», «win», «diet», «health», «meet», «date» и т.д. Включите воображение, придумывайте доменные имена, которые выглядят и звучат как бренды.

3. **Всегда используйте** Cloudflare для сокрытия IP-адресов ваших серверов. Многие рекламные сети запоминают IP-адреса доменов в заблокированных аккаунтах, однако они никогда не забанят IP-адреса одной из крупнейших CDN-компаний, которая обслуживает 10 % всего Интернета. Adspect полностью поддерживает Cloudflare в режиме прокси.

4. **Не используйте** технические домены хостинговых компаний. Они выглядят подозрительно и вместе с тем уникально идентифицируют отдельные серверы.

5. **Не используйте** виртуальный хостинг Namecheap. Там включен WAF (web application firewall), блокирующий по умолчанию POST-запросы, на которых работает наша система, что приводит к ошибкам 403 Forbidden.

6. **Не называйте** файлы контент- или белой страницы `index.html`, так как вероятно, что они будут иметь приоритет над нашим файлом `index.php` при обработке запросов, в URL которых явно не указано имя файла после `/`, из-за чего вместо фильтра Adspect будет открываться сама

страница. Всегда используйте разные имена файлов для контент- и белой страницы, которые сложно угадать.

7. **Всегда проверяйте**, что ваши белые страницы не содержат битых ссылок, незагружающихся изображений или скриптов с ошибками. Проверять можно при помощи инструментов разработчика в браузере во вкладках Консоль и Сеть — потенциальные проблемы будут отображены красным.
8. **Не используйте** веб-ресурсы (изображения, стили, скрипты) со сторонних доменов, если только это не широко известные CDN (content delivery network), как у jQuery, Bootstrap, Font Awesome, Google Fonts и т.п. Скачивайте подключаемые файлы и размещайте их локально.
9. **Всегда настраивайте** HTTPS для ваших страниц. Cloudflare предоставляет бесплатные сертификаты SSL/TLS для доменных имен в режиме проксирования. Let's Encrypt также предоставляет инфраструктуру для управления бесплатными сертификатами SSL/TLS.
10. **Рекомендуется** использовать хостинг в непосредственной близости от целевой аудитории, в идеале в той же стране. Это особенно важно при работе с форматом popunder.

## 8.2 Рекомендации по клоакингу

1. **Никогда не используйте** доменные имена, креативы, белые страницы повторно после бана в одной и же рекламной сети без изменений. Регистрируйте новые доменные имена для новых аккаунтов, уникализируйте креативы и лэндинги.
2. **Всегда используйте** наиболее строгие ручные фильтры по стране, ОС, браузеру и языкам. Установите их зеркально таргетингам ваших рекламных кампаний.
3. **Всегда используйте** режим отображения белой страницы без редиректа, если возможно. Это требование **является обязательным в Facebook и Google Ads** при использовании PHP-интеграции!
4. **Всегда проверяйте**, что ваши белые страницы выглядят убедительно и правдоподобно, а содержимое соотносится с рекламными кампаниями (креативами, языками, таргетингами). **Никогда не указывайте** в качестве белых страниц перенаправление на Google и другие подобные явно нецелевые ресурсы.
5. **Используйте собственные белые страницы** вместо конструкторов сайтов (Shopify, Wix, Tilda и др.) при работе с Facebook и Google Ads, т.к. эти рекламные платформы в последнее время начали превентивно банить рекламные кампании, ведущие на сайты на конструкторах из-за их частого использования для клоакинга.
6. При использовании конструкторов **регулярно проверяйте** доступность ваших сайтов — нередко такие сервисы банят сайты при подозрении на их использование в клоакинг-схемах.
7. При использовании конструкторов с Facebook **отдельно клоачьте** контент-ссылки ваших основных потоков при помощи PHP-интеграции других потоков (то есть указывайте `index.php` другого потока в качестве контент-ссылки), чтобы предотвратить раскрытие вашего контента из-за доступа Facebook к истории переходов WebView в их приложении.
8. **Указывайте ссылки** на правдоподобные terms of use, privacy policy и cookies policy на белых страницах при работе с более строгими рекламными сетями, такими как Facebook, Google Ads, Microsoft Advertising и т.п. **Европейский закон о Cookie также требует**, чтобы сайты явно запрашивали разрешение на использование cookies.
9. **Добавляйте файлы** `robots.txt` и `sitemap.xml` в корневую директорию вашего домена, особенно при работе с рекламой в поисковиках (Google Ads, Microsoft Advertising, Verizon Media Native и т.п.)

10. **Не используйте** скопированные лэндинги без изменений, всегда уникализируйте их так или иначе. Это поможет обойти потенциальные блокировки по сигнатурам страниц.
11. **Не используйте** на белых страницах материалы, защищенные авторским правом, так как они могут быть обнаружены и отклонены модерацией.
12. **Не используйте** слишком простые, одностраничные, сломанные (в плане верстки и функциональности), не оптимизированные для мобильных устройств или просто низкокачественные белые страницы. Всегда помните, что белая страница должна выглядеть как правдоподобный и полезный сайт, с аутентичным контентом.
13. **Не используйте** лэндинги от якобы «белых» офферов в качестве белых страниц — понятие рекламных сетей о «белом» контенте может сильно отличаться от вашего. **Никогда не используйте** в качестве белых страниц прямые партнерские ссылки.
14. **Не изменяйте** белые страницы в работающих кампаниях. Более строгие рекламные сети могут обнаружить даже незначительные изменения вроде добавления тегов `<script>` и запустить процедуру проверки кампании или всего рекламного аккаунта.

## 8.3 Пиксель Facebook

Если вам необходимо использовать пиксель Facebook для «отстука» событий конверсии с вашей контент-страницы, то **не используйте** их стандартный скрипт, т.к. он раскроет вашу контент-страницу в заголовке Referer. Для этого есть безопасные альтернативы.

**Все перечисленные способы также подходят для защиты пикселей других рекламных сетей.**

### 8.3.1 Глобальное отключение referrer

Один из способов избежать утечки referrer-а — отключить его глобально для страницы целиком. Для этого добавьте следующий код в тег `<head>` страницы с вашим пикселем:

```
<meta name="referrer" content="no-referrer">
```

### 8.3.2 Альтернативный пиксель

Другой способ обезопасить пиксель Facebook — использовать собственную версию пикселя с отключенной передачей referrer. Facebook предоставляет «короткую» версию пикселя для посетителей без JavaScript:

```
<img height="1" width="1" style="display:none" src="https://www.facebook.com/tr?id=111111111111111&
↪ev=Lead&noscript=1">
```

Скопируйте URL пикселя из атрибута `src` и используйте его в одном из двух безопасных вариантов ниже в зависимости от нужного вам способа применения:

1. Статический способ с HTML iframe, подходит для вызова пикселя при загрузке страницы:

   ```
   <iframe height="1" width="1" style="display:none" src="https://www.facebook.com/tr?
   ↪id=111111111111111&ev=Lead&noscript=1" referrerpolicy="no-referrer">
   ```

2. Динамический JavaScript-способ, подходит для вызова пикселя из скрипта:

```
<script>
fetch("https://www.facebook.com/tr?id=111111111111111&ev=Lead&noscript=1", {mode: "no-cors",␣
↪referrerPolicy: "no-referrer"});
</script>
```

### 8.3.3 Postback-прокси

Если вам необходимо использовать postback CPA-сети для «спуска» пикселя Facebook, то не используйте для этого прямую ссылку пикселя. Вместо этого разместите на своем домене postback-прокси и нацельте postback на него:

```
<?php

$curl = curl_init();

curl_setopt($curl, CURLOPT_URL, 'https://www.facebook.com/tr?' . $_SERVER['QUERY_STRING']);
curl_setopt($curl, CURLOPT_FOLLOWLOCATION, true);
curl_setopt($curl, CURLOPT_USERAGENT, 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/
↪537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36');

curl_exec($curl);
curl_close($curl);
```

Используйте URL этого скрипта с параметрами пикселя Facebook в качестве postback URL в CPA-сети:

```
https://example.com/postback.php?id=111111111111111&ev=Lead&noscript=1
```

Скрипт будет принимать postback и перенаправлять его в Facebook с вашего домена и с подменой строки user agent.

Глава 9

# Приемы и хитрости

Гибкая природа файлов `index.php` вкупе с механизмом отображения страниц без редиректа по имени файла (который использует конструкцию `require()` языка PHP) позволяют создавать более сложные схемы обработки трафика. В этой главе мы опишем несколько таких схем, которые могут оказаться для вас очень полезными.

## 9.1 Цепочки из потоков

Так как файл `index.php`, используемый Adspect для фильтрации трафика, является обыкновенным PHP-скриптом, его можно использовать в качестве контент-страницы или белой страницы в любом другом потоке, то есть один поток может перенаправлять посетителей в другой поток. Это позволяет строить цепочки из потоков. Типичную настройку такой цепочки лучше всего проиллюстрировать примером из реальной практики.

Предположим, что у вас есть рекламная кампания в таком источнике трафика, который поставляет браузерный трафик вперемешку с трафиком из мобильных приложений, при этом не предоставляя настройки для их разделения. Такие рекламные сети существуют — это сети push-уведомлений, базы которых состоят как из подписчиков на WebPush, так и из подписчиков на уведомления в мобильных приложениях («in-app») и PWA. Вам хотелось бы разделять эти типы трафика, отправляя WebPush-подписчиков на оффер `https://example.com/webpush-offer`, а подписчиков in-app/PWA на другой оффер `https://example.com/inapp-offer`.

Вы можете решить эту задачу путем создания цепочки из двух потоков с разными настройками в отношении трафика из мобильных приложений. Первый поток A будет принимать входящие клики и отфильтровывать трафик из приложений на белую страницу. Второй поток B будет подключен к потоку A в качестве его белой страницы, чтобы отделять благонадежных посетителей из приложений от ботов и модераторов.

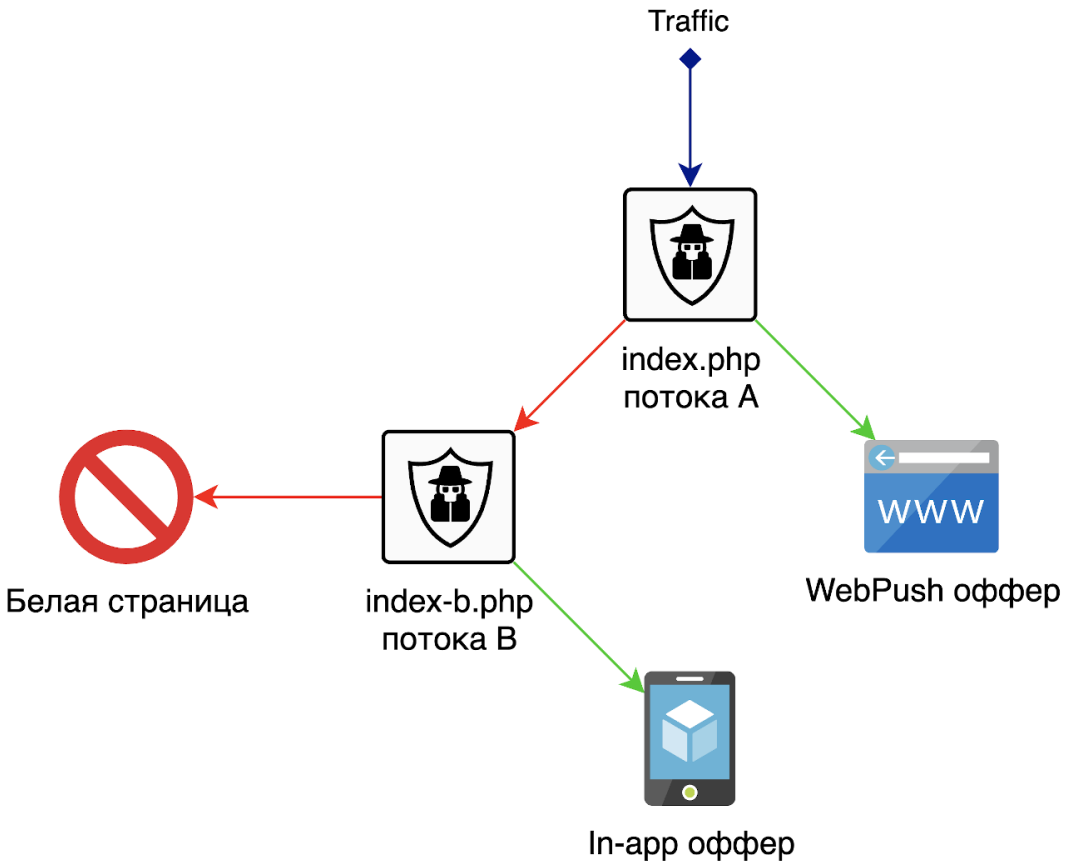


Схема прохождения трафика

В этой схеме поток A будет иметь следующие определяющие настройки:

- Контент-страница: `https://example.com/webpush-offer`
- Белая страница: `index-b.php`
- Разрешить трафик из мобильных приложений: *нет*

Определяющие настройки для потока B:

- Контент-страница: `https://example.com/inapp-offer`
- Белая страница: `https://google.com/`
- Разрешить трафик из мобильных приложений: *да*

Запрет трафика из мобильных приложений во входном потоке A будет отправлять такой трафик вместе с другими отфильтрованными посетителями на белую страницу, в качестве которой выступает поток B. Поток B в свою очередь будет заново анализировать трафик и отправлять хороших посетителей из приложений на отдельный оффер, отфильтровывая всех остальных на настоящую белую страницу (Google в нашем примере).

Далее вам просто потребуется разместить файлы `index.php` обоих потоков в одной папке: оставьте файл `index.php` потока A названным как есть, а файл потока B переименуйте в `index-b.php`, который и будет являться суррогатной белой страницей для потока A.

## 9.2 Выделенный поток для черного списка IP-адресов

У потоков есть полезная настройка «Заносить все IP-адреса в черный список в режиме «Модерация», которая позволяет автоматизировать сбор IP-адресов модераторов в черном списке потока в режиме «Модерация». Эта настройка может использоваться для создания единого черного списка в выделенном для этой цели потоке.

Порядок действий:

1. Создайте отдельный поток для сбора единого черного списка. Переведите его в режим «Модерация» и включите настройку «Заносить все IP-адреса в черный список в режиме «Модерация». Это приведет к тому, что IP-адреса всех посетителей в потоке будут заноситься в его черный список автоматически в момент каждого клика.
2. Используйте файл `index.php` этого потока в качестве белой страницы для других потоков, как было описано выше. Это приведет к занесению IP-адресов всех неблагонадежных посетителей в черный список выделенного потока. Если вы опасаетесь, что такой черный список со временем станет слишком широким и будет приводить к большому количеству ложноположительных результатов (как было упомянуто в главе о фильтрации), то используйте поток в качестве белой страницы в других потоках только на период модерации.
3. Наблюдайте за автоматическим пополнением черного списка IP-адресов в вашем выделенном потоке и копируйте его в другие потоки время от времени (мы понимаем, что это неудобно, и уже работаем над решением для создания общих черных списков на несколько потоков).

## 9.3 Комбинирование клоакеров

Если у вас есть доступ к другим решениям для клоакинга и защиты трафика, то вы можете использовать их совместно с Adspect, чтобы потенциально увеличить надежность защиты ценой увеличения накладных расходов на фильтрацию. Так как у большинства наших конкурентов также имеются понятия контент-страницы и белой страницы, то вам следует всегда располагать Adspect в хвосте цепочки клоакеров и создавать для каждой цепочки два отдельных потока:

- Один поток будет использоваться в качестве контент-страницы вышестоящего клоакера, принимая от него трафик, который тот посчитал хорошим. Контент-страницей этого потока будет ваш целевой оффер или лэндинг, а белой страницей — настоящая белая страница, при помощи которой будет осуществляться клоакинг. Установите этот поток в режим «Фильтр».
- Другой поток будет использоваться в качестве белой страницы вышестоящего клоакера, принимая от него трафик для целей сбора черного списка IP-адресов «плохих» по мнению вышестоящего клоакера посетителей, а также для обучения на этом трафике нашей системы машинного обучения *VLA*. Полученные данные позволяют нам перенимать у других клоакинг-решений их критерии фильтрации и тем самым делать Adspect еще более точным. Обязательно включите настройку «Заносить все IP-адреса в черный список в режиме «Модерация» для сбора IP-адресов в черном списке потока, как это было описано выше. В качестве контент-страницы и белой страницы укажите вашу конечную белую страницу, при помощи которой будет осуществляться клоакинг. Оставьте поток постоянно работать в режиме «Модерация».

Глава 10

# Недостатки и подводные камни

Как и у любой сложной системы, у Adspect есть свои недостатки и подводные камни. Вам следует о них знать. В этой главе мы расскажем, как избежать распространенных ошибок, чтобы не ставить на кон успех ваших рекламных кампаний.

## 10.1 Не выделяйтесь!

Большинство рекламных сетей практикует рутинную перепроверку всех рекламных кампаний время от времени. Помимо помощи в прохождении первичной модерации при запуске новой кампании, первостепенная задача любого клоакинг-сервиса заключается в защите уже работающих кампаний от этих повторяющихся фоновых проверок. Adspect справляется с этой задачей очень хорошо, что доказано многими успешными кампаниями в различных рекламных сетях.

Но есть одно «но»: если ваша рекламная активность выделяется на фоне других рекламодателей в глазах конкретной сети, то это рано или поздно привлечет внимание их модераторов, они начнут изучать ваши кампании «с пристрастием», неизбежно «пробьют клоаку» и применят к вам административные санкции. Мы можем гарантировать прочную защиту от рутинных проверок, но ни один сервис не защитит вас от специально проводимого расследования по подозрению в нарушении тех или иных правил.

Запомните: *не выделяйтесь!* Если вы будете неосторожны и привлечете к себе внимание персонала сети, то вас раскроют. Пути назад уже не будет. Приведем список рекомендаций, чтобы этого не произошло:

- Не лейте слишком много трафика с одного аккаунта. Большие объемы обычно подразумевают стабильную прибыль и таким образом вызывают интерес к природе ваших кампаний.
- Не создавайте слишком много кампаний в одном аккаунте. Чем их больше, тем больше материала для проверок, тем пропорционально чаще они происходят и тем выше шанс нарваться на неприятности.
- Всегда используйте трекер. Долго работающие без трекера affiliate-кампании заставляют наблюдателя задуматься, как рекламодателю удается поддерживать их прибыльность.

- Всегда используйте трекинговые параметры и макросы в ссылках. Эта рекомендация по смыслу схожа с предыдущей и особенно актуальна для кампаний с широкими настройками таргетинга.
- Используйте функцию постбэка, если она поддерживается рекламной сетью.

Из изложенных выше соображений вытекает принцип разделения ответственности: Adspect отвечает за защиту ваших кампаний от рутинной (пере)модерации, но ответственность за непривлечение к себе внимания лежит на вас.

## 10.2 Длинные цепочки редиректов

Один из главных недостатков облачных сервисов, таких как Adspect, в том, что они увеличивают задержки при обработке каждого клика из-за сетевого лага между вашим трекером и бэкенд-серверами сервиса. Если вы наблюдаете большие технические потери в разделе «Статистика», то это может быть признаком слишком высоких сетевых задержек.

Мы настоятельно рекомендуем делать цепочки редиректов как можно короче. Размещайте лэндинги на своем сервере и используйте файловый механизм их показа вместо редиректов на внешние URL-ы (подробнее здесь). Размещайте трекер либо до, либо после файла `index.php` в цепочке прохождения трафика, но не с обеих сторон. Выбирайте хостинг для трекера, наиболее географически приближенный к целевой стране или региону вашего трафика, если это возможно.

Также стоит упомянуть, что мы разрабатываем hosted-решение для фильтрации трафика, которое позволит нашим клиентам нивелировать «облачные» задержки за счет переноса систем фильтрации непосредственно на их серверы или трекеры, тем самым убирая необходимость поддержания постоянной связи с нашими бэкенд-серверами. Дополнительная информация будет опубликована позднее.

## 10.3 Ложноположительные

Ложноположительные — это решения фильтра о блокировании благонадежных посетителей из-за ложного отнесения их к нежелательным. Ни одно решение не может гарантировать точность в 100%, но мы достаточно уверены в нашем продукте, чтобы утверждать, что частота ложноположительных срабатываний у Adspect является наименьшей на рынке, зачастую на порядок ниже в сравнении с некоторыми конкурентами. Конечно, существуют решения с еще более низкими показателями фильтрации, но это их недоработка, а не заслуга, — эти решения пропускают многих нежелательных посетителей на ваш контент. Подобные ошибки классификации называются ложноотрицательными и могут быть легко доказаны сравнительным покликовым анализом решений. Adspect позволяет выгружать логи решений в форме сырых CSV-отчетов.

## 10.4 Ложноотрицательные

Ложноотрицательные решения случаются тогда, когда фильтр не распознает опасность в посетителе и пропускает его на контент. Это является той самой причиной, по которой «клоаку пробивают» время от времени. Причина кроется в практической невозможности определить всех потенциально существующих враждебных посетителей. Все используемые для этого меры можно так или иначе обойти при наличии достаточной мотивации и экспертизы. В параграфе «Не выделяйтесь!» выше мы описали причины появления этой мотивации у тех, от кого вы защищаете свой контент, и будьте уверены, что у них есть вся необходимая техническая экспертиза.

Запомните: *ложноотрицательные и все их последствия — результат привлечения внимания!*

Глава 11

# Реферальная программа

У Adspect есть реферальная программа, которая позволяет нашим клиентам зарабатывать деньги за привлечение новых клиентов. Реферальная программа работает по модели revenue share, то есть комиссионные отчисления рассчитываются от суммы каждой подписки, приобретенной клиентом, которого вы привлекли.

**Комиссионные отчисления составляют 5 %.** Однако, они могут быть увеличены индивидуально в зависимости от числа привлеченных клиентов. Пожалуйста, свяжитесь с нами, если у вас есть значительное присутствие на ресурсах, посвященных партнерскому маркетингу и SMM: форумах, блогах, Telegram-группах и т.п.

Комиссионные зачисляются на баланс аккаунта. Каждый раз, когда вы создаете счет на подписку, сначала расходуются средства с баланса и вычитаются из общей суммы счета, которую нужно оплатить. Это означает, в частности, что при наличии достаточной суммы на балансе подписку можно оплатить целиком из этих средств. При каждом зачислении комиссионных вы получите реферальный чек в разделе «Счета».

Ваша реферальная ссылка и список привлеченных клиентов находятся в нижней части профиля. Используйте эту ссылку для продвижения Adspect, и каждый клиент, зарегистрировавшийся по ней, будет закреплен за вами. В техническом плане, мы используем совместно cookie со сроком жизни один месяц и параметр в ссылке, которую отправляем по электронной почте при регистрации, так что даже если клиент завершит регистрацию с другого устройства, он все равно будет закреплен за вами.

Глава 12

# REST API

Adspect предоставляет REST API для программного управления потоками. API использует JSON-кодирование данных и поддерживает несколько методов для всех основных операций над потоками. Для аутентификации используется HTTP-аутентификация типа Basic, в которой ключ API передается в качестве имени пользователя, а пароль оставляется пустым. Ваш ключ API находится в вашем профиле.

Каждый запрос к API должен содержать два обязательных заголовка:

1. `Content-Type: application/json` для обозначения JSON-кодирования данных;
2. `Authorization: Basic ###` для аутентификации, где `###` заменяется на `base64(ключ API + ":")`.

Базовый URL для всех API-методов — `https://api.adspect.net/v1/`. Описания методов ниже указывают пути относительно этого базового URL. ID потоков в API-методах должны указываться как полные UUID, например `cbb360ff-5a28-41d0-9ac8-9889a01149fa`.

На текущий момент реализованы только методы для управления потоками.

## 12.1 Формат потоков

Каждый поток представляется в виде JSON-объекта, который содежит следующие свойства:

- `stream_id` — полный ID потока в формате UUID;
- `account_id` — полный ID аккаунта в формате UUID, только для чтения;
- `name` — название потока, строка;
- `mode` — режим потока, строка, одна из `Filter`, `Review`, `Money` или `White`;
- `money_pages` — массив из одного или более (до 254) объектов контент-страниц, каждый в следующем формате:
  - `page` — целевой URL или имя файла для отображения, строка;

  - `arg_passthru` — флаг проброса URL-параметров на данную контент-страницу, логический;
  - `weight` — относительный вес страницы для сплит-тестирования, целочисленный;
  - `enabled` — включена ли данная контент-страница, логический;
- `white_page` — URL белой страницы или имя файла для отображения, строка;
- `white_arg_passthru` — флаг проброса URL-параметров на белую страницу, логический или целочисленный;
- `ml_precision` — точность VLA в процентах, целочисленный;
- `cost_parameter` — имя параметра цены клика, строка;
- `sid_parameter` — имя параметра sub ID, строка;
- `cid_parameter` — имя параметра click ID, строка;
- `enable_fp` — флаг фильтрации по JavaScript-отпечаткам, логический или целочисленный;
- `paranoid` — флаг режима паранойи, логический или целочисленный;
- `allow_apps` — разрешены ли мобильные приложения, логический или целочисленный;
- `countries` — массив строк разрешенных стран в формате ISO 3166-1 alpha-2;
- `os` — массив строк разрешенных операционных систем;
- `browsers` — массив строк разрешенных браузеров;
- `languages` — массив строк кодов разрешенных языков браузера;
- `timezones` — массив разрешенных часовых поясов — целочисленных часовых сдвигов относительно UTC;
- `tz_match_ip` — проверять соответствие часового пояса браузера и местоположения, логический или целочисленный;
- `url_rules` — массив URL-правил (до 64), каждое из которых в следующем формате:
  - `param` — имя URL-параметра, строка;
  - `op` — оператор правила, один из:
    - `EXISTS` — параметр существует;
    - `NEXISTS` — параметр не существует;
    - `REGEX` — значение совпадает с регулярным выражением;
    - `IREGEX` — значение совпадает с регулярным выражением (без учета регистра);
    - `NREGEX` — значение не совпадает с регулярным выражением;
    - `NIREGEX` — значение не совпадает с регулярным выражением (без учета регистра);
    - `EQ` — значение равно аргументу;
    - `NEQ` — значение не равно аргументу;
    - `GT` — значение больше аргумента;
    - `GE` — значение больше или равно аргументу;
    - `LT` — значение меньше аргумента;
    - `LE` — значение меньше или равно аргументу;
    - `ASSIGN` — назначить новое значение параметру;

        * `RENAME` — переименовать параметр;
        * `DELETE` — удалить параметр;
    - `arg` — аргумент правила, строка;
    - `enabled` — включено ли правило, логический;
- `ua_regex` **(устарело, к удалению)** — регулярное выражение для фильтрации по user agent, строка;
- `referer_regex` **(устарело, к удалению)** — регулярное выражение для фильтрации по referrer, строка;
- `ip_on_review` — заносить все IP-адреса в черный список в режиме «Модерация», логический или целочисленный.

Пример:

```
{
   "stream_id": "1eacc6d0-875f-6f5c-bff8-00162501c2b4",
   "account_id": "1eaa2ce5-d4dd-63ec-b8a4-00162501c2b4",
   "name": "Example stream",
   "mode": "Filter",
   "money_pages": [
      {
         "page": "https://example.com/offer1?clid={clickid}",
         "arg_passthru": true,
         "weight": 10,
         "enabled": true
      },
      {
         "page": "https://example.com/offer2?clid={clickid}",
         "arg_passthru": true,
         "weight": 20,
         "enabled": true
      }
   ],
   "white_page": "white.html",
   "white_arg_passthru": 0,
   "ml_precision": 95,
   "cost_parameter": "cost",
   "sid_parameter": "sourceid",
   "cid_parameter": "",
   "enable_fp": 1,
   "paranoid": 0,
   "allow_apps": 1,
   "countries": [
      "CA",
      "US"
   ],
   "os": [
      "iOS",
      "macOS"
   ],
   "browsers": [
      "Google Chrome"
   ],
   "languages": [
      "en",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
      "fr",
      "es",
   ],
   "timezones": [
      -5,
      -6,
      -7,
   ],
   "tz_match_ip": 1,
   "url_rules": [
      {
         "param": "secretkey",
         "op": "EQ",
         "arg": "4gHzQvF2IoqeQ",
         "enabled": true
      }
   ],
   "ua_regex": "",
   "referer_regex": "",
   "ip_on_review": 1
}
```

## 12.2 GET /streams

Возвращает массив всех потоков в аккаунте.

## 12.3 GET /streams/<id>

Возвращает указанный поток.

## 12.4 POST /streams

Создает и возвращает новый поток. Укажите объект потока в JSON-формате в теле запроса.

## 12.5 PATCH /streams/<id>

Обновляет поток. Укажите объект потока в JSON-формате в теле запроса.

## 12.6 DELETE /streams/<id>

Удаляет поток.

## 12.7 index.php и ajax.php

Вы можете скачать файлы `index.php` и `ajax.php` для любого потока при помощи запросов:

- `index.php` — `GET https://clients.adspect.ai/getindex.php?sid=<id>&mode=<mode>`
- `ajax.php` — `GET https://clients.adspect.ai/getindex.php?sid=<id>&mode=ajax`

Где `<mode>` является одним из:

- `redirect` — перенаправление на внешний URL при помощи кода ответа HTTP 302;
- `iframe` — отображение внешнего URL на вашем домене в тэге `<iframe>`;
- `proxy` — отображение внешнего URL на вашем домене путем HTTP-проксирования.