IAB RUSSIA
КОМИТЕТ ПО ONLINE BRANDING
FRAUD & BRAND SAFETY WHITE PAPER

iab russia

Председатель комитета IAB Russia по Online Branding: Сафаева Эльвира, Директор по работе с клиентами Weborama в Восточной Европе и Центральной Азии.
Руководитель проекта: Аборонова Мария, Planning excellence & Brand safety lead, MediaCom.
Редактор проекта: Егор Тимофеев, РБК

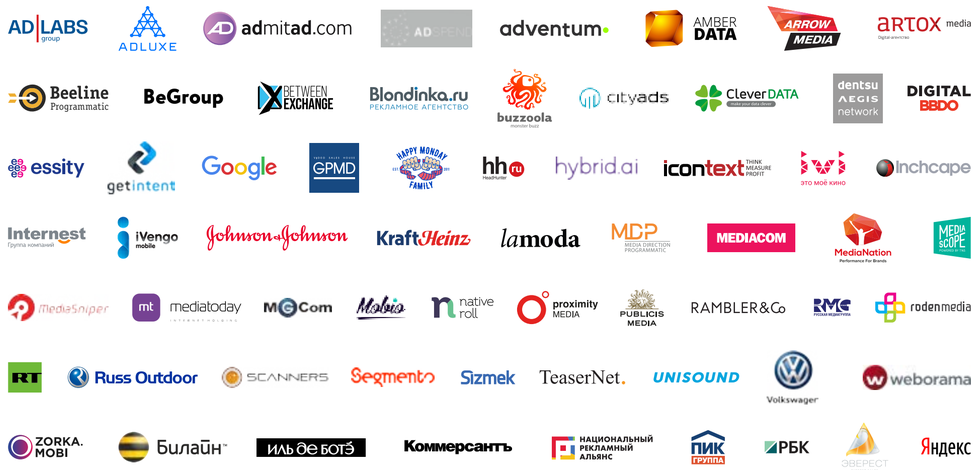
Активное участие принимали:
Виктория Игнатьева, ivi.ru
Сергей Коренков, GPM-Digital
Любовь Ячкова, IMHO
Ксения Зазулова, Initiative
Сергей Патрин, Publicis Media
Алексей Фиошкин, Admon

СОДЕРЖАНИЕ

ЗАКАЗЧИКИ ИССЛЕДОВАНИЯ

IAB Russia Fraud & Brand Safety White Paper 2018 был подготовлен по инициативе Комитета по Online Branding IAB Russia, поддержанной решением общего собрания действующих членов IAB Russia 22 ноября 2017 года.

Мы выражаем благодарность компаниям-членам IAB Russia, которые оказали активную поддержку в подготовке документа.



Благодарим за участие в подготовке документа экспертов Рабочей группы по Fraud & Brand Safety Комитета по Online Branding IAB Russia, а также представителей компаний, не входящих в состав Комитета, и, в частности, Любовь Пшеничникову (Weborama), Сафаеву Эльвиру (Weborama), Аборонову Марию (MediaCom), Егора Тимофеева (РБК), Викторию Игнатьеву (ivi.ru), Сергея Коренкова (GPM-Digital), Любовь Ячкову (IMHO), Ксению Зазулову (Initiative), Сергея Патрина (Publicis Media), Алексея Фиошкина (Admon).

ВВОДНАЯ ЧАСТЬ

ОПИСАНИЕ ИССЛЕДОВАНИЯ

В целях составления White Paper было проведено предварительное исследование среди членов рабочей группы IAB, паблишеров, агентств и рекламодателей с целью определить текущую ситуацию и основные болевые точки в сфере измерений Fraud (он же «фрод») и Brand Safety (он же «безопасность бренда» и «BS»).

Всего в исследовании принял участие 41 представитель рынка в период май-июль 2018.

Все определения к терминам будут предоставлены далее по ходу документа (блоки Fraud и Brand Safety).

УРОВЕНЬ ЭКСПЕРТИЗЫ В СФЕРЕ ВЕРИФИКАЦИИ ТРАФИКА

Следует отметить, что, хотя именно рекламодатели являются заказчиками технологий по выявлению фрода и соблюдению безопасности бренда, они же обладают минимальными знаниями и экспертизой в данной сфере. Это объясняется в первую очередь тем, что в представлении рекламодателей центрами компетенции должны становиться медийные агентства, накапливающие экспертизу и отрабатывающие эффективные рабочие процессы. Рекламодатели в данной схеме являются конечными заказчиками и получают готовые решения и результат «под ключ» (размещения с соблюдением гайдлайнов по Fraud и BS, детальные отчеты-презентации, кейсы). В том числе подобные центры компетенции ожидаются и от крупных паблишеров. И, действительно, агентства и паблишеры показывают высокий уровень компетенции или готовности повышать экспертизу и внедрять новые технологии.

Корректное определение понятия Fraud могут предоставить 56% опрошенных против 71% корректных ответов на вопрос об определении понятия BS

Рис. 1

Самый высокий процент корректных ответов по теме Fraud наблюдается среди паблишеров, так как качественные измерения трафика входят в их ежедневный рабочий процесс и требуют роста экспертизы.

В теме BS по доле корректных ответов лидируют агентства, что отражает картину распределения ролей: команда агентства, «ведущая» определенного рекламодателя, максимально погружена в ценности конкретного бренда.

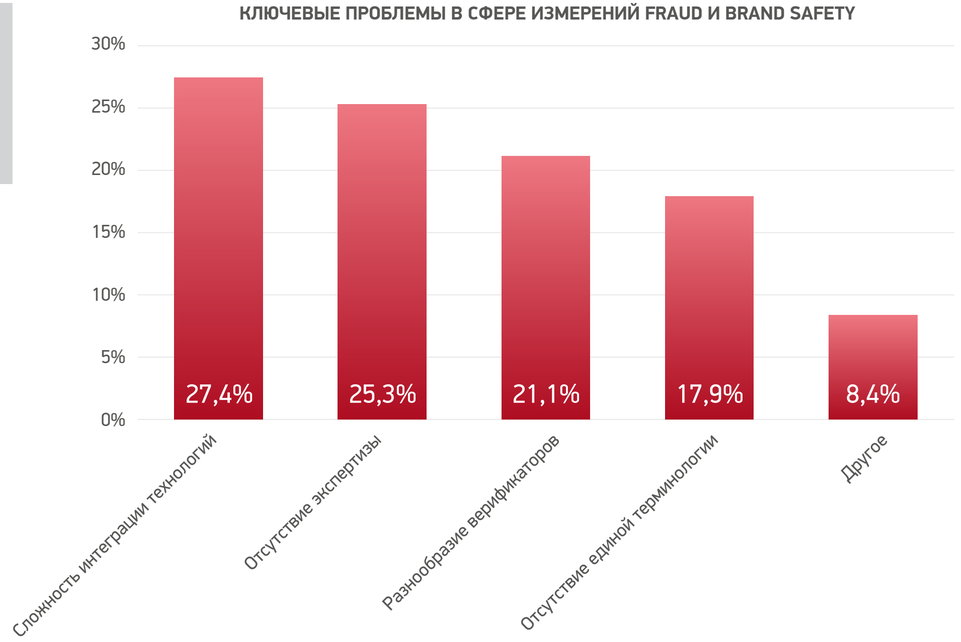


рис.2

Среди ключевых проблем в сфере измерений первое место (27,4%) по мнению опрошенных занимает сложность интеграции технологий аудита (можно предположить, что это во многом обусловлено проблемой локализации глобальных технологий под конкретные реалии Рунета), на втором месте — отсутствие экспертизы (25,3%), и на третьем — разнообразие верификаторов, иными словами — сложность выбора оптимальной технологии из списка существующих на рынке (рис. 2).

Уровень экспертизы и неравномерное ее распределение по игрокам рынка иллюстрируют рис. 3 и 4.

рис. 3

54% опрошенных заявили, что обладают экспертизой в сфере работы с Fraud, при этом основной центр компетенции находится на стороне агентств (рис. 3). Эта картина хорошо отражает рабочие процессы: как правило, рекламодатель ожидает экспертизу и готовые рабочие решения от своего агентства, а также от крупных паблишеров.

Экспертиза в измерениях и работе с Brand safety

Наличие экспертизы по игрокам рынка

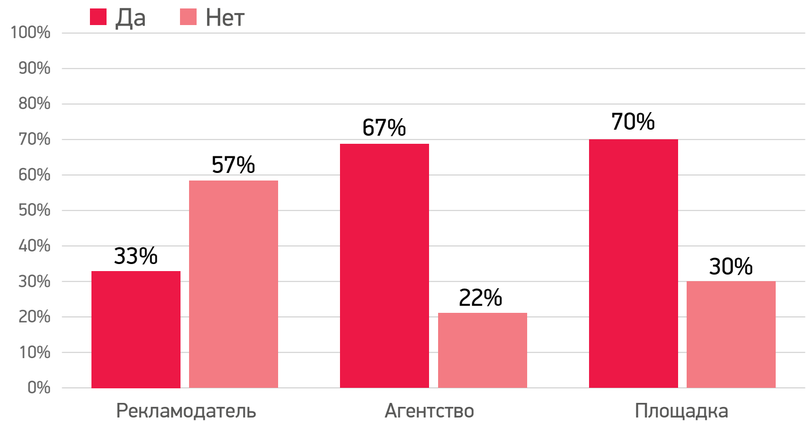


рис. 4

46% опрошенных заявили, что обладают экспертизой в сфере BS, при этом основной центр компетенции находится на стороне агентств и паблишеров. Можно отметить, что для паблишеров вопрос безопасности бренда чаще всего подразумевает отсутствие нелегального контента и возможность настройки показов рекламы в определенных категориях контента (рис. 4).

ВЕРИФИКАЦИЯ: FRAUD

83% опрошенных указали, что используют методы для определения Fraud-трафика на более или менее постоянной основе (рис. 5).

Какими методами определения Fraud трафика Вы пользуетесь?

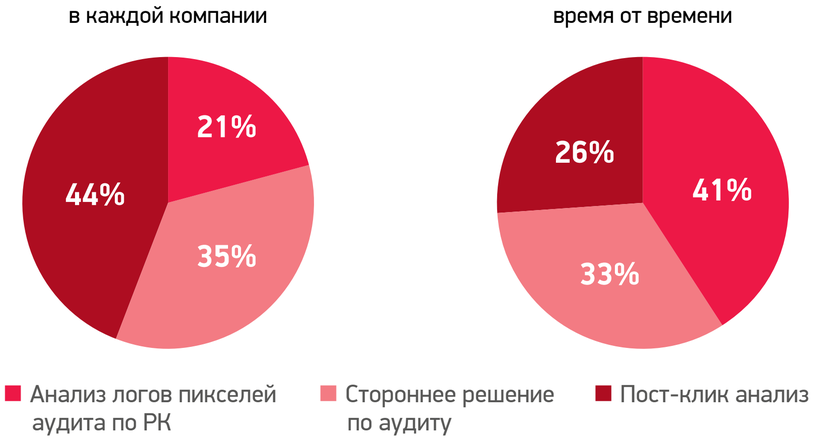


рис. 5

При этом самым распространенным из постоянных методов является анализ поведения пользователей на сайте (пост-клик).

Чаще всего игроки рынка обращают внимание на такую метрику, как общий % Fraud-трафика (44%), и значительно меньшая доля (22%) смотрит более детально на отдельные категории Fraud (рис. 6).

Какие показатели в измерениях Fraud являются для вас ключевыми?

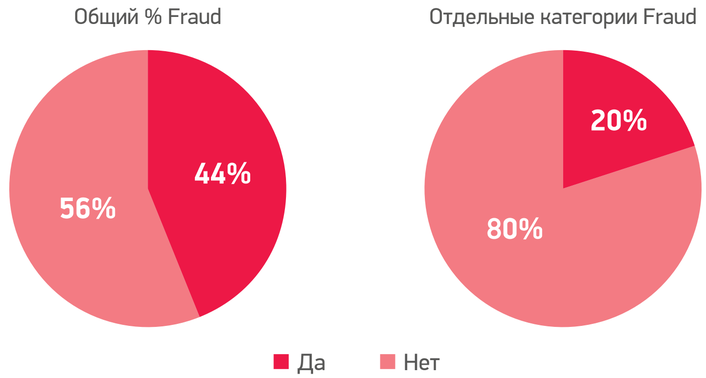


рис. 6

Основными причинами не использовать технологии для измерения Fraud являются: делегирование такого использования подрядчикам — агентствам и паблишерам (44%), отсутствие знания о технологиях (16%), отсутствие экспертизы для возможности выбора вендора (16%), сложность интеграции новой технологии (12%) и стоимость технологии (4%). (рис. 7).

рис. 7

82% опрошенных считают, что предоставление доказательств Fraud является важным аспектом измерений. При этом в качестве предпочтительного формата доказательств указывают предоставление списка источников и сценариев фрода (55,6%), скриншоты (22,2%) и пост-клик анализ (22,2%) (рис. 8).

Насколько важны доказательства фрода? В каком виде Вы их ожидаете?

рис. 8

58% опрошенных считают, что факт сертификации технологии крайне важен, и еще 30% уверены, что важнее то, как технология работает.

Среди компаний, предложенных опрошенными, осуществляющих (или тех, которые могли бы осуществлять) сертификацию технологий, лидируют IAB и MRC, затем следует ряд паблишеров, технологий и технологических компаний. Ответы приведены исходя из представлений отвечающих игроков, поэтому «хвост» в том числе из компаний, которые не предлагают своих решений, показателен (рис 9).

Для Вас важна сертификация технологии по измерению Fraud, или достаточно результата работы? Кто бы мог сертифицировать эти технологии или уже это делает?

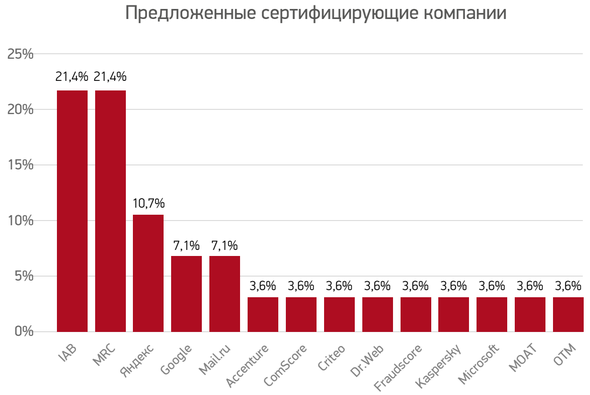
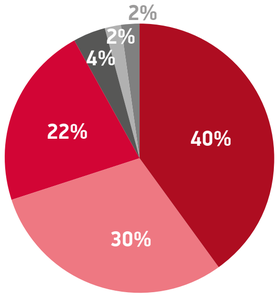


рис. 9

Среди барьеров на пути внедрения технологий по измерению Fraud игроки рынка особенно выделяют отсутствие единого подхода к определению Fraud (40%), разнообразие верификаторов, которые необходимо внедрять в сайты / сертифицировать паблишерам (30%) и отсутствие единого подхода к тому, какой процент Fraud-трафика считать допустимым (22%).



Какие барьеры Вы видите для повсеместного внедрения измерения Fraud?

- Отсутствие единого подхода в определению Fraud
- Разнообразие верификаторов, которые надо интегрировать в сайты
- Отсутствие единого подхода к тому, какой % Fraud считать допустимым
- [Высокая] Стоимость использования технологии
- Низкая осведомленность о проблеме, отсутствие экспертизы
- Отсутствие локального сертифицирующего органа

рис. 10

ВЕРИФИКАЦИЯ: BRAND SAFETY

В качестве способов выполнения требований BS 25,8% опрошенных указали использование Black-листа, то есть списка ресурсов, размещение на которых недопустимо. 24,2% опрошенных напротив, используют white-лист, то есть список ресурсов, на которых размещение должно быть ограничено. Сторонние системы аудита используют для этих целей менее 20% опрошенных (рис. 11).

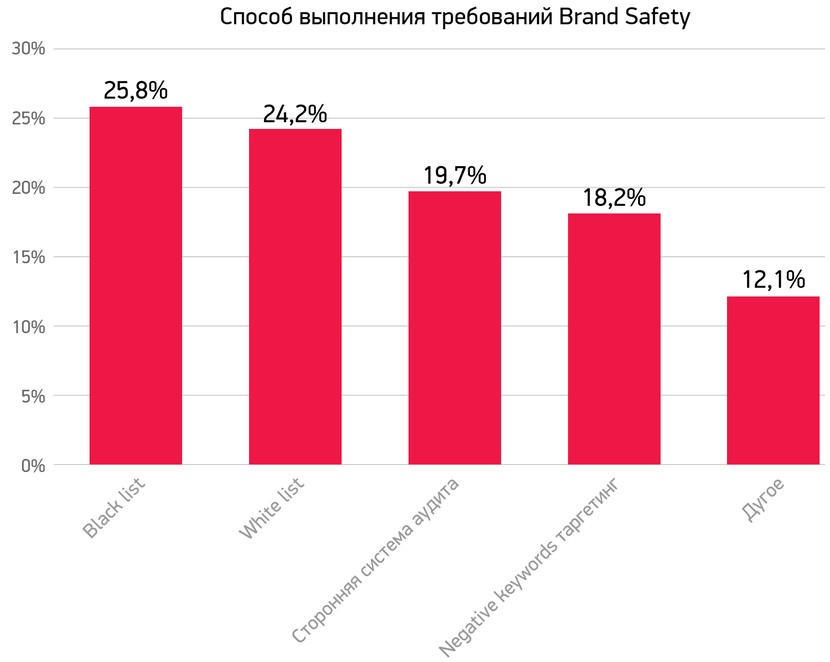


рис. 11

Основными причинами не использовать технологии для измерения BS являются: делегирование такого использования подрядчикам — агентствам и паблишерам (37%), отсутствие знания о технологиях (26%), отсутствие экспертизы для возможности выбора вендора (15%), сложность интеграции новой технологии (7%) и несоответствие возможностей технологий ожиданиям игроков (например, невозможность определения окружения плеера для каждого показа рекламы) (4%).

Отдельно стоит отметить 11% опрошенных, заявивших, что они не видят необходимости в использовании таких технологий — это в первую очередь паблишеры, уверенные, что их контент уже соответствует требованиям BS (например, по редакционной политике) (рис. 13).

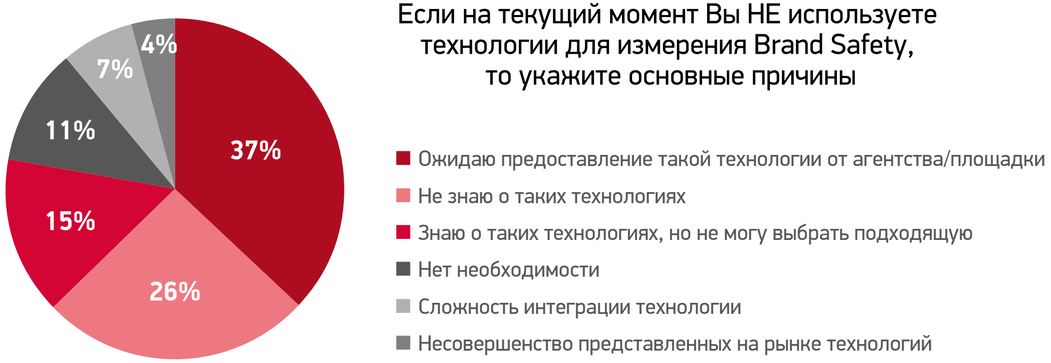


рис. 12

78% опрошенных указывают, что крайне важно получать от технологии доказательства размещения в небезопасном контенте (нарушения Brand Safety в размещении). При этом в качестве предпочтительного формата предоставления доказательств перечисляются: скриншоты (48,1%), стандартный отчет (33,3%), список адресов страниц размещения рекламы (14,8%) и предоставление логов аналитики (3,7%) (рис. 14).

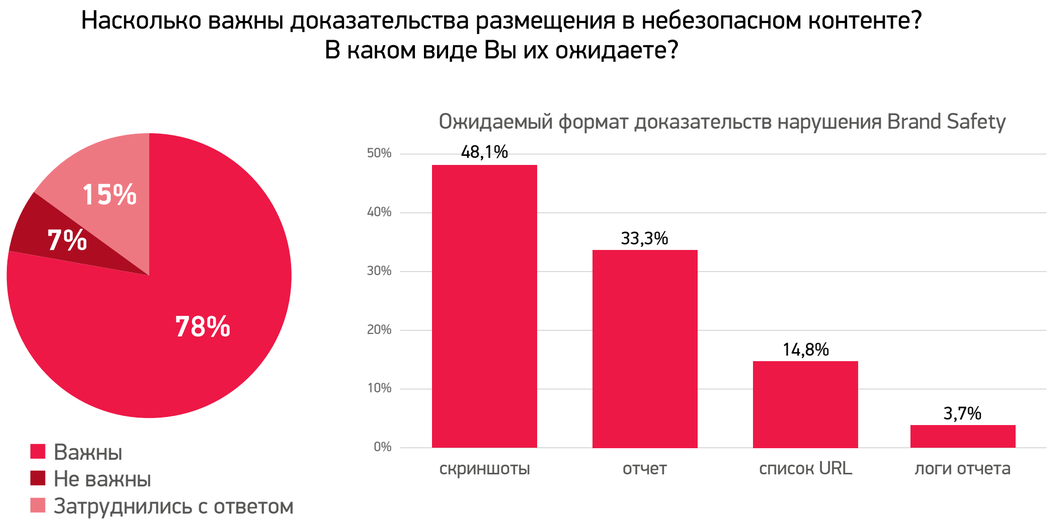


рис. 13

В вопросе о важности сертификации технологий по измерению BS мнения игроков рынка совпадают с мнениями в аналогичном вопросе про технологии для измерения Fraud.

59% опрошенных считают, что сертификация технологии крайне важна, и 41% уверены, что важнее то, как технология работает.

Среди предложенных опрошенными компаний, сертифицирующих технологии, картина также повторяется: первыми идут IAB и MRC, затем паблишеры, технологии и технологические компании (рис. 15).

Для Вас важна сертификация технологии по измерению Brand Safety, или достаточно результата работы? Кто бы мог сертифицировать эти технологии или уже это делает?

рис. 14

Среди барьеров на пути внедрения технологий по измерению BS игроки рынка в первую очередь выделяют отсутствие единого подхода к определению безопасности бренда (51%), разнообразие верификаторов, которые необходимо внедрять в сайты / сертифицировать паблишерам (22%), и отсутствие единого подхода к тому, какой процент небезопасного трафика считать допустимым (18%). Также важными препятствиями являются техническая сложность верификации контента (4%), стоимость технологий (2%) и отсутствие достаточной экспертизы (2%).

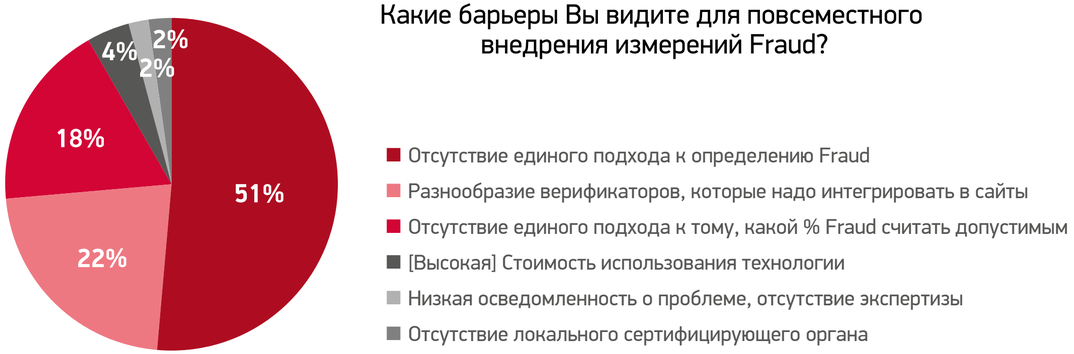


рис. 15

ВЫВОДЫ ПО ИССЛЕДОВАНИЮ

- Несмотря на то, что многие игроки рынка уже используют те или иные технологии для измерения качества инвентаря, уровень экспертизы в этой сфере в целом по рынку недостаточен, а существующая экспертиза неоднородна и фрагментарна.
- Центрами компетенции в сфере измерений являются агентства и крупные паблишеры, рекламодатели ожидают получать от них экспертизу и готовые решения.
- Основными препятствиями для внедрения измерений являются сложность технической интеграции, отсутствие экспертизы и отсутствие единого мнения рынка по ключевым вопросам измерений.
- Стоимость технологий не попала в топ-список препятствий для их внедрения, что можно толковать как готовность рынка к инвестициям в измерения.

- На рынке нет единого мнения о том, какие методы измерений должны применяться, какие метрики являются ключевыми и в каком виде должны предоставляться результаты измерений.
- Игроки рынка ожидают, что технологии измерения должны иметь сертификацию, поэтому может быть целесообразным создание локального сертифицирующего органа на базе IAB Russia.
- Тема верификации трафика является на данный момент достаточно сложной для понимания и слабо освещенной, игрокам рынка необходимо предоставить понятные и простые рекомендации и готовые рабочие процессы.
- Необходима образовательная работа и обмен опытом между существующими центрами компетенции, составление карты рынка измерений и глоссария, формирование методички по работе с измерителями.

БЛОК FRAUD

ОПРЕДЕЛЕНИЕ ПОНЯТИЯ FRAUD

Фрод – это недействительный трафик, являющийся результатом намеренной манипуляции с откруткой рекламы и/или её измерениями, либо создающий фиктивную пользовательскую активность.

Согласно стандартам IAB/MRC фродовый трафик делится на две категории: General Invalid traffic или Sophisticated Invalid traffic*.

General Invalid Traffic (GIVT) – базовый недействительный трафик, который можно идентифицировать и фильтровать с помощью стандартных проверок параметров, включающий в себя:

- Known data-center traffic – трафик, который исходит от дата-центров и не является человеческим.
- Bots, spiders, crawlers – трафик, который исходит от ботов и поисковых роботов. Определяется согласно списку от международных организаций IAB/ABC. Боты представляют из себя не человеческую активность, условно делятся на «хороших» (Google, Mediascope web crawlers, etc) и «плохих», а также могут выглядеть как реальные пользователи.
- Не человеческая активность – трафик с активностью не соответствующей человеческой. Например, клики, произошедшие до загрузки страницы в неизвестном браузере, что само по себе невозможно.

*Источник: http://mediaratingcouncil.org/101515_IVT%20Addendum%20FINAL%20(Version%201.0).pdf

Sophisticated Invalid Traffic (SIVT) – сложный для определения недействительный трафик, требующий расширенного анализа для идентификации и включающий следующие основные категории:

- Bots, spiders, crawlers - трафик, который исходит от ботов под видом реальных пользователей, но не включенный в категорию GIVT.
- Hijacked session/devices/ad tags/creative– трафик пришедшийся на ситуации, когда пользователь был принудительно перенаправлен на другой сайт, вкладку или магазин приложений как с помощью вредоносного ПО так и без него. Вредоносное ПО заставляет браузер запускать новое окно браузера без ввода пользователем.
- Hidden ads – трафик пришедшийся ситуации, когда рекламное объявление прогрузилось, но технически не может быть отображено из-за особенностей вставки кода рекламы на веб-страницу.
- Invalid proxy – трафик, который исходит из промежуточного прокси-устройства, которое существует, чтобы манипулировать подсчетами трафика или создавать/пропускать недействительный трафик. Недействительные прокси-серверы могут использоваться для маршрутизации трафика, происходящего из дата-центров, ботов или других источников, с тем чтобы их происхождение представляло собой обычный дом или бизнес.
- Adware/Malware – трафик с рекламного или вредоносного ПО, основная задача которого стимулирование манипуляций с измерениями
- Pixel Stuffing – технология «обвешивания» всего сайта, поддерживаемого рекламой, в пиксель размером 1x1, что приводит к отображению не просматриваемых объявлений.

СЛОВАРЬ ТЕРМИНОВ

Бот – специальная программа, выполняющая автоматически и/или по заданному расписанию какие-либо действия через интерфейсы, предназначенные для людей.

Дата-центр или центр (хранения и) обработки данных (ЦОД/ЦХОД) – это специализированное здание для размещения (хостинга) серверного и сетевого оборудования и подключения абонентов к каналам сети интернет. Дата-центр исполняет функции обработки, хранения и распространения информации, как правило, в интересах корпоративных клиентов — он ориентирован на решение бизнес-задач путём предоставления информационных услуг.

Поисковый робот – программа, являющаяся составной частью поисковой системы и предназначенная для перебора страниц интернета с целью занесения информации о них в базу данных поисковика. По принципу действия «паук» напоминает обычный браузер. Он анализирует содержимое страницы, сохраняет его в некотором специальном виде на сервере поисковой машины, которой принадлежит, и отправляется по ссылкам на следующие страницы.

Прокси-сервер (Proxy) – промежуточный сервер (комплекс программ) в компьютерных сетях, выполняющий роль посредника между пользователем и целевым сервером (при этом о посредничестве могут как знать, так и не знать обе стороны), позволяющий клиентам как выполнять косвенные запросы (принимая и передавая их через прокси-сервер) к другим сетевым службам, так и получать ответы. Прокси-сервер позволяет защищать компьютер клиента от некоторых сетевых атак и помогает сохранять анонимность клиента, но также может использоваться мошенниками, для скрытия адреса сайта, уличённого в мошенничестве, изменения содержимого целевого сайта (подмена), а также перехвата запросов самого пользователя.

БЛОК BRAND SAFETY

ОПРЕДЕЛЕНИЕ ПОНЯТИЯ BRAND SAFETY

Brand safety – защита бренда рекламодателя и его рекламных креативов от упоминания в негативном/неблагоприятном для репутации бренда информационном контексте.

В настоящий момент верификация brand safety специализированными тулами включает в себя анализ ключевых слов на странице и метатэгов под изображениями. Технологических средств анализа самих изображений и видеоряда у данных систем пока что нет.

Поддержание безопасности бренда во время рекламной кампании в интернете не позволяет рекламным сообщениям показываться рядом с неподходящим или нелегальным контентом, что минимизирует риск неправильного выбора площадки, защищает репутацию бренда.

Общие типы контента с неблагоприятным содержимым, согласно IAB:**

- контент с возрастными ограничениями (Adult Content, «для взрослых»);
- призывы к опасным или незаконным действиям;
- спорные темы: оккультизм, табуированные темы, нетрадиционный образ жизни и т.д.;
- нарушение авторских прав;
- наркотики, алкоголь и другие опасные для здоровья человека вещества;
- пропаганда употребления наркотиков, алкоголя и других веществ, оборот которых запрещен или ограничен законодательством;
- пропаганда насилия или жестокости;
- контент, содержащий недействительный трафик (GIVT и SIVT);
- разжигание ненависти / профанация;
- вирусы, вредоносные файлы, шпионские программы;
- политические темы / религия;
- немодерируемый пользовательский контент.

** IAB, Guidelines for the Conduct of Ad Verification February 14, 2012
https://www.iab.com/wp-content/uploads/2015/06/Ad-Verification-Guideline-for-the-Conduct-of.pdf

Другие ограничения по типам контента не представляется возможным стандартизировать для всего рынка. Однако можно выделить факторы, от которых эти ограничения зависят:

- этика (например, некорректно размещать рекламу мясных продуктов на сайтах с вегетарианской тематикой);
- внутриотраслевые соглашения (носят рекомендательный характер, но их несоблюдение может повлечь репутационные риски для компании. В качестве примера можно привести международное соглашение, подписанное крупнейшими производителями продуктов питания (в том числе, Coca-Cola, MARS, PepsiCo, Nestle и т.д.) по ограничению рекламы сладкой продукции, направленной на детей младше 12 лет);
- внутренние корпоративные политики и политики размещения (например, некоторые детские бренды крупных рекламодателей являются исключениями из внутриотраслевых соглашений и имеют «розовый паспорт», который позволяет таргетировать рекламу на детей. Также для большинства крупных рекламодателей недопустимым считается размещение на сайтах, содержащих нелицензионный контент (однако до сих пор нет точного и общепринятого определения «пиратского» сайта));
- соответствие цели рекламной кампании (например, появление рекламы авиакомпании рядом с новостями об авиакатастрофе может вызвать у пользователей неприятную ассоциацию с брендом авиакомпании. Однако важно, что подобные новости привлекают большую аудиторию, и вполне возможно, что для бренда страховой компании данный контекст будет релевантен).

ВЕРИФИКАЦИОННЫЕ ТУЛЫ: ОБЗОР

В рамках работы с верификационными тулами необходимо разделять их на два блока:

1. **Ad server** – система управления рекламой, технологический сервис для размещения рекламных объявлений, включающий в себя хостинг рекламных материалов (баннеры, видео), транслирование рекламы на сайты, в соответствии с запросом паблишеров и реализация аудита доставки трафика.

   Экосистема делится на два типа инструментов в зависимости от функционала:

   а) Ad server паблишера – для реализации запуска рекламных кампаний. На российском рынке представлены компаниями Adfox, Google Ad Manager (DoubleClick for Publishers), Adriver, RB.Mail, etc.;

   б) Ad server рекламодателя – для независимой аналитики рекламных размещений. На российском рынке представлены компаниями Adriver, Weborama, Sizmek, Google Campaign Manager (DoubleClick), etc.

2. **Verification tool** – инструмент, специализирующийся на верификации качества трафика, а именно viewability, fraud и brand safety (анализе контента страницы, на которой была размещена реклама бренда).

Для измерения fraud и brand safety мы рекомендуем использовать тулы, которые обеспечивают измерение Fraud и Brand Safety по стандартам MRC и/или IAB Tech Lab:

- Adloox
- Admon
- Google Marketing Platform (DoubleClick)
- DoubleVerify
- Integral Ad science
- MOAT
- Sizmek

Также на российском рынке есть тулы, которые предоставляют услуги по верификации Fraud и Brand Safety не по стандартам IAB/MRC, а по собственной методологии.

- Adfox (для паблишеров)
- Adriver
- Brainrus (для паблишеров, ограничение по форматам)
- Native-roll (для паблишеров, ограничение по форматам)
- RB.Mail.ru (для паблишеров)
- Weborama
- etc.

КОММЕНТАРИИ ОТ ВЕРИФИКАЦИОННЫХ ТУЛОВ

В рамках подготовки документа мы так же собрали наиболее распространённые вопросы к верификационным тулам.

Ниже приводим их с ответами от всех систем, работающих по стандартам IAB/MRC.

Показываете ли вы Measurement rate / Validation rate по этим метрикам? Если нет, то готовы ли?

(Measurement/Validation rate – процент показов от общего количества поставленного трафика, который верификационный тул смог проанализировать на качественные метрики)

MOAT

Мы показываем количество проанализированных показов, включая показы, где был обнаружен недействительный траффик.

Adloox

Да, метрика доступна в интерфейсе системы.

Sizmek

Да, конечно, показываем.

Integral Ad Science

Да, доступно в интерфейсе.

DoubleVerify

Да, доступно в интерфейсе. Так же мы даем рекомендации по устранению причин низкого показателя Measurement rate.

Admon

Нет, но готовы показать.

Google Marketing Platform (DoubleClick)

Да, показываем.

Применяется ли кириллица для Brand Safety? Есть ли возможность в открытых источниках или в рамках частного запроса получить информацию о том, какие слова формируют ту или иную категорию контента?

MOAT

Да, наш продукт работает с русским языком, и мы можем выслать клиентам список слов, формирующих каждый из сегментов.

Adloox

Да, наш продукт работает с русским языком, но к сожалению, содержание сегментов мы не раскрываем.

Sizmek

Да, решение работает для русского языка/кириллицы. Мы не оперируем словарями. Технология Sizmek основана на семантическом анализе, и подход на основе ключевых слов для нас не работает. Нам просто нечего раскрывать.

Впрочем, словари могут быть разработаны для дополнительной защиты (или DCO-таргетингов) для стадий пре-бида и креативной оптимизации.

Integral Ad Science

Да, наш продукт работает с русским языком, но к сожалению, раскрыть содержание сегментов мы не можем.

DoubleVerify

Наше решение работает с любым языком.

Admon

Да, наше решение работает с кириллицей.

Google Marketing Platform (DoubleClick)

Да, наш продукт работает с русским языком. Клиенты могут определить, какие слова они хотят заблокировать. Они так же могут выбрать стандартные категории, предлагаемые Google, либо сформировать на их основе собственные кастомные категории.

Будете ли вы предоставлять бенчмарки клиенту (больше или меньше среднего метрики кампании, чем вообще по рынку)?

MOAT

Мы предоставляем как глобальные, так и региональные бенчмарки по отдельным странам.

Adloox

В системе доступны средние глобальные показатели.

Sizmek

Да, планируем выпускать официальные справочные цифры по рынку.

Integral Ad Science

Стараемся предоставлять локальные бенчмарки в том числе.

DoubleVerify

Мы предоставляем как глобальные, так и региональные бенчмарки по отдельным странам, так же мы готовы предоставлять бенчмарки для клиентов, с учетом их истории размещений.

Admon

Да, по запросу.

Google Marketing Platform (DoubleClick)

Нет, мы не предоставляем данные по рынкам и не раскрываем детали размещений конкурентов наших клиентов.

Можем ли мы говорить, что ваше определение фрода соответствует стандартам IAB/MRC?

MOAT

Да, 100%. MOAT аккредитован IAB/MRC на определение фродового траффика.

Adloox

Да, 100%. Adloox аккредитован IAB/MRC на определение фродового траффика.

Sizmek

Да, мы придерживаемся всех стандартов, а также приводим дополнительные параметры.

Integral Ad Science

Да, IAS аккредитован IAB/MRC на определение фродового траффика.

DoubleVerify

Да, мы аккредитованы IAB/MRC на определение фродового траффика.

Admon

Да, мы работаем по индустриальным стандартам IAB/MRC.

Google Marketing Platform (DoubleClick)

Да, мы аккредитованы IAB/MRC на определение фродового траффика.

Что вы считаете Brand Safety? Дайте, пожалуйста, определение.

MOAT

В нашей системе безопасным будет тот показ, который был размещен в контенте, не содержавшим слова, попадающие в стандартные категории небезопасного траффика IAB – например, «терроризм».

Так же мы создаем для клиентов кастомные списки слов, соответственно, для разных клиентов безопасными могут быть разные типы контента.

Adloox

Размещение рекламы в контенте, который был предварительно проверифицирован на предопределенные категории контента и исключает критические для бренда ключевые слова.

Sizmek

В нашем понимании небезопасные показы/среда/инвентарь — это любое окружение, потенциально способное навредить бренду в восприятии потребителей в случае некоего ассоциированного взаимодействия бренда с таким окружением (показ рядом, участие в чём-либо, упоминание где-то и т.д).

У бренда может быть политика по контенту, может и не быть. В любом случае, есть общепонятные негативные темы.

Также для отдельных категорий или брендов могут существовать собственные критерии (например, неблагоприятные темы для автоиндустрии).

Под понятие Brand Safe в таком случае подпадает всё то окружение, которое не несёт в себе никаких рисков для бренда.

Integral Ad Science

Размещение рекламы в контенте, который может нанести вред бренду.

DoubleVerify

Настройка определенный контекстуальных таргетингов и выбор только того инвентаря, который обеспечит выполнение политик безопасности бренда.

Admon

Brand safety – практика определения параметров рекламных размещений, которые соответствуют рекламной политике бренда и не вредят его репутации.

Основные категории:

- креатив (соответствие брендбуку, актуальность (не использование устаревших креативов), соответствие copyright);

- окружение (white/black lists сайтов, содержание страниц);

- формат размещения (кликандеры/попандеры/пуши, размер изображений, допустимое разрешение);

При запуске кампании рекламодателю предлагается заполнить опросник со списком возможных угроз и отметить что для него является приемлемым, а что нет.

Google Marketing Platform (DoubleClick)

Для многих брендов определенные типы контента всегда будут недопустимыми (например, терроризм, контент 18+, и т.д.). Однако так же много брендов, чьи требования Brand Safety более гибкие, если размещение происходит в подходящем контексте.

Стратегия бренда и его политики безопасности тесно связаны. Для продвижение бренда и его ценностей важно обеспечивать его размещение в релевантном для него окружении.

Для Brand Safety вы делаете только распознавание контента по тексту, но делается ли распознавание картинок и видео на страницах?

MOAT

Изображения и видео – это те типы контента, которые мы пока не можем верифицировать, но мы работаем в этом направлении.

Adloox

В данный момент мы не делаем распознавание изображений и видео, но это станет доступно в 2019 году. Пока что мы можем заблокировать размещение рекламы, если контент страницы определяется системой как небезопасный. После этого в ручном режиме отсматриваются страницы, отмеченные Adloox ботом. Это обеспечивает двойную проверку сайтов, которые мы блокируем, и дает контроль качества не только текстового контента, но и визуального.

Sizmek

Наше решение работает только с текстами (семантический анализ). Впрочем, фактор графического содержания, где это возможно, учитывается благодаря анализу служебных параметров (например, метатегов). Планы по включению графики в анализ у нас есть, сроки привести не можем.

Integral Ad Science

IAS анализирует мета данные изображений (текст в коде изображения, описывающий то, что на нём изображено), но не предоставляет непосредственно распознавание изображений. Для видео решение еще не до конца разработано.

DoubleVerify

Только распознавание мета данных изображений.

Admon

Только текст на данном этапе.

Google Marketing Platform (DoubleClick)

Классификация контента сайтов происходит автоматически кроулером Google и семантическими технологиями. На основании данных этого анализа определяется основная тематика каждой веб-страницы. Распознавание изображений и видео не производится.

Какая ваша рекомендация по сравнению результатов разных верификаторов?

MOAT

Основной фактор – это «измеримость». Все аккредитованные системы должны отчитываться о своей способности замерить видимость, недействительный траффик и т.д. Если вы хотите сравнить результаты MOAT с другой системой по тем же самым размещениям, то более правильными в таком случае будут данные системы, которая смогла верифицировать больший объем траффика.

Adloox

Всегда есть небольшая разница в данных между разными тулами. Допустимо менее 5%. Также, некоторые компании не отображают все категории SIVT – но это будет стандартизировано в рамках следующего заседания MRC по соблюдению стандартов.

Sizmek

Для начала, рекомендуем, конечно, обсудить. Мы всегда готовы связаться и обсудить цифры.

Для сравнения данных необходимо сравнивать одинаковые показатели. У всех вендоров разные таксономии, встречаются выходящие за рамки рекомендаций IAB/MRC параметры.

Технологии могут отличаться в подходах к замеру стандартных показателей или Brand Safety. Конкретные случаи должны изучаться отдельно.

Мы верим, что постоянные измерения в максимальном объёме будут демонстрировать надёжные цифры, несмотря на различие в методиках.

Integral Ad Science

В первую очередь нужно всегда выбирать партнера, который работает со стандартами IAB/MRC и/или имеет соответствующую сертификацию. Из-за разных настроек у систем результаты могут варьироваться, но вы должны для себя выбрать тот источник, которому сможете доверять.

DoubleVerify

Необходимо учитывать разные подходы тулов к измерениям и сравнивать между собой результаты систем, которые работают в рамках одних и тех же стандартов.

Admon

Обычно мы предоставляем скриншоты и другие доказательства.

СЕРТИФИКАЦИЯ ВЕРИФИКАЦИОННЫХ ТУЛОВ

В настоящий момент из индустриальных аккредитаций есть сертификация компанией MRC.

Media Rating Council (MRC) – глобальная организация, целью которой является улучшение качества аудиторных измерений путем оценки сервисов и предоставления лучшего понимания применения (и ограничений) информации проведенной оценки. Центральным элементом мониторинга MRC является ежегодный внешний аудит различных технологий, который проводится специализированной командой независимых аудиторов. Компании, работающие в США, могут получить аккредитацию MRC по предоставляемым ими сервисам, которая будет подтверждать способность системы предоставлять тот или иной сервис.

Актуальные данные по наличию/отсутствию аккредитации на Fraud и Brand safety у тулов, которым доступна аккредитация MRC, вы можете найти на официальном ресурсе MRC:

http://mediaratingcouncil.org/June%202017%20MRC%20GIVT%20Status%20Report%20for%20Accredited%20Digita...

http://www.mediaratingcouncil.org/Accredited%20Services.htm

Относительно работы с российским рынком приводим комментарий компании MRC:

В ближайшем будущем MRC не планирует проводить аудиты сервисов, не работающих на территории США. Однако возможно проведение международных аудитов компаний, не имеющих представительств в США и не работающих с американскими клиентами, если членами MRC будет принято такое решение, и если такой аудит будет иметь высокий приоритет для индустрии.

Таким образом, аккредитация от MRC локальных тулов и решений, учитывающих в своей методологии стандарты MRC, практически не представляется возможным.

ОБЩИЕ ПРАВИЛА ПО РАБОТЕ С ВНЕШНИМИ ВЕРИФИКАТОРАМИ

Нужно понимать, что сертификация тула не дает 100% гарантии качества предоставляемого сервиса, а только подтверждает его наличие. Для того, чтобы определиться с подходящим тулом, лучшим вариантом будет проводить A/B тесты с разными верификаторами и выбирать на основании их результатов.

Также мы предлагаем общие подходы к работе с верификаторами от паблишеров и рекламных агентств.

ПАБЛИШЕРЫ

Промер Fraud и Brand Safety становится неотъемлемой частью рекламной digital экосистемы. В процесс измерения вовлечены как продавцы, так и покупатели. Продавцы производят измерения с целью контроля инвентаря своих поставщиков и возможности гарантировать достижение определенных качественных показателей для своих рекламных продуктов. Рекламодатели контролируют выполнение заявляемых продавцами качественных показателей.

На рынке представлен целый ряд технологических решений, занимающихся замерами Fraud и Brand Safety, также рядом клиентов используются собственные методики выявления нарушений. Каждое из решений имеет собственную систему маркеров и алгоритмы работы. В этой ситуации очевидна неизбежность расхождения в результатах измерения, произведенных разными поставщиками. Кроме того, опыта работы с предшествующими системами арбитража (пиксели на показ, например) показывает невозможность достижения 100% точности измерения и отсутствия потерь и ошибок в работе технологии.

Для полноценного функционирования системы мониторинга и предотвращения мошенничества в digital рекламе необходимо прийти к согласованной системе взаимодействия всех сторон, участвующих в процессе измерения (Seller, Buyer, Measurement tool), которая бы учитывала все особенности и реальную практику измерений. Важно понимать, что полноценное измерение включает в себя и сравнительную аналитику замеров, произведенных различными технологическими решениями и постоянное обновление, и модификация самих инструментов, являющуюся результатом такой аналитики.

Для иллюстрации того, как работает эта система, мы подготовили несколько примеров из реальной практики:

Пример 1

Решение по промеру от одного из измерителей стабильно показывало высокий уровень SIVT Fraud в категории AdWare, при этом процент фиксируемых фрод-показов не зависел от конкретных площадок, на трафике которых проводились измерения, и составлял порядка 24%. Анализ логов показал:

- С одной стороны, основной причиной, по которой измеритель относит показы к фроду, является то, что такие показы пришлись на «устаревшие» версии браузера Chrome (как правило, вредоносное рекламное ПО действительно блокирует обновление браузера до новой версии).
- С другой стороны, измеритель некорректно определял сам браузер и относил к устаревшим версиям Chrome текущую версию Яндекс Браузера.

На основании проведенного анализа измеритель скорректировал свои алгоритмы по определению браузеров, что, как следствие, привело к снижению фрода в категории SIVT AdWare до 1-2%.

Пример 2

Решение по промеру измерителя показывало отсутствие фрода на трафике одной из кампаний, в то же время статистика по пост-клику показывала аномальное поведение некоторых пользователей, пришедших на сайт с клика по рекламе.

На основании статистики по пост-клику удалось выявить сегменты инвентаря, с которых приходили пользователи с «нетипичным» поведением, после чего измеритель смог провести дополнительный анализ данных сегментов.

Результаты анализа показали, что появились новые методы генерации фрод-трафика, ранее не известные измерителю. В результате измеритель доработал алгоритмы распознавания мошеннического инвентаря, что позволило локализовать и отключить эти источники на уровне селлера.

Важно отметить, что сложность алгоритмов определения фрода отличается для разных типов такого фрода. Если GIVT фрод определяется достаточно простыми алгоритмами, основанными на анализе ip адресов, версий браузеров и т.д., то для определения SIVT фрода используются сложные алгоритмы, основанные на анализе многих факторов и поведения сразу многих пользователей, т.е., по сути, строится модель «нормального» поведения пользователя, а отклонения от этой модели считаются фродом.

При этом любая модель подразумевает некоторые допуски и, как следствие, неизбежно возникают погрешности измерения. Так же необходимо учитывать и то, что каждый измеритель самостоятельно разрабатывает алгоритмы определения фрода, что приводит к тому, что два измерителя на одном и том же инвентаре могут показывать несколько отличающиеся друг от друга результаты.

Рекомендации по правилам взаимодействия сторон при проведении измерений.

С учетом накопленного опыта и принимая во внимание то, что алгоритмы определения GIVT и SIVT фрода различаются по сложности, рекомендуется детально разбирать каждый случай обнаружения фрода.

Компании-заказчику рекомендуется сформулировать критерии, определяющие, что они считают критическим уровнем фрода и коммуницировать их для компании-измерителя. Компания-заказчик будет детально рассматривать случаи фрода, превышающие эти пороги и им потребуется взаимодействие с компанией-измерителем.

К примеру: если показатель GIVT фрода превышает 1% или показатель SIVT фрода превышает 10%.

Для анализа фрода поставщик инвентаря от измерителя может потребовать предоставить следующие данные:

- В случае, если замер проводился измерителем, работающим по стандартам IAB/MRC (см. блок «Верификационные тулы»), предоставляется отчет (или доступ к онлайн-статистике), в котором в разбивке по дням будет указано количество промеренных показов, количество показов, которое отнесено к GIVT (с разбивкой по категориям), количество показов, которое отнесено к SIVT (с разбивкой по категориям).
- В случае, если замер проводился другими измерителями, предоставляется необходимая для анализа детализация.

  К примеру, логи с указанием времени показа, полного User-agent, referrer, домена.

Как правило, детальные логи по промеру как на стороне поставщика инвентаря, так и на стороне измерителя хранятся ограниченное время ввиду их объема. В связи с этим необходимо уточнять срок хранения данных у компании-измерителя, чтобы гарантировать, что данные по рассматриваемому трафику не были удалены, и инициировать анализ причин превышения пороговых значений с учетом этого срока.

Перед поиском причин фрода необходимо убедиться, что общая статистика по показам (досмотрам, кликам) между поставщиком инвентаря и измерителем расходится не более чем на 10%. В противном случае перед поиском причин фрода необходимо выяснить и устранить причину общего расхождения статистики между поставщиком инвентаря и измерителем.

В случае, если общий уровень фрода по кампании не превышает пороговых показателей, но есть превышения по отдельным сайтам, поставщик инвентаря должен принять такие показатели во внимание и, в случае, если показатели будут подтверждены внутренним аудитом поставщика, исключить такие сайты из пула инвентаря.

Все решения о наличии или отсутствии фрода должны основываться на анализе промера показа рекламных сообщений. Любые дополнительные источники информации (статистика и логи с посадочной страницы, поведение пользователя на такой странице) должны приниматься во внимание, но не могут использоваться для оценки уровня фрода применительно к показам рекламной кампании.

РЕКЛАМНЫЕ АГЕНТСТВА

Для качественной работы с fraud и brand safety в первую очередь нужно изучить определения этих понятий – для этого публикуется данный документ. Во вторую очередь рекомендуем для каждого размещения использовать верификационные тулы, которые замеряют fraud и brand safety по стандартам IAB/MRC.

В рамках анализа fraud необходимо разделять общий показатель на категории GIVT и SIVT. Результаты нужно разбирать в трехстороннем порядке с паблишером и верификационным тулом, чтобы понять, что привело к отнесению тулом траффика к тому или иному виду fraud, не имела ли место ошибка. Так как паблишер и рекламодатель могут использовать разные верификационные тулы, для анализа данных необходимо сравнивать одинаковые показатели с допущением погрешности в +/- 10-15%. У всех вендоров разные таксономии, встречаются выходящие за рамки рекомендаций IAB/MRC параметры.

Для анализа brand safety перед началом размещения необходимо согласовать с рекламодателем, какие категории контента/отдельные ключевые слова являются для него небезопасными, где его размещать категорически нельзя, и получить подтверждение от паблишера, что он может обеспечить открутку размещения с учетом требований рекламодателя. После того, как размещение состоялось, опять же нельзя исключать анализ статистики верификатора клиента и данных площадки, особенно если это разные тулы. Каждый верификатор имеет свои критерии отнесения контента к той или иной категории, и статистики могут расходится. Обязательно нужно учитывать это и проверять, не было ли ошибки с той или иной стороны.

В целом бренд должен определить для себя, какой %fraud и non-brand safe показов для него будет основанием для отнесения сайта в black list и выбирать стратегию размещения, относительно этого подхода. В расширенном виде к этим метрикам должен быть так же добавлен бенчмарк по Viewability.

О IAB RUSSIA

The Interactive Advertising Bureau (IAB) Russia

Некоммерческое партнерство содействия развитию интерактивной рекламы входит в международную сеть ассоциаций IAB, основная задача которой – рост и развитие рынка интерактивной рекламы. Отделения IAB успешно работают в 43 странах на 4 континентах.

Приоритетными направлениями деятельности The Interactive Advertising Bureau (IAB) Russia являются:

- Образовательная деятельность;
- Работа над формированием индустриальных стандартов, гайдлайнов и глоссария;
- Проведение отраслевых мероприятий, включая MIXX Conference и MIXX Awards;
- Проведение исследований в области интернет рекламы с учетом имеющихся международных методологий и практик в этой сфере.

Контакты:
127018, г. Москва, ул. Полковая, д.3, стр. 3, этаж 4.
телефон/факс: +7 (495) 662 39 88
email: add@iabrus.ru
www.iabrus.ru

Fraud & Brand Safety White Paper 2018 подготовлен Комитетом по Online Branding IAB Russia.
Руководитель проекта Мария Аборонова.
Октябрь 2018 года