СТАНДАРТ АРИР

по классификации сложного недействительного трафика

(SIVT — Sophisticated Invalid Traffic)

Комитет по борьбе с фродом

Сопредседатели:

Виктория Кинаш, Яндекс

Жанна Смолицкая, Weborama

Сергей Игнатов, Admon.ai

Митя Горелик, MCCom

Москва, 2026

арир

Содержание

Благодарности

Виктория Суровцева / Яндекс

Жанна Смолицкая / Weborama

Ксения Святова / Weborama

Наталья Лифатова / Weborama

Ксения Савинич / Weborama

Мария Климова / TargetADS

Вячеслав Марков / TargetADS

Роман Филиппов / AdRiver

Роман Кохановский / AdRiver

1 Цель и область применения

Настоящий документ устанавливает единую классификацию сложного недействительного трафика (SIVT) для интернет-рекламы и единые правила отнесения рекламных событий к четырём верхнеуровневым категориям. Цель стандарта — обеспечить сопоставимость отчётности верификаторов, бенчмарков и результатов рекламных кампаний.

Стандарт применяется к рекламным событиям, для которых верификатор располагает достаточными данными: рекламными запросами, показами, кликами, видео-событиями, установками, конверсиями и иными измеряемыми взаимодействиями. Конкретный набор поддерживаемых сред и событий раскрывается в методологии верификатора.

Документ определяет классификацию, границы категорий и правила отчётности. Он не устанавливает единых алгоритмов, моделей, порогов или обязательных списков: верификаторы могут использовать собственные технические методы при условии соблюдения общей логики классификации.

2 Термины и место SIVT в системе стандартов

- GIVT (General Invalid Traffic) — базовый недействительный трафик, который можно идентифицировать и фильтровать с помощью стандартных проверок параметров (известные дата-центры, краулеры по User-Agent, избыточная активность по базовому порогу, небраузерные HTTP-заголовки, клики без показов, повторные клики, недействительные размеры размещений).
- SIVT (Sophisticated Invalid Traffic) — сложный для определения недействительный трафик, требующий расширенного анализа для идентификации.
- Invalid Traffic (IVT) — недействительный трафик, являющийся результатом намеренной манипуляции с откруткой рекламы и/или её измерениями либо создающий фиктивную пользовательскую активность.
- IVT Total — совокупный объём недействительного трафика, включающий GIVT Total и SIVT Total.

Ключевой принцип: SIVT является классификацией после GIVT. Событие, уже отнесённое к GIVT, не должно повторно учитываться в SIVT, даже если у него присутствуют дополнительные сложные сигналы.

3 Обязательная последовательность верификации

Для сопоставимости результатов применяется следующая логическая последовательность. Технически проверки могут выполняться параллельно, но дедупликация и отчётность должны воспроизводить именно этот порядок.

- Этап GIVT. Ко всему исходному объёму применяются категории действующего GIVT Стандарта АРИР. Выявленные события исключаются из дальнейшей SIVT-классификации.
- Этап SIVT. Только оставшийся после GIVT объём проверяется на четыре категории настоящего стандарта. Каждое событие включается в SIVT Total один раз.

- Этап видимости. Только после исключения GIVT и SIVT для валидных отрисованных показов определяется видимость в соответствии со Стандартом АРИР по измерению видимости.

Расчётная логика: IVT Total = GIVT Total + SIVT Total после дедупликации. Валидный трафик = исходный учитываемый объём минус IVT Total. Видимость рассчитывается на валидных показах, а не используется как способ определения IVT.

4 Общие правила классификации SIVT

- Однократный учёт. Одно рекламное событие включается в IVT Total только один раз. Дополнительные сигналы могут сохраняться как служебные атрибуты, но не суммируются повторно.
- Основной механизм нарушения. Категория выбирается по тому механизму, который непосредственно сформировал недействительное событие: автоматизация, компрометация ПО, мотивированное действие человека либо манипуляция инвентарём/измерением.
- Приоритет доказуемого сигнала. Более прямое и технически подтверждаемое нарушение имеет приоритет перед косвенной поведенческой интерпретацией. Если нарушение можно подтвердить детерминированными данными (например, логами для рекламодателя или подписью источника инвентаря), такая классификация считается приоритетной.
- Proxy/VPN/IP rotation не являются IVT сами по себе. Они используются только как дополнительные сигналы в составе одной из четырёх категорий и не образуют отдельной категории.
- Простые пороговые и списочные признаки относятся к GIVT. SIVT не дублирует известные дата-центры, известных краулеров по User-Agent, избыточную активность по базовому порогу, небраузерные HTTP-заголовки, клики без показов, повторные клики и недействительные размеры размещений.
- Видимость и качество контакта не являются SIVT сами по себе. Невидимость показа, high ad density / заклаттеренность, attention-показатели и несоответствие формата размещения учитываются в профильных отчётах, если отсутствует самостоятельная техническая фальсификация.

5 Классификация SIVT

В настоящем стандарте выделены четыре базовые категории SIVT по объекту, на котором локализовано основное нарушение: непользовательская техническая инфраструктура, пользовательское устройство или программная среда, действия реальных пользователей, а также рекламный инвентарь или система измерений. Это верхнеуровневая классификация, которая позволяет не углубляться в большое количество частных и пересекающихся типов, используемых MRC, и привести методологии всех верификаторов к единой структуре отчётности.

5.0. Сводная таблица категорий и соответствие MRC

Название категории	Английское наименование	Основной объект нарушения	Агрегируемые категории MRC
Автоматизированный трафик с выделенного устройства	Automated Non-Human Traffic	Непользовательская техническая инфраструктура	#1 Automated browsing from a dedicated device; #7 Bots/spiders/crawlers (sophisticated); #10 Invalid proxy traffic
Вредоносное и нежелательное программное обеспечение	Malware & Adware Traffic	Пользовательское устройство или программная среда	#2 Automated browsing from a non-dedicated device; #11 Adware & Malware
Мотивированная недействительная активность	Incentivized Invalid Activity	Действия реальных пользователей	#3 Incentivized human invalid activity; #12 Incentivized manipulation of measurement
Манипуляции с инвентарём и измерениями	Inventory & Measurement Manipulation	Рекламный инвентарь или система измерений	#4 Manipulated activity; #5 Falsified measurement events; #6 Domain & App misrepresentation; #8 Hijacked ad tags & creatives

Категории MRC, не образующие самостоятельных категорий SIVT, и их трактовка приведены в разделе 6 и Приложении А.

5.1. Автоматизированный трафик с выделенного устройства
Automated Non-Human Traffic

Определение. Недействительный рекламный трафик, который после исключения GIVT формируется без участия реального пользователя с серверов, виртуальных машин, эмуляторов, headless-браузеров, специализированных ферм устройств и иной непользовательской технической инфраструктуры, которая в текущем состоянии и в момент генерации рекламных событий не используется для формирования обычного пользовательского трафика и не способна его формировать.

Объект и механизм нарушения. Источником такого трафика являются программно управляемые либо специально выделенные устройства и среды, предназначенные для автоматической генерации рекламных запросов, а также связанных с ними рекламных или других событий, имитирующих действия человека. Основное нарушение локализовано на стороне устройства и сети: реальный пользователь отсутствует как источник действия.

Типовые сценарии и примеры:

- Automated Browsing — недействительный трафик от автоматических средств имитации пользовательской активности (эмуляторы, специализированное ПО автоматизации, системы мониторинга и тестирования, если они не отфильтрованы на этапе GIVT).
- Боты и краулеры, маскирующиеся под реальных пользователей и детектируемые только сложными методами (имитация движений мыши, скроллинга, правдоподобных параметров браузера и устройства).
- Фермы устройств, домашние роутеры и иные среды без обычной пользовательской активности.
- Недействительный прокси-трафик (Invalid proxy traffic) — прокси-инфраструктура, существующая для манипуляции счётчиками или передачи недействительного трафика, рассматривается в этой категории только совместно с признаками автоматизированной генерации событий.

Сигналы детекции. Аномальное поведение и последовательности действий; аномальные распределения в срезах (geo/IP, частота, время реакции); технические характеристики устройства и окружения; признаки средств автоматизации; сетевые сигналы (IP дата-центров, цепочки прокси, ротация IP, аномальный профиль ASN) как подтверждающие.

Применимость к типам событий. Показы, клики, видео-события, переходы, сессии, установки, конверсии.

Разграничение со смежными категориями. Трафик, возникающий на реальном пользовательском устройстве вследствие работы вредоносного или нежелательного ПО, относится к категории Вредоносного и нежелательного программного обеспечения, а не Автоматизированного трафика с выделенного устройства. Если ключевым подтверждаемым сигналом является подмена идентификатора, агента или источника, событие относится к категории Манипуляций с инвентарём и измерениями. Известные автоматизированные источники, легитимные боты и краулеры по спискам, известный недействительный трафик дата-центров и простая избыточная активность по базовому порогу выявляются на этапе GIVT и в категории Автоматизированного трафика с выделенного устройства повторно не учитываются.

Соответствие MRC. #1 Automated browsing from a dedicated device; #7 Bots and spiders or other crawlers masquerading as legitimate users (sophisticated means); #10 Invalid proxy traffic.

5.2. Вредоносное и нежелательное программное обеспечение
Malware & Adware Traffic

Определение. Недействительный рекламный трафик, который после исключения GIVT возникает на реальном пользовательском устройстве, в браузере, приложении или иной программной среде, способной в тот же период формировать обычный пользовательский трафик, но рекламные события полностью либо частично инициируются, изменяются или дополняются установленным программным обеспечением без осознанного участия пользователя.

Объект и механизм нарушения. Источником активности является пользовательское устройство или программная среда, в которой одновременно может происходить легитимное взаимодействие реального пользователя, однако часть рекламных событий создаётся вследствие её компрометации. Основное нарушение локализовано в исполняемом слое (приложение / ПО).

Типовые сценарии и примеры:

- Рекламное ПО (Adware) — ПО, созданное для фейковых показов рекламы, внедрения неавторизованных рекламных кодов и оверлеев на посещаемые сайты или подмены рекламных кодов владельца сайта.
- Botnet — сеть устройств с вредоносным ПО под централизованным управлением, используемая без ведома пользователя для накрутки рекламы; в том числе мобильные ботнеты, CTV/OTT-устройства.
- Тулбары, браузерные расширения и заражённые приложения, запускающие фоновую рекламную активность, автоматическую загрузку рекламных материалов или действия от имени пользователя.
- Automated browsing from a non-dedicated device — автоматизированная активность, запускаемая ПО на реальном устройстве пользователя без его осознанного участия.

Сигналы детекции. Поведенческие аномалии; смешение фродовых и нефродовых сессий на одном устройстве; «групповая динамика» заражённых устройств; технические признаки вредоносного или нежелательного ПО; появление нелегитимных форматов на легитимных сайтах; телеметрия взаимодействия пользователя с рекламой; сетевые аномалии как дополнительные сигналы.

Применимость к типам событий. Показы, клики, видео-события, установки, конверсии.

Разграничение со смежными категориями. В отличие от категории Автоматизированного трафика с выделенного устройства, устройство реально и может использоваться человеком. Если непосредственно подтверждено, что основное нарушение состоит в подмене или несанкционированном внедрении рекламного кода, тега, креатива, домена, приложения, места размещения, источника инвентаря или измеряемого события (в том числе внедрение неавторизованных оверлеев, продажа неавторизованного инвентаря через скомпрометированную среду), такой случай относится к категории Манипуляций с инвентарём и измерениями как к наиболее прямо доказуемому объекту нарушения.

Перспектива. Внедрение криптографической подписи показов позволит детерминированно подтверждать авторизованный источник инвентаря и более чётко разделять кейсы между Вредоносным и нежелательным программным обеспечением и Манипуляциями с инвентарём и измерениями. Документ фиксирует это как целевое направление рынка, а не как действующее обязательное требование.

Соответствие MRC. #2 Automated browsing from a non-dedicated device; #11 Adware and Malware that conduct deceptive actions.

5.3. Мотивированная недействительная активность
Incentivized Invalid Activity

Определение. Недействительный рекламный трафик, который после исключения GIVT формируется на реальных пользовательских устройствах в результате осознанных действий людей, совершаемых не вследствие естественного интереса к рекламе, контенту или продукту, а ради денежного вознаграждения, бонуса, выполнения задания, получения иной выгоды либо намеренного искусственного изменения рекламных или измерительных показателей.

Объект и механизм нарушения. Нарушение локализовано в намерении человека: действие совершает реальный пользователь, но мотивация не является органическим интересом. Устройство, ПО и рекламный код при этом обычно штатные.

Типовые сценарии и примеры:

- Мотивированный трафик (Incentivized traffic) — неорганический трафик от пользователей, цель которых — получить бонус или вознаграждение за выполнение определённых действий.
- Организованные или массовые просмотры, клики, переходы, досмотры видео, установки, регистрации, конверсии, выполняемые участниками клик-ферм (click farms), бирж заданий, paid-to-click-сервисов, CPA-мотивированных каналов и приложений для заработка.
- Стимулированная манипуляция измерениями (incentivized manipulation of measurement) — мотивированное продвижение или искусственное изменение измеряемых показателей без ведома и разрешения измеряемой сущности.

Сигналы детекции. Первичная детекция — по частотным и статистическим аномалиям (синхронность действий, повторяемость сценариев, неестественное время реакции, аномальные кластеры микроконверсий, несоответствие поведения ожидаемой аудитории). Уточнение — по подтверждённым спискам приложений, сайтов, бирж и источников мотива, а также путём ручной валидации. Часть событий с выраженными признаками может быть классифицирована автоматически; отнесение конкретного домена или источника к мотиву, как правило, подтверждается ручной валидацией.

Применимость к типам событий. Клики, переходы, досмотры видео, установки, регистрации, конверсии, показы.

Разграничение со смежными категориями. Событие, уже отнесённое к GIVT по базовому порогу избыточной активности, повторно в категории Мотивированной недействительной активности не учитывается. Если рекламное событие создано, изменено или подменено технически и не соответствует фактически совершённому действию человека, оно относится к категории Манипуляций с инвентарём и измерениями. Само по себе низкое качество аудитории, высокая или низкая активность пользователей, низкая вовлечённость либо слабая результативность кампании не являются достаточным основанием для отнесения к категории Мотивированной недействительной активности. Легитимные rewarded-форматы не относятся к мотивированной недействительной активности, если характер вознаграждения заранее раскрыт, соответствует условиям размещения и не вводит рекламодателя в заблуждение.

Соответствие MRC. #3 Incentivized human invalid activity; #12 Incentivized manipulation of measurement.

5.4. Манипуляции с инвентарём и измерениями
Inventory & Measurement Manipulation

Определение. Недействительный рекламный трафик и недействительные рекламные события, которые после исключения GIVT возникают вследствие подмены, искажения или несанкционированного изменения рекламного инвентаря, цепочки поставки рекламы, рекламного кода либо данных измерения и вводят рекламодателя, рекламную платформу или верификатора в заблуждение относительно фактического источника, места, способа показа или совершённого события.

Объект и механизм нарушения. Нарушение локализовано в рекламном коде, инвентаре или системе измерения. Пользователь может быть реальным, но рекламно-измерительная среда подменяется или используется мошеннически.

Типовые сценарии и примеры:

- Подмена домена или приложения (Домен спуфинг, App ID spoofing, domain laundering), искажение сведений об источнике и продавце инвентаря, продажа неавторизованного инвентаря.
- Перехват или несанкционированное внедрение рекламных тегов и креативов (hijacked ad tags and creatives), фрод-скрипты.
- Подделка событий трекинга (Falsified Measurement) — фальсификация показов, viewability, кликов, локации, реферера, consent string, конверсий, атрибутов пользователя; SSAI spoofing; SDK Spoofing; спуфинг аналитики или CPA-трекера; атрибуционный фрод.
- Манипулированная активность (manipulated activity): forced redirects, forced clicks, clickjacking, попандеры (Popunder), кликандеры (Clickunder) и иные механизмы, вызывающие непреднамеренные действия пользователя.

MFA-сайты. В категорию Манипуляций с инвентарём и измерениями могут включаться сайты Fake Domains & MFA (Made for Advertising) и связанные сети доменов, если расширенный анализ подтверждает систематическое создание или представление такого инвентаря с целью введения рекламодателя в заблуждение относительно его фактической природы и источника. Детекция MFA обычно ведётся по поведенческим и алгоритмическим признакам, но после подтверждения факт становится таблично доказуемым (домен входит в подтверждённую сеть). Сам факт нахождения домена в предварительном списке, низкое качество контента или высокая плотность рекламы без подтверждения схемы не являются достаточным основанием для признания всего трафика домена SIVT.

Auto-refresh. Bad Autorefresh — чрезмерно частое авто-обновление страницы или рекламного блока с целью накрутки показов — относится к категории Манипуляций с инвентарём и измерениями, если обновление не является заранее раскрытым и согласованным условием размещения.

Сигналы детекции. Внешний мониторинг; сверка заявленного и фактического размещения; сопоставление наблюдаемого и декларированного инвен-

таря; невозможная или нелогичная временная последовательность рекламных событий; несоответствие между слоями данных (технические характеристики против статистических показателей); анализ IP и хостингового окружения как подтверждающего сигнала.

Применимость к типам событий. Показы, клики, видео-события, события видимости, конверсии, установки.

Разграничение со смежными категориями. Если один случай одновременно имеет признаки автоматизации, malware, adware или мотивированной активности, но при этом непосредственно и технически подтверждена подмена инвентаря, рекламного кода, домена, приложения, источника или измеряемого события, он относится к категории Манипуляций с инвентарём и измерениями как к наиболее прямо доказуемому объекту нарушения. Сама по себе невидимость показа, высокая плотность рекламы, low viewability, attention-показатели, outstream-as-instream или иное несоответствие ожидаемого формата без самостоятельного подтверждения манипуляции к категории Манипуляций с инвентарём и измерениями не относятся (см. раздел 6).

Соответствие MRC. #4 Manipulated activity; #5 Falsified measurement events; #6 Domain and App misrepresentation; #8 Hijacked ad tags and creatives.

5.5. Приоритеты и разрешение пересечений

Каждое рекламное событие относится только к одной категории SIVT. При наличии нескольких признаков выбирается категория, которая отражает основной объект нарушения и подтверждается наиболее прямыми и технически проверяемыми данными; дополнительные признаки могут сохраняться как атрибуты события, но не приводят к его повторному учёту.

Применяются следующие правила приоритета:

- **Правило доказуемости.** Прямое доказательство манипуляции с инвентарём или измеряемым событием (категория Манипуляции с инвентарём и измерениями) имеет приоритет перед косвенной поведенческой интерпретацией. Если нарушение можно подтвердить детерминированными данными, такая классификация приоритетна.

- **Правило proxy/сети.** Proxy/VPN/IP rotation не являются IVT сами по себе. Они относятся к категории Автоматизированного трафика с выделенного устройства, если используются как инфраструктура доставки автоматизированного нечеловеческого трафика, и к категории Манипуляций с инвентарём и измерениями, если используются для подмены источника, домена, приложения или измеряемого события.

- **Правило ПО.** Adware/Malware относятся к категории Вредоносного и нежелательного программного обеспечения, пока нарушение локализовано на устройстве или в ПО пользователя. Если основное нарушение связано с подменой рекламного кода, тегов, креативов, цепочки поставки или измеряемых событий, кейс классифицируется как Манипуляции с инвентарём и измерениями.

Правило человека. Если реальный человек фактически совершает рекламное действие ради вознаграждения или выгоды — категория Мотивированная недействительная активность. Если событие создано, изменено или подменено технически и не соответствует фактическому действию человека — категория Манипуляции с инвентарём и измерениями.

6 Граничные случаи и сигналы, не образующие SIVT

Раздел консолидирует пограничные сигналы, которые на практике вызывают расхождения. Перечисленные ниже признаки сами по себе не образуют отдельной категории SIVT.

Сигнал	Трактовка	Куда относится
Proxy / VPN / relay / IP rotation	Не IVT сам по себе; дополнительный сетевой сигнал	Автоматизированный трафик с выделенного устройства (как инфраструктура автоматизации) или Манипуляции с инвентарём и измерениями (как маскировка подмены); отдельной категории нет
MFA / Fake Domains	SIVT только при подтверждении схемы введения в заблуждение	Манипуляции с инвентарём и измерениями
Bad Autorefresh	SIVT, если не раскрыт и не согласован как условие размещения	Манипуляции с инвентарём и измерениями
Hidden / скрытые показы	Дополнительный фактор; не самостоятельная основа классификации SIVT	Учитывается как атрибут; при подтверждённой технической манипуляции — Манипуляции с инвентарём и измерениями
High ad density / заклаттеренность	Характеристика качества контакта, не IVT	Профильный отчёт по качеству инвентаря
Невидимость показа / low viewability	Качество контакта, измеряется после очистки IVT	Стандарт АРИР по измерению видимости
Attention-показатели	Качество контакта, не IVT	Профильные отчёты
Outstream-as-instream	Несоответствие формата; введение в заблуждение, но технически не IVT (нет ботов и автоматической подмены)	Отдельный отчёт по качеству размещения
Кукистафинг / Кукидропинг (cookie stuffing)	Манипуляция атрибуцией; для медийного IVT неактуально/ устарело	Не SIVT (или Манипуляции с инвентарём и измерениями при подтверждённой схеме)
Misappropriated / пиратский контент	Характеристика контента	Brand Safety, не IVT

Граница «качество контакта против IVT» проводится так: видимость, плотность рекламы, формат и attention отражают качество и среду рекламного контакта и учитываются в профильных отчётах. К SIVT они переходят только при самостоятельном подтверждении технической фальсификации.

7 Применимость по средам

Классификация: Автоматизированный трафик с выделенного устройства/Вредоносное и нежелательное программное обеспечение/Мотивированная недействительная активность/Манипуляции с инвентарём и измерениями применяется одинаково ко всем средам; различается набор доступных сигналов и характерных механик.

- **Web (desktop / mobile web).** Манипуляции реализуются преимущественно через код страницы и рекламные теги: ad injection, фрод-скрипты, попандеры/кликандеры, domain spoofing, hidden/stacked показы.
- **In-app (mobile).** Характерны SDK Spoofing, install hijacking, атрибуционный фрод, мотивированные приложения и биржи заданий, мобильные ботнеты, App ID spoofing.
- **Video / OLV.** Falsified measurement по видео-событиям; несоответствие in-stream / out-stream учитывается отдельно как качество размещения (раздел 6).
- **CTV / OTT.** Bundle ID spoofing, несоответствие типа инвентаря (display vs video, in-stream vs standalone), генерация SDK-событий без реального взаимодействия, прокси/маршрутизация, скрывающая источник.

Конкретный перечень поддерживаемых сред и событий раскрывается в методологии верификатора.

8 Формирование SIVT Total и отчётность

Все четыре категории: Автоматизированный трафик с выделенного устройства, Вредоносное и нежелательное программное обеспечение, Мотивированная недействительная активность и Манипуляции с инвентарём и измерениями включаются в SIVT Total и далее в IVT Total. SIVT Total рассчитывается как дедуплицированное объединение событий этих категорий; события, ранее отнесённые к GIVT, в расчёт SIVT Total не включаются.

Правила отчётности:

- **Единый учёт в Total.** Каждая из категорий: Автоматизированный трафик с выделенного устройства/Вредоносное и нежелательное программное обеспечение/Мотивированная недействительная активность /Манипуляции с инвентарём и измерениями учитывается в SIVT Total и не выводится из него отдельной «исключаемой» колонкой. В частности, malware/adware (категория Вредоносное и нежелательное программное обеспечение) включается в Total, а не отображается рядом с Total как невычитаемая величина.

- **Дедупликация.** Событие учитывается в SIVT Total один раз, по основной категории; прочие сработавшие сигналы сохраняются как атрибуты.
- **Базовые показатели.** SIVT rate рассчитывается как доля событий SIVT в учитываемом объёме; рекомендуется приводить разбивку по категориям Автоматизированный трафик с выделенного устройства/Вредоносное и нежелательное программное обеспечение/Мотивированная недействительная активность/Манипуляции с инвентарём и измерениями.
- **Раскрытие охвата.** Рекомендуется указывать долю событий, по которым у верификатора было достаточно данных для определения IVT (IVT decision rate), как меру полноты, а не как тип нарушения.
- **Порядок измерений.** После исключения GIVT и SIVT видимость определяется только для оставшихся валидных отрисованных показов в соответствии со Стандартом АРИР по измерению видимости. Невидимость показа или иной показатель качества контакта не используется для повторного отнесения события к SIVT без самостоятельного подтверждения технической манипуляции.

9 Требования к методологии верификатора

Стандарт не предписывает конкретных алгоритмов, но для сопоставимости верификатор раскрывает в своей методологии:

- Перечень поддерживаемых сред и типов событий;
- Соответствие собственных продуктовых метрик категориям Автоматизированного трафика с выделенного устройства/Вредоносного и нежелательного программного обеспечения/Мотивированной недействительной активности/Манипуляций с инвентарём и измерениями настоящего стандарта;
- Роль списков и баз (домены, бандлы, IP-диапазоны, биржи мотива, источники) и порядок их актуализации/ревалидации;
- Роль ручной валидации и её соотношение с автоматической детекцией;
- Трактовку proxy/VPN и иных сетевых сигналов как факторов, а не самостоятельной категории.

Направления рыночной кооперации (не нормативные). Участники рассматривают развитие общих рыночных справочников (начиная с валидного списка User-Agent, далее — дата-центры и сетевые признаки) и внедрение криптографической подписи показов для детерминированного подтверждения авторизованного источника инвентаря. Эти инициативы фиксируются как цель и не являются обязательными требованиями текущей редакции.

Приложение А. Соответствие SIVT категории MRC

№ MRC	Оригинальное название	Категория SIVT	Примечание
1	Automated browsing from a dedicated device	Автоматизированный трафик с выделенного устройства	Выделенные устройства, эмуляторы, фермы
7	Bots/spiders/crawlers masquerading (sophisticated)	Автоматизированный трафик с выделенного устройства	Сложная детекция; простые случаи — GIVT
10	Invalid proxy traffic	Автоматизированный трафик с выделенного устройства	Только совместно с признаками автоматизации
2	Automated browsing from a non-dedicated device	Вредоносное и нежелательное программное обеспечение	Реальное заражённое устройство
11	Adware and Malware that conduct deceptive actions	Вредоносное и нежелательное программное обеспечение	При подмене кода/инвентаря → Манипуляции с инвентарём и измерениями
3	Incentivized human invalid activity	Мотивированная недействительная активность	Click farms, биржи заданий, PTC, CPA-мотив
12	Incentivized manipulation of measurement	Мотивированная недействительная активность	Если технически подменено событие → Манипуляции с инвентарём и измерениями
4	Manipulated activity	Мотивированная недействи-тельная активность	Попандеры, кликандеры, forced clicks/redirects
5	Falsified measurement events	Манипуляции с инвентарём и измерениями	SSAI/SDK spoofing, атрибуционный фрод
6	Domain and App misrepresentation	Манипуляции с инвентарём и измерениями	Domain spoofing, MFA-сети
8	Hijacked ad tags and creatives	Манипуляции с инвентарём и измерениями	По первичному механизму; перспектива — крипто-подпись
9	Hidden/stacked/covered/ transparent/invisible ad serving	— / Манипуляции с инвентарём и измерениями	Доп. фактор; SIVT только при подтверждённой манипуляции
13	Misappropriated (pirated/stolen) content	—	Brand Safety, не IVT
14	Cookie stuffing, recycling or harvesting	— / Манипуляции с инвентарём и измерениями	Для медийного IVT неактуально; Категория Манипуляции с инвентарём и измерениями при подтверждённой схеме

Приложение В. Связанные термины глоссария

Термины, используемые в настоящем стандарте и смежные с ними, приведены по Глоссарию по фроду и рекламе АРИР:

1	Automated Browsing
2	Боты
3	Botnet
4	Рекламное ПО (Adware)
5	Тулбар (Toolbar)
6	Мотивированный трафик (Incentivized traffic)
7	Попандер (Popunder)
8	Кликандер (Clickunder)
9	Домен спуфинг (Domain Spoofing)
10	Fake Domains & MFA Domains
11	Фрод-скрипт (Fraud-script)
12	Спуфинг аналитики или CPA-трекера
13	Falsified Measurement
14	SDK Spoofing
15	Атрибуционный фрод
16	Кликфлуд / Кликспам
17	Install hijacking
18	Hidden
19	Невидимые показы
20	Bad Autorefresh
21	High ad density
22	Ghost ad call
23	Кукистафинг / Кукидропинг
24	Шейвинг