

**Методика выявления признаков использования
средств обхода блокировок на клиентских устройствах**

Оглавление

1. Назначение документа	2
2. Термины и сокращения	2
3. Общее описание методики и последовательности ее внедрения	3
4. Ложноположительные срабатывания и способы их минимизации	4
5. GeoIP	5
6. Мобильные устройства	7
7. Точность	8
8. Широта охвата	11
9. Критерии принятия решения о выявлении средств обхода	13

1. Назначение документа

Настоящая методика предлагают унифицированный подход к выявлению на пользовательских устройствах VPN и Proxu, используемых для обхода блокировок запрещенных ресурсов РКН.

Методика описывает основные этапы выявления VPN и Proxu и используемые методы выявления, а также определяет очередность внедрения методики.

Помимо самих методов рассматриваются существующие ограничения и сложности при их применении, связанные с ложноположительными срабатываниями.

2. Термины и сокращения

Термин	Определение
VPN	Технология создания зашифрованного туннеля, при которой часть или весь трафик устройства направляется через удалённый сервер.
Proxu	Посредник на уровне приложений (HTTP-proxu, SOCKS-proxu и др.), через который проходят сетевые запросы.
GeoIP	Определение географического местоположения (страна, регион, город) по IP-адресу с помощью специализированных баз данных или внешних API.
ASN	Autonomous System Number (Номер автономной системы) - идентификатор сети в глобальной маршрутизации (BGP). Позволяет определить владельца IP-адреса и тип сети.
Split tunneling	Режим работы VPN, при котором через туннель направляется трафик только выбранных приложений, а остальной трафик идёт напрямую.
ПО	Программное обеспечение

3. Общее описание методики и последовательности ее внедрения

Существуют три основных области, анализ которых позволяет производить детектирование использования VPN на клиентском устройстве:

- Анализ клиентских сессий на сервере (GeoIP);
- Анализ сетевых подключений и интерфейсов на клиентском устройстве;
- Анализ системных настроек и таблиц маршрутизации на клиентском устройстве.

Использование одного или нескольких методов выявления использования средств обхода блокировок не дает 100% гарантии точности результата из-за возможных ложноположительных срабатываний. Причины возникновения таких ситуаций рассматриваются в разделе 4.

Анализ клиентских сессий на сервере состоит в сравнении IP-адреса подключения с репутационной БД. К преимуществам метода относятся:

- Универсальность. Возможность применять анализ независимо от операционной системы (ОС) клиентского устройства;
- Прозрачность для клиента. Проверка производится на стороне сервера и не требует изменения клиентского приложения.
- Скорость. Быстрое внедрение в сравнении с другими методами.
- Простота. Относительная простота проверок.

Принимая во внимание перечисленные преимущества, внедрение анализа клиентских сессий на сервере следует производить в качестве первого этапа по внедрению методов выявления VPN на клиентских устройствах.

Более детальное описание анализа клиентских сессий на сервере приведено в разделе 5.

Для повышения точности выявления следует в качестве второго этапа внедрять проверки на клиентских устройствах. Поскольку больше половины клиентских устройств составляют мобильные устройства под управлением ОС Android и iOS, а 80% приложений, с помощью которых можно проводить выявление средств обхода, установлено именно на этих устройствах, то внедрение анализа сетевых подключений и интерфейсов и анализа системных настроек и таблиц маршрутизации на клиентском устройстве следует внедрять именно в этом сегменте. Внедрение проверок на устройства под управлением других ОС следует отнести к последующим более поздним этапам.

Внедрение проверок на клиентских устройствах следует разбить на два подэтапа. На первом подэтапе следует внедрять прямые проверки, указывающие на использование VPN и Proxu. Второй подэтап нацелен на повышение точности выявления VPN и Proxu и снижения уровня ложных срабатываний за счет внедрения косвенных признаков использования VPN и Proxu. Детальные описания методов анализа на клиентских устройствах рассматриваются в разделах 6 и 7.

Завершающий этап нацелен на достижение максимальной широты охвата клиентских устройств. Детальное описание методов анализа и существующих проблем для данного этапа рассматривается в разделе 8.

Таблица 1. Этапность внедрения методики выявления средств обхода блокировок на клиентских устройствах

Этап	Название	Описание
1	GeoIP	Выявление использования VPN на стороне сервера за счёт сравнения IP с репутационными БД
2а	Мобильные устройства	Анализ прямых признаков использования VPN на Android и iOS
2б	Точность	Анализ косвенных признаков использования VPN на Android и iOS
3	Широта охвата	Анализ на остальных клиентских устройствах

4. Ложноположительные срабатывания и способы их минимизации

В процессе применения алгоритма возможны ситуации, когда признаки, интерпретируемые как использование VPN/Проxy, возникают в легитимных сценариях использования устройства.

Основные источники ложноположительных срабатываний:

- Корпоративный VPN. Устройства, подключенные к корпоративной сети через служебный VPN для доступа к внутренним ресурсам.
- Антивирусное ПО и средства защиты. Некоторые антивирусы и межсетевые экраны создают виртуальные интерфейсы или изменяют маршрутизацию для фильтрации трафика.
- Docker, WSL2, Hyper-V, VirtualBox, QEMU/KVM, Android Emulator и другие среды виртуализации и контейнеризации, создающие виртуальные адаптеры, маршруты и частные подсети.
- NAT может приводить к тому, что GeoIP-базы могут определять точку выхода в регионе отличном от местонахождения устройства вследствие особенностей организации связи.

Список мер для минимизации ложноположительных срабатываний приведен ниже:

- Формирование белых списков. Создание и ведение базы известных корпоративных VPN и легитимных прокси-серверов.
- Анализ динамики подключений. Учет исторических данных. Если устройство использует корпоративный VPN в рабочее время и отключает его вне рабочего, такой сценарий может быть идентифицирован и исключен.
- Верификация по портам и протоколам. Дополнительный анализ используемых портов и протоколов туннелирования. Корпоративные VPN часто используют стандартные порты (например, 443 для SSL VPN), в то время как сервисы обхода ограничений могут применять специальные или динамические порты.
- Повторная проверка с задержкой. При невозможности вынесение однозначного решения рекомендуется выполнить повторный анализ через некоторое время для исключения временных аномалий сетевого подключения.
- Комбинирование с другими источниками данных. Использование дополнительных факторов: данные GPS устройства, информация о сотовой вышке, история предыдущих успешных аутентификаций.

5. Этап1: GeoIP

5.1.Цели этапа

Целью проверки является определение геолокации устройства, полученного путем сравнения IP адреса точки входа трафика с данными из специализированных референсных баз данных (GeoIP).

5.2.Область применения

Анализ клиентских сессий проводится на серверной стороне.

Анализ покрывает все устройства, а также подключения клиентов через web.

5.3. Источники данных GeoIP

В качестве референсной БД должна выступать система «Реестр адресно-номерных ресурсов сети Интернет» (РАНР).

До момента ее ввода в эксплуатацию допускается использование альтернативных БД. Наиболее широко распространённые из них MaxMind и IP2Location.

Для повышения точности анализа допускается подключение дополнительных коммерческих или внутренних источников данных.

5.4. Сценарии выявления средств обхода блокировок

Признаки, используемые при анализе GeoIP:

- определение страны и региона по IP-адресу,
- выявление аномалий: частая смена стран, резкие изменения локаций между сессиями;
- определение ASN и организации-владельца IP. Сравнение с диапазонами, выделенными дата-центрам и хостинг-провайдерам;
- проверка в репутационных списках: VPN/Proху-адреса, TOR exit nodes, публичные Proху;
- проверка диапазонов в «белых списках» корпоративных сетей и CDN для снижения ложных срабатываний.

Алгоритм применения методики.

1. Определить внешний IP клиентской сессии на стороне сервера.
2. Определить GeoIP по этому IP-адресу.
3. Определить ASN, тип сети и наличие признака hosting.
4. Проверить адрес по репутационным спискам VPN, proху и TOR.
5. Сопоставить полученные данные с историей прошлых сессий, типичными странами, регионами и доверенными диапазонами.
6. При наличии результатов анализа на клиентской стороне сравнить результаты с GeoIP.
7. Принять решение об использовании средств обхода блокировок на основании результатов шагов 1–6:
 - По результатам серверной и клиентской проверки устройство находится в РФ, нет признаков hosting и репутационного риска. Решение: VPN не выявлен.
 - Серверная проверка – устройство зарубежом; клиентская проверка – устройство в РФ. Решение: Выявлен VPN.
 - По результатам серверной и клиентской проверки устройство находится зарубежом. Решение: Требуется дополнительная проверка.
 - По результатам серверной проверки IP имеет признак hosting или входит в списки подсетей спискам VPN, proху и TOR. Решение: Выявлен VPN независимо от совпадения страны.

5.5. Альтернативные источники определения местоположения устройства

Альтернативным источником данных о местоположении устройства является определение местоположения по идентификаторам базовых станций мобильной сети,

PLMN, либо по Wi-Fi точкам доступа, BSSID, с последующим обращением к GeoIP. Вычисление координат производится методом аппроксимации по известным координатам объектов инфраструктуры.

При наличии согласия пользователя на использование приложением данных о геолокации, эти данные также могут быть использованы в анализе. Использование координат не может заменить проверку GeoIP, а лишь дополняет ее.

Использование координат повышает точность анализа для снижения уровня ложноположительных срабатываний.

Координаты не доказывают отсутствие использования VPN.

5.6. Ограничения GeoIP

- GeoIP имеет ограниченную точность для мобильных сетей, CGNAT, корпоративных сетей и пограничных регионов.
- Корпоративные легальные VPN часто в качестве точки терминирования имеют дата-центр и по GeoIP могут определяться как средствами обхода блокировок.
- CDN и глобальные сервисы могут исказить местоположение устройства без использования VPN.
- Пользовательские Proxu могут иметь IP обычного домашнего провайдера и не выявляться по ASN и hosting.
- Новые VPN-серверы появляются быстрее, чем обновляются репутационные базы.
- Изменение геолокации при роуминге. При нахождении пользователя в роуминге точка выхода в интернет может находиться в стране пребывания, что создаст несоответствие GeoIP.

6. Этап 2а: Мобильные устройства

6.1. Цели этапа

Целью проверки является анализ прямых признаков использования средств обхода блокировок на мобильных устройствах под управлением Android и iOS.

6.2. Область применения

Анализ клиентских сессий проводится на клиентском устройстве.

Анализ производится на мобильных устройствах Android и iOS.

6.3. Общие принципы анализа прямых признаков на клиентских устройствах

Прямыми признаками использования средств обхода блокировок являются системные признаки VPN и Proxu в Android и iOS. Сбор признаков осуществляется приложением на клиентском устройстве через системные API в рамках стандартных пользовательских привилегий.

Проверка должна выполняться в момент запуска приложения или аутентификации или при выполнении ключевого действия в приложении (подтверждение покупки/перевода,

указание конечной точки маршрута и т.п.). Что является ключевым действием в приложении определяет его разработчик.

Проведение непрерывного контроля или отправка пустых результатов анализа запрещена, поскольку это негативно будет влиять на расход трафика и потребление заряда батареи клиентского устройства.

Проведение анализа на клиентских устройствах не зависит от анализа на серверной стороне и является самостоятельной проверкой, тем не менее основная задача анализа состоит в подтверждении и/или уточнении данных, полученных в ходе GeoIP анализа.

6.4.Android

Для Android используются системные API `ConnectivityManager` и `NetworkCapabilities`. Предлагаемые подходы не требуют root-доступа и должны работать со стандартными привилегиями приложения.

Прямыми признаками использования VPN являются:

- флаг `IS_VPN` в `Score(Policies)`;
- наличие транспорта VPN в `Transports`;
- наличие `VpnTransportInfo`;
- наличие свойства `TRANSPORT_VPN` у `activeNetwork` при проверке `hasTransport`.

Примеры диагностических значений:

```
Score(Policies: ):
EVER_EVALUATED&IS_UNMETERED&IS_VPN&EVER_VALIDATED&IS_VALIDATED
Transports: WIFI|VPN
VpnTransportInfo{type=1, sessionId=PCAPdroid VPN, bypassable=false
longLivedTcpConnectionsExpensive=false}
```

Для выявления Proxu следует проводить анализ `System.getProperty` и иных доступных системных настроек. При выявлении в системных настройках данных об IP и порте Proxu вероятно весь трафик направляется через него.

Список характерных Proxu-портов для разных технологий:

- SOCKS: 1080, 9000, 5555, 16000-16100;
- http: 80, 443, 3128, 3127, 8000, 8080, 8081, 8888;
- прозрачные Proxu: 80, 443, 4080, 7000/7044, 8082, 12345;
- Tor: 9050, 9051, 9150.

6.5.iOS

На iOS доступ к системным данным существенно ограничен. Поэтому использование прямых признаков на iOS сильно затруднено. Анализ прямых признаков возможен только в том случае, если само приложение создает конфигурации, которые могут быть расценены, как средства обхода блокировок.

Для выявления использования системного Proxu следует использовать системный API `CFNetworkCopySystemProxySettings()` для получения настроек текущего подключения.

Наличие IP и порта указывает на наличие Proxu и направление всего трафика устройства через него.

6.6. Ограничения Мобильных устройств

- Резидентские прокси и сценарии, где внешний IP выглядит как обычный адрес провайдера.
- Системы приватности и фильтрации, если они не маркируются как VPN средствами ОС.

7. Этап 2б: Точность

7.1. Цели этапа

Целью проверки является анализ косвенных признаков использования средств обхода блокировок на мобильных устройствах под управление Android и iOS.

7.2. Область применения

Анализ клиентских сессий проводится на клиентском устройстве.

Анализ производится на мобильных устройствах Android и iOS.

7.3. Общие принципы анализа косвенных признаков на клиентских устройствах

Косвенными признаками использования средств использования блокировок являются имена интерфейсов, значения MTU, аномалии таблиц маршрутизации и измененные DNS. Косвенные признаки могут возникать и при использовании устройства без средств обхода блокировок. В связи с этим использование только косвенных признаков при принятии решения не является допустимым. Использование косвенных признаков используется только для повышения точности результата выявления VPN и Proxu.

Сбор косвенных признаков проводится в рамках единого процесса сбора данных о клиентском устройстве.

7.4. Android

В качестве косвенного признака можно проверять флаг NOT_VPN в Capabilities. Для обычных сетей этот флаг присутствует, при активном VPN отсутствует.

без VPN: Transports: WIFI Capabilities:
NOT_METERED&INTERNET&NOT_RESTRICTED&TRUSTED&NOT_VPN&VALIDATED&NOT_ROAMING&FOREGROUND&NOT_CONGESTED&NOT_SUSPENDED&NOT_VCN_MANAGED

с VPN: Transports: WIFI|VPN Capabilities:
NOT_METERED&INTERNET&NOT_RESTRICTED&TRUSTED&VALIDATED&NOT_ROAMING&FOREGROUND&NOT_CONGESTED&NOT_SUSPENDED&NOT_VCN_MANAGED

Имена интерфейсов tun0, tun1, tap0, wg0, ppp0, ipsec могут указывать на активное VPN-соединение и являются косвенными признаками, поскольку интерфейсы с аналогичными именами могут создавать антивирусы, фильтры контента, корпоративные защитные средства, системные компоненты и другие сервисы.

Еще одним инструментом для сбора косвенных признаков для ОС Android 12+ могут использоваться сервисные данные вида `dumpsys vpn_management` и `dumpsys activity service` предоставляющие список активных VPN с указанием пакета.

```
VPNs:
  0: io.github.romanvht.byedpi
    Active package name: io.github.romanvht.byedpi
    Active vpn type: 1

ServiceRecord{... io.github.romanvht.byedpi/.services.ByeDpiVpnService}
intent={act=android.net.VpnService ...}
```

7.5.iOS

В iOS существуют следующие способы выявления косвенных признаков использования средств обхода блокировок:

- Анализ системных проху-настроек через `CFNetworkCopySystemProxySettings()`.
- Анализ ключа `__SCOPED__` и перечня активных интерфейсов.
- Использование `NWPathMonitor` для отслеживания изменений состояния сети.
- Использование `NEVPNManager` в тех сценариях, где приложение вправе им пользоваться и имеет соответствующие права.

Функция `CFNetworkCopySystemProxySettings()` возвращает словарь с текущими настройками. Внутри ключа `__SCOPED__` содержатся имена активных интерфейсов. Наличие интерфейсов с именами `utun`, `tap`, `tun`, `ppp`, `ipsec` может указывать на работающий VPN.

Косвенным признаком может выступать наличие параметра `P2P`, выставленного в параметрах интерфейса. `NWPathMonitor` позволяет отслеживать изменения состояния сети в реальном времени. В обработчике `pathUpdateHandler` можно анализировать список `path.availableInterfaces` на наличие интерфейсов с типом `.other` и именем, содержащим `utun`.

Выделим `NEVPNManager` как отдельный расширенный инструмент для выявления косвенных признаков. Он предоставляет детальную информацию только по тем VPN, которые были сконфигурированы через само приложение, либо доступны приложению по модели `NetworkExtension`. Для его использования требуются специальные права, `entitlements`. Таким образом `NEVPNManager` ограниченно полезен, но не может решить задачу выявления VPN в общем виде.

Отдельно стоит выделить встроенный сервис `iCloud Private Relay`. Этот сервис не должен автоматически классифицироваться как запрещенный VPN, хотя его использование и позволяет обходить блокировки. Работа с этим сервисом требует отдельной логики обработки для снижения рисков ложных срабатываний.

7.6.Маршрутизация

Ниже приведены аномалии в таблицах маршрутизации устройств, косвенно указывающие на использование VPN:

- Маршрут по умолчанию, указывающий на интерфейс, отличный от основного физического или беспроводного.

- Наличие выделенных маршрутов, направляющих трафик на нестандартные шлюзы.
- Отсутствие прямого маршрута до шлюза интернет-провайдера при активном соединении.
- Использование нестандартных значений MTU.
- Наличие маршрутов, указывающих на использование split tunneling, когда часть трафика идет через туннель, а часть напрямую.

Приведенные признаки могут дополнять проверки на серверной стороне или при анализе прямых признаков на клиентском устройстве. Выявление только этих признаков не является основанием для вынесения решения выявлен VPN.

Причины, ограничивающие применение анализа маршрутизации при выявлении VPN:

- Частные диапазоны 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16 встречаются повсеместно в офисных, домашних и контейнерных средах.
- Метрики маршрутов меняются автоматически в зависимости от среды и не являются уникальным признаком VPN.
- Множественные интерфейсы и виртуальные маршруты создаются WSL2, Hyper-V, VirtualBox, антивирусами, средствами родительского контроля и иными легитимными компонентами.

Ниже приведены аномалии в таблицах маршрутизации устройств, косвенно указывающие на использование Proxu:

- Маршрут по умолчанию настроен на передачу трафика в виртуальный сетевой интерфейс;
- Наличие в таблице маршрутизации выделенных маршрутов.
- Большое количество установленных соединений на локальный порт;
- Использование клиентами случайных портов;
- Отсутствие прямых внешних соединений.

Анализ таблиц маршрутизации не применим для iOS, поскольку доступ приложений к информации о других приложениях и системных настройках ограничен.

7.7.DNS

Анализ настроек DNS также относится к косвенным признакам. Явное изменение DNS-сервера на публичный адрес либо DNS внутри VPN-сети может быть уточняющим признаком, но сам по себе недостаточен.

Причины, ограничивающие применение анализа настройки DNS при выявлении VPN:

- DNS может быть изменен и без VPN, например приложениями фильтрации или блокировки рекламы.
- Пользователь может вручную задать DNS, например публичный или корпоративный.
- Некоторые VPN не меняют DNS и оставляют DNS родительской сети.

- Локальные DNS-адреса и направление DNS в виртуальный интерфейс полезны только в комбинации с иными признаками.

Ниже приведены аномалии в настройке DNS, косвенно указывающие на использование Proxu:

- DNS-серверам назначаются локальные адреса;
- Все DNS-запросы направляются в виртуальный сетевой интерфейс.

7.8.Дополнительные технические методы выявления Proxu

- Проверка специализированных утилит, например proxuchains или tsocks.
- Выявление системных процессов проху-серверов по именам процессов и характерным портам.
- Анализ правил межсетевого экрана, iptables или pf, на наличие перенаправлений на локальный проху.
- Мониторинг активных соединений к нестандартным или удаленным портам.
- Проверка локальных сертификатов и признаков Man in the Middle проху.

7.9.Ограничения Точности

- В режиме split tunneling часть приложений может работать напрямую, поэтому проверка по одной активной сети недостаточна.
- Proxu-in-app, кастомные туннели и пользовательские реализации обхода, не отражающиеся в системных API.

8. Этап 3: Широта охвата

8.1.Цели этапа

Целью проверки является анализ прямых и косвенных признаков использования средств обхода блокировок на любых клиентских устройствах.

8.2.Область применения

Анализ клиентских сессий проводится на клиентском устройстве.

Анализ производится на устройствах с операционными системами отличными от Android и iOS.

8.3.Проблематика Ширины охвата

Расширение методики выявления средств обхода блокировок на клиентские устройства под управлением систем Windows, семейства UNIX, MacOS связано с определенными сложностями. С одной стороны, использованием приложений на этих устройствах незначительно в сравнении с мобильными устройствами. С другой стороны, на таких устройствах применяются технологии, не характерные для мобильных устройств, но которые могут приводить к ложным срабатываниям.

Принимая во внимание описанные выше аргументы решение о расширении ширины охвата устройств должно применяться после внедрения и накопления определенной статистических данных об эффективности выявления средств обхода.

Выработка методов выявления для этих устройств должна также после завершения первых этапов.

8.4. MacOS

Особенности выявления использования средств обхода в MacOS:

- Анализ интерфейсов через `getifaddrs()` позволяет перечислить сетевые интерфейсы, включая виртуальные.
- Анализ таблицы маршрутизации позволяет выявлять нестандартную маршрутизацию трафика.
- `Transparent Proxy API` является отдельным типом сетевого контура, который может быть полезен для выявления.
- Системные расширения `Network Extensions` требуют явного разрешения пользователя.
- Принудительная маршрутизация `enforceRoutes` может рассматриваться как дополнительный технический признак.

8.5. UNIX и Linux

Особенности выявления использования средств обхода в UNIX/Linux:

- Характерные имена интерфейсов: `tun`, `tap`, `wg`, `utun`, `ppp`.
- Используются только активные интерфейсы со статусом UP и назначенным IP-адресом.
- Для туннельных интерфейсов VPN MTU часто меньше стандартных значений, например 1350 или 1400.
- Наличие нескольких маршрутов по умолчанию, маршрутов через виртуальные интерфейсы, нетипичных подсетей и измененных DNS может использоваться как дополнительная аналитика.
- Анализ `/etc/resolv.conf` и иных конфигураций DNS полезен только как поддерживающий фактор.
- Сравнение локальных и публичных IP-адресов, а также принадлежность адреса ЦОД, также относятся к дополнительным признакам.

8.6. Windows

Особенности выявления использования средств обхода в Windows:

- Для выявления активных удаленных подключений может использоваться `RasEnumConnection`.
- Для анализа сетевых адаптеров допускается использовать `GetAdaptersAddresses` или `GetAdaptersInfo`.
- Признаками могут выступать виртуальный тип адаптера, `IfType = IF_TYPE_PROP_VIRTUAL`, характерные названия VPN, TAP, Wintun, WireGuard, OpenVPN и состояние UP.
- В качестве расширенного метода можно анализировать реестр на предмет выявления VPN и проху-настроек.
- Проверка шлюза по умолчанию, DNS, расхождения публичного и локального IP, а также метрик интерфейсов относится к дополнительным факторам точности.

Для всех desktop и UNIX-платформ сохраняется общее правило: интерфейсы, маршруты, MTU, частные подсети и DNS сами по себе не являются достаточным основанием для жесткого решения без серверного риска или иных сильных подтверждений.

8.7. Ограничения Ширины охвата

- Методика не рассматривает ситуации, когда VPN разворачивается на пользовательском маршрутизаторе. В этом случае на клиентском устройстве отсутствуют локальные артефакты и выявление средств обхода блокировок затруднено.
- Методика не рассматривает ситуации, когда VPN или Proxu разворачивается внутри виртуальной машины или контейнера, работающего на клиентском устройстве.

9. Критерии принятия решения о выявлении средств обхода

Для выявления использования средств обхода на клиентских устройствах используется комплексный подход при принятии решения, поскольку ни одна отдельная проверка не дает 100% точности.

Таблица 2 Матрица принятие решений

GeoIP	Прямые признаки	Косвенные признаки	Решение
НЕ выявлен	НЕ выявлен	НЕ выявлен	Обход не выявлен
НЕ выявлен	Выявлен	НЕ выявлен	Обход не выявлен
НЕ выявлен	НЕ выявлен	Выявлен	Обход не выявлен
Выявлен	НЕ выявлен	НЕ выявлен	Требуется доп. проверка
НЕ выявлен	Выявлен	Выявлен	Требуется доп. проверка
Выявлен	Выявлен	НЕ выявлен	Обход выявлен
Выявлен	НЕ выявлен	Выявлен	Обход выявлен
Выявлен	Выявлен	Выявлен	Обход выявлен

- Обход выявлен: все проверки не выявили использование VPN и Proxu, либо признаки использования выявлены только на одной из первых двух проверках.
- Требуется дополнительная проверка: признаки использования VPN выявлены на двух проверках, но между ними имеются противоречия. Требуется повторная проверка с расширенным набором критериев, либо проверка в ручном режиме.
- Обход выявлен: признаки выявлены на первой и второй проверке и при этом на третьей проверке установлено, что IP-адрес источника принадлежит инфраструктуре VPN/Proxu или его геолокация достоверно не соответствует ожидаемой

10. Дополнительные методы выявления средств обхода

10.1. Метод анализа задержек

Альтернативным способом проверки, не требующем использования внешних сервисов является метод анализа задержек SNITCH (Server-side Non-intrusive Identification of Tunneled CHaracteristics). Метод основан на измерении времени отклика (RTT — Round-Trip Time) между сервером и клиентом. При прохождении трафика через VPN, он идет в обход маршрутом через на VPN-сервер, что неизбежно вносит дополнительную задержку. Подход SNITCH комбинирует данные геолокации IP-адреса с точными измерениями сетевых задержек до "контрольных точек" (landmarks). Аномально высокая задержка для геолокации IP-адреса, указывает на использование VPN.

10.2. Анализ HTTP-заголовков

Наличие заголовков X-Forwarded-For, Forwarded или Via может указывать на прохождение через промежуточный проху-узел. Этот признак должен использоваться с осторожностью, поскольку сам сервис или CDN также может легитимно формировать часть таких заголовков.