СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования

С развитием информационных технологий и увеличением количества интернет-ресурсов государства всё чаще прибегают к региональным блокировкам контента. Однако пользователи находят эффективные способы обхода таких ограничений. Это порождает необходимость в изучении и разработке методов, которые могут ограничить или предотвратить подобные обходы.

Степень разработанности

Тематика активно обсуждается как в технических, так и в правовых кругах. Существуют исследования по DPI, анализу VPN-трафика, но проблема остается актуальной и недостаточно решённой в условиях постоянного технологического развития.

Цели и задачи

Цель: исследовать современные методы обхода региональных блокировок и разработать рекомендации по их эффективному предотвращению.
Задачи:

- систематизировать методы обхода;
- проанализировать слабые места текущих фильтраций;
- рассмотреть современные подходы к блокировке;
- предложить меры по усилению контроля с учетом правовых ограничений.

Научная новизна

Предлагается анализ поведения сетевого трафика и комбинированные подходы, которые ещё не применяются массово в российских реалиях.

Теоретическая и практическая значимость

Результаты исследования могут быть полезны провайдерам, правительственным структурам и компаниям, обеспечивающим кибербезопасность.

Методы исследования

- аналитический метод;
- компаративный анализ;
- моделирование и тестирование сетевого трафика;
- экспертная оценка существующих решений.

Основные положения

1. Современные способы обхода блокировок легко масштабируются и анонимны.
2. DPI и поведенческий анализ наиболее перспективны для их обнаружения.
3. Борьба должна учитывать баланс между безопасностью и цифровыми правами.

1. VPN-СЕРВИСЫ

Виртуальная частная сеть (VPN, Virtual Private Network) представляет собой технологию, обеспечивающую защищённое соединение между пользователем и удалённым сервером через открытую сеть — в первую очередь, через Интернет. Основное назначение VPN — создание зашифрованного канала передачи данных, позволяющего не только скрыть исходный IP-адрес пользователя, но и эффективно обходить географические ограничения и цензуру, действующую в той или иной стране.

Когда пользователь подключается к VPN, между его устройством и сервером создаётся защищённый туннель. Этот туннель формируется с использованием специальных протоколов, обеспечивающих как шифрование, так и стабильность соединения. Наиболее распространёнными протоколами являются OpenVPN, IKEv2/IPSec и WireGuard, а также более устаревшие варианты, такие как L2TP/IPSec и PPTP. Несмотря на то что некоторые из них уже не рекомендуются к использованию из-за уязвимостей, они всё ещё встречаются в некоторых сервисах.

После установки туннеля весь исходящий трафик пользователя шифруется и проходит через VPN-сервер, прежде чем попасть в Интернет. Это шифрование делает невозможным перехват и анализ данных со стороны провайдера или органов контроля. Более того, на внешних ресурсах пользователь будет идентифицирован по IP-адресу VPN-сервера, а не по своему реальному адресу. Это значит, что сайт, находящийся, например, под блокировкой в России, будет «видеть» пользователя как находящегося в Германии или США, в зависимости от выбранного сервера.

Для повышения устойчивости к блокировке самих VPN-соединений некоторые сервисы используют технологии маскировки — специальные методы сокрытия самого факта использования VPN. Такие подходы особенно важны в странах с агрессивной интернет-цензурой, где VPN-трафик отслеживается и блокируется. Среди популярных методов можно выделить Obfsproxy, XOR obfuscation, Stunnel (использующий SSL-туннелирование), а также Pluggable Transports, широко применяемые в сети Tor.

Популярность VPN в качестве инструмента обхода блокировок объясняется рядом причин. Во-первых, это высокая доступность — существует большое количество как платных, так и бесплатных решений с интуитивно понятными приложениями для всех популярных платформ. Во-вторых, VPN крайне прост в использовании: зачастую достаточно установить

приложение и нажать одну кнопку. В-третьих, VPN обеспечивает высокий уровень анонимности, особенно при использовании маскирующих технологий. И наконец, благодаря шифрованию заголовков и полезной нагрузки, VPN-соединения эффективно обходят системы DPI (глубокой инспекции пакетов) и фильтрацию на основе SNI (Server Name Indication).

Тем не менее, у технологии есть и свои ограничения. Из-за шифрования и дополнительной маршрутизации скорость соединения может заметно снижаться, особенно при подключении к удалённым серверам. Современные DPI-системы способны распознавать VPN-трафик по его специфическим признакам — например, по структуре TLS-соединения, характерным паттернам во время рукопожатия или типичным портам. В некоторых странах, таких как Китай, Иран или Россия, использование VPN регулируется или прямо запрещено на законодательном уровне. Кроме того, при неправильной настройке возможны утечки DNS или IP, которые сводят на нет весь эффект анонимности.

На практике использование VPN для обхода блокировок можно проиллюстрировать следующим примером. Пользователь, находящийся в России, хочет получить доступ к новостному сайту, который заблокирован как по IP-адресу, так и на уровне DNS. Он запускает VPN-клиент и подключается к серверу, расположенному в Германии. После этого весь его трафик направляется через Германию, и для сайта пользователь выглядит как посетитель из Европы. В результате ни DNS-блокировка, ни IP-фильтрация, установленные в РФ, не препятствуют доступу к ресурсу.

2. ПРОСКИ-СЕРВИСЫ

Прокси-сервер (от англ. *proxy* — «посредник») представляет собой сервер, который служит промежуточным звеном между клиентом и целевым интернет-ресурсом. Когда пользователь использует прокси, он не отправляет запросы напрямую на веб-сайт. Вместо этого запросы направляются на прокси-сервер, который от своего имени пересылает их на целевой ресурс. Для внешнего мира все выглядит так, будто запросы поступают от прокси-сервера, а не от самого пользователя. Это помогает скрыть реальный IP-адрес и местоположение пользователя.

Существует несколько типов прокси-серверов, каждый из которых обладает своими особенностями и областями применения. Среди них выделяются:

1. HTTP-прокси. Эти прокси-серверы работают только с HTTP-запросами, что ограничивает их применение исключительно для веб-сайтов. Они не поддерживают шифрование, что делает их уязвимыми для перехвата и анализа трафика. Такой прокси легко обнаруживается системами глубокой инспекции пакетов (DPI), и, несмотря на свою простоту, они предоставляют низкий уровень безопасности.
2. HTTPS-прокси (SSL-прокси). В отличие от HTTP-прокси, эти серверы поддерживают шифрование, что делает их более безопасными. HTTPS-прокси часто используются для обхода блокировок, так как шифрованный трафик сложнее анализировать и перехватывать. Эти прокси идеально подходят для работы с веб-браузерами, которые поддерживают расширения для прокси.
3. SOCKS-прокси (например, SOCKS5). SOCKS-прокси действуют на более низком уровне (транспортном) и могут передавать практически любой тип трафика — не только HTTP(S), но и почту, FTP и другие протоколы. SOCKS5 является самым популярным вариантом, так как он поддерживает аутентификацию и используется в таких приложениях, как Tor-клиенты, для анонимного серфинга.
4. Ротационные (или анонимные) прокси. Эти прокси-серверы постоянно меняют свой IP-адрес, что позволяет избежать блокировок, которые основаны на анализе количества запросов с одного IP. Они часто используются для повышения анонимности и предотвращения блокировки, так как с каждым новым запросом пользователь будет использовать новый адрес.

Принцип работы прокси-сервера довольно прост: пользователь настраивает соединение с прокси-сервером, будь то вручную или через специальное ПО. Все его запросы сначала направляются на этот сервер, который выполняет запросы от своего имени и передаёт результаты обратно пользователю. При этом реальный IP-адрес и местоположение пользователя остаются скрытыми, поскольку целевой ресурс видит только IP-адрес прокси-сервера.

Прокси-сервера имеют несколько значительных преимуществ при обходе блокировок. Во-первых, они просты в реализации: достаточно изменить настройки браузера или установить специальное расширение, чтобы начать использовать прокси. Во-вторых, прокси-серверы заменяют реальный IP-адрес пользователя на свой собственный, что помогает обойти блокировки, основанные на фильтрации IP. Также можно использовать разные прокси для

разных сайтов или сервисов, что даёт возможность обходить блокировки на уровне конкретных ресурсов.

Однако у прокси-серверов есть и недостатки. Во-первых, некоторые из них, такие как HTTP-прокси, не поддерживают шифрование, что делает трафик уязвимым для перехвата и анализа. Во-вторых, прокси часто передают заголовки с информацией о реальном IP-адресе пользователя, что снижает уровень анонимности. Кроме того, простые прокси-серверы, такие как HTTP-прокси, легко распознаются и блокируются системами DPI. Наконец, бесплатные прокси-серверы часто перегружены или нестабильны, что снижает их надёжность и скорость.

Применение прокси-серверов для обхода блокировок также достаточно просто. Например, пользователь может настроить свой браузер на работу с прокси-сервером из другой страны, и все запросы, включая те, которые направляются к заблокированным ресурсам, будут проходить через этот сервер. Это позволяет обойти блокировки, основанные на фильтрации по IP или региональным ограничениям.

Пример: Если в России заблокирован сайт по IP или DNS, пользователь может подключиться через SOCKS5-прокси, расположенный, например, в Нидерландах. В таком случае трафик будет направляться через этот прокси-сервер, и для целевого сайта пользователь будет выглядеть как человек из Европы, что помогает обойти блокировки, установленные на уровне национальных фильтров.

3. TOR-СЕТЬ

Tor (The Onion Router) — это распределённая анонимизирующая сеть, предназначенная для обеспечения конфиденциальности пользователей в Интернете. Она работает путём направления трафика через серию узлов, которые управляются добровольцами, а также использует многослойное шифрование, аналогичное структуре луковицы, благодаря чему скрывается как источник данных, так и маршрут их передачи.

Принцип работы сети Tor заключается в маршрутизации данных через три узла, каждый из которых выполняет свою роль, обеспечивая анонимность на разных этапах:

1. Входной узел (Entry node) — этот узел знает лишь IP-адрес пользователя, но не может определить, к какому ресурсу направляется трафик.

2. Промежуточный узел (Relay node) — он служит для перемешивания трафика, делая его сложнее для анализа.
3. Выходной узел (Exit node) — последний узел в цепочке, который делает запрос от имени пользователя, не зная его настоящего IP.

При этом каждый узел в сети Tor шифрует трафик, распаковывая только один слой шифрования, что добавляет дополнительный уровень безопасности. Поскольку данные проходят через несколько случайно выбранных узлов, маршруты постоянно меняются, что ещё больше увеличивает анонимность пользователей.

Tor является мощным инструментом для обхода блокировок и цензуры. Он предлагает несколько значительных преимуществ:

1. Высокая анонимность: из-за того, что ни один узел в сети не знает, кто именно является пользователем, а также к какому ресурсу тот обращается, анонимность остаётся на высоком уровне.
2. Обход цензуры и фильтрации: из-за структуры маршрутизации и особенностей шифрования, Tor-трафик крайне сложно заблокировать, особенно если используется дополнительная защита в виде мостов и маскировки трафика.
3. Отсутствие доверия к одному посреднику: в отличие от VPN или прокси-сервисов, где весь трафик проходит через один сервер, в Tor каждый узел знает лишь предшествующий и следующий узлы, что уменьшает риски утечек данных.

Для усиления защиты и улучшения обхода блокировок Tor использует несколько механизмов. Одним из них являются Tor Bridges (мосты), которые представляют собой неафишируемые узлы, не публикуемые в открытых списках, что позволяет избежать блокировки самой сети Tor. Также существуют Pluggable Transports — специальные модули, которые маскируют трафик Tor под обычные протоколы, такие как HTTPS, Skype или видео. Наиболее известными из них являются:

1. obfs4 — шифрует трафик, делая его трудным для анализа.
2. meek — перенаправляет трафик через крупные CDN, такие как Google или Azure, что затрудняет блокировку.

3. snowflake — использует браузеры добровольцев как временные прокси, обеспечивая динамическую маршрутизацию трафика.

Однако, несмотря на все преимущества, у Tor есть и некоторые недостатки. Прежде всего, это медленная скорость. Многоступенчатая маршрутизация и возможная перегрузка узлов сети Tor могут значительно замедлить работу. Также многие веб-сайты блокируют выходные узлы Tor или требуют дополнительных проверок, таких как капчи, что затрудняет использование некоторых сервисов. Выходной узел, хотя и скрывает IP-адрес пользователя, остаётся уязвимым, так как данные на выходе могут быть перехвачены, если не используется HTTPS.

Пример использования Tor: пользователь, находящийся в стране с ограничениями доступа к новостному сайту, запускает Tor Browser. Браузер автоматически подключается к сети, используя либо мост, либо обычный входной узел. После этого трафик шифруется и проходит через три узла, выходя через exit-node в другой стране. В результате, несмотря на локальные цензурные ограничения, пользователь получает доступ к ресурсу.

4. АЛЬТЕРНАТИВНЫЕ МЕТОДЫ ОБХОДА БЛОКИРОВОК

Кроме широко известных методов, таких как VPN, прокси и Tor, существуют и другие технические подходы, которые могут эффективно обходить блокировки, особенно те, что основаны на DNS-фильтрации, SNI-инспекции и анализе трафика. Рассмотрим некоторые из них.

4.1 Изменение DNS-серверов

Один из самых простых и доступных способов обойти блокировки — это использование сторонних DNS-серверов. В ряде стран блокировка интернета начинается с подмены или удаления DNS-записей на уровне провайдера. Изменив настройки DNS на устройствах, пользователи могут обойти эти ограничения. Примеры популярных публичных DNS-серверов:

- Google Public DNS: 8.8.8.8, 8.8.4.4
- Cloudflare DNS: 1.1.1.1
- OpenDNS: 208.67.222.222

Однако использование сторонних DNS-серверов имеет свои ограничения. Если провайдер применяет DPI (Deep Packet Inspection), он может блокировать доступ к IP-адресам таких серверов. Кроме того, если блокировка осуществляется на уровне IP-адреса, обход через DNS становится бесполезным, поскольку проблема заключается уже в самом адресе сайта.

4.2 DNS over HTTPS (DoH) и DNS over TLS (DoT)

Чтобы предотвратить подмену и перехват DNS-запросов, были разработаны методы шифрования DNS-трафика. DNS over HTTPS (DoH) и DNS over TLS (DoT) — это две таких технологии, которые обеспечивают безопасность и обход блокировок. Эти методы шифруют DNS-запросы, что делает их трудными для анализа и фильтрации.

- DoH (DNS over HTTPS): Запросы передаются как обычный HTTPS-трафик, что делает их неотличимыми от стандартных веб-запросов.
- DoT (DNS over TLS): Запросы шифруются с использованием протокола TLS.

Преимущества этих технологий очевидны: они делают подмену DNS-запросов невозможной без расшифровки трафика, а блокировки, основанные на DNS, теряют свою эффективность. Однако существуют и недостатки. Некоторые страны и провайдеры пытаются блокировать известные DoH-серверы, такие как Google или Cloudflare. Также, для использования DoH и DoT необходимо, чтобы поддержка этих технологий была встроена в операционную систему или браузер.

4.3 ESNI / ECH (Encrypted Server Name Indication)

Когда используется HTTPS, доменное имя (Server Name Indication, SNI) передается открытым текстом во время процесса TLS-handshake. Это создаёт возможность для провайдеров блокировать трафик, даже если содержимое данных зашифровано. Для решения этой проблемы был предложен механизм ESNI (Encrypted SNI), а затем он был заменён на более современный ECH (Encrypted Client Hello), который является частью протокола TLS 1.3.

- ESNI (Encrypted SNI): Шифрует только доменное имя в запросах.
- ECH (Encrypted Client Hello): Шифрует весь блок Client Hello, включая SNI, что делает невозможным определение запрашиваемого ресурса на основе только SNI.

Преимущества этих технологий заключаются в скрытии даже самого факта обращения к конкретному сайту, что делает фильтрацию по домену невозможной. Однако такие

технологии поддерживаются не всеми браузерами, и для их работы требуется совместимость как со стороны серверов, так и DNS, через записи типа HTTPS RR.

4.4 CDN-обход (Domain Fronting)

Метод domain fronting представляет собой способ обхода блокировок, при котором трафик направляется к одному домену, например, google.com, а реальный запрос скрывается внутри HTTPS-запроса и отправляется на другой сайт. Это позволяет обойти блокировки, поскольку провайдер видит только google.com и не может заблокировать трафик без негативных последствий, таких как отключение популярных сервисов.

Пример использования domain fronting: запрос к сайту example.com инкапсулируется в HTTPS-запрос, направляемый на google.com. Провайдер видит только google.com, а реальный запрос проходит к заблокированному сайту.

Тем не менее, это метод активно блокируется крупными CDN-провайдерами по требованию государств, и, например, Google и AWS больше не поддерживают domain fronting. Поэтому он может работать лишь в специфических случаях или при использовании альтернативной инфраструктуры.

5. МЕТОДЫ БОРЬБЫ С VPN

5.1 Блокировка по IP-адресам VPN-серверов

Одним из распространённых методов блокировки VPN-сервисов является блокировка по IP-адресам. Поскольку большинство VPN-сервисов используют публичные IP-адреса своих серверов, государственные органы или интернет-провайдеры могут собирать эти адреса в чёрные списки и запрещать подключение к ним на уровне фаервола или DPI-систем. Информация о таких IP-адресах может поступать из публичных списков VPN-адресов, автоматического мониторинга трафика пользователей или логов хостинг-провайдеров.

Однако данный метод имеет свои недостатки: VPN-сервисы могут периодически менять IP-адреса или использовать динамическую ротацию, что затрудняет блокировку. Кроме того, бывает сложно отличить трафик VPN от обычного серверного трафика, если используется нестандартный порт.

5.2 Блокировка по портам

VPN-сервисы часто используют определённые порты по умолчанию. Например, OpenVPN работает через порт 1194 (UDP или TCP), PPTP — через порт 1723, а L2TP/IPsec использует порты 500, 4500 и 1701. Блокировка этих портов позволяет ограничить или заблокировать доступ к VPN-серверам.

Тем не менее, это решение не всегда эффективно, поскольку многие VPN могут перенастроить свои подключения на порты 443 (HTTPS) или 80 (HTTP), что делает их трафик неотличимым от обычного веб-сёрфинга. Более того, некоторые VPN-клиенты используют технологии обхода, такие как obfsproxy или stunnel, которые маскируют трафик и делают его трудным для идентификации.

5.3 Глубокая инспекция пакетов (DPI)

Технология Deep Packet Inspection (DPI) позволяет анализировать содержимое сетевых пакетов и распознавать сигнатуры VPN-протоколов, даже если они используют нестандартные порты. DPI может обнаруживать нестандартные handshake-сообщения, характерные для OpenVPN или WireGuard, а также определять временные характеристики и структуру пакетов, характерные для VPN-трафика. Также возможна идентификация TLS-соединений с нетипичными параметрами.

Для обхода таких систем, VPN-сервисы применяют различные методы обфускации, такие как использование obfsproxy или xor-патчей, а также шифруют handshake-сообщения. Также используются протоколы с камуфляжем, например, Shadowsocks, Outline или trojan, которые позволяют маскировать VPN-трафик.

5.4 Блокировка по SNI и TLS fingerprint

Метод блокировки по SNI (Server Name Indication) заключается в том, что при использовании TLS-соединений (например, с OpenVPN over TLS), доменное имя может передаваться в незашифрованном виде, что позволяет определить, что соединение устанавливается с VPN-хостом. Также возможен анализ TLS fingerprint, который представляет собой уникальный отпечаток, создаваемый на основе параметров TLS-соединения, таких как алгоритмы шифрования и версии протоколов.

Для борьбы с этим методом VPN-сервисы используют шифрование SNI (или его полное удаление, как в случае с ECH), а также искажают параметры TLS, чтобы сделать их похожими на обычный трафик браузера.

5.5 Активация принудительного MITM (man-in-the-middle)

Некоторые государства реализуют централизованный перехват TLS-трафика путём установки на устройствах пользователей доверенного корневого сертификата. Это позволяет расшифровывать VPN-туннели и блокировать их. Примером такого подхода является попытка Казахстана в 2019 году внедрить обязательный корневой сертификат для перехвата TLS-соединений.

Этот метод нарушает принципы безопасности TLS и вызывает негативную реакцию со стороны пользователей. Кроме того, массовая реализация на всех устройствах оказывается технически сложной.

5.6 Ограничение трафика и QoS

Если провайдер не может заблокировать VPN, он может использовать метод замедления трафика. При обнаружении характерного паттерна VPN-соединений скорость может быть урезана до уровня, когда использование VPN становится невозможным или крайне неудобным. Кроме того, устанавливаются лимиты на количество подключений, а также применяются меры по приоритизации трафика, например, предпочтение HTTP/HTTPS.

Этот метод имеет свои ограничения, поскольку границы между VPN-трафиком и трафиком легитимных сервисов могут быть нечёткими. В результате, при замедлении VPN-соединений может ухудшиться качество работы и других легитимных сервисов.

5.7 Юридические и организационные меры

Помимо технических методов, государства могут предпринимать юридические и организационные меры, направленные на ограничение использования VPN. Они могут требовать от VPN-провайдеров сотрудничества или регистрации, а также вводить официальные запреты на использование нелегальных VPN-сервисов (например, в России). Также вводятся административные и уголовные меры ответственности за использование "неразрешённых" VPN.

Эти меры являются дополнением к техническим методам блокировки и могут значительно ограничить доступ пользователей к VPN-сервисам.

6. МЕТОДЫ БОРЬБЫ С TOR

Сеть Tor была создана с целью обеспечения анонимности и обхода цензуры. Однако, несмотря на сложность полного блокирования этой сети, правительства и интернет-провайдеры всё же применяют различные методы для борьбы с её использованием. Это включает в себя как блокировку известных узлов, так и более сложные методы, такие как анализ трафика, который использует обфускацию.

6.1 Блокировка известных IP-адресов узлов Tor

Одним из способов противодействия Tor является блокировка известных IP-адресов её узлов. В сети Tor большинство узлов — открытые, и их IP-адреса можно найти в публичных реестрах, которые обновляются через специальные файлы, называемые consensus. Эти файлы распространяются Tor Directory Authorities, и их можно использовать для автоматической блокировки IP-адресов через фаерволы провайдеров. Сюда входят:

- Входные узлы (или Guard nodes),
- Промежуточные узлы,
- Выходные узлы.

Кроме того, могут блокироваться и Bridge-узлы, если они не скрыты. Однако этот метод имеет свои ограничения, так как блокировка становится неэффективной при использовании мостов или протоколов, таких как obfs4. Кроме того, удалённые мосты сложнее обнаружить без активного мониторинга трафика.

6.2 Глубокая инспекция пакетов (DPI)

Провайдеры, использующие DPI (глубокую инспекцию пакетов), могут анализировать этапы подключения пользователя к сети Tor, распознавая характерные TLS-handshake-сигнатуры. Это позволяет обнаружить попытки подключения к публичным узлам Tor, поскольку их трафик отличается от обычного HTTPS-трафика. Вдобавок, DPI-системы могут распознавать версии обфускационных протоколов, таких как obfsproxy.

Для противодействия этому Tor использует технологию Pluggable Transports (PT). Это такие протоколы, как:

- obfs4, который добавляет псевдослучайную обфускацию трафика,
- meek, который туннелирует трафик через HTTPS CDN (например, через Google),

- snowflake, который использует браузеры добровольцев как промежуточные прокси.

Эти меры позволяют скрыть трафик Tor от системы DPI, делая его более трудным для обнаружения.

6.3 Блокировка мостов (Bridges)

Bridge-узлы (или мосты) Tor используются для обхода цензуры в странах с жесткими ограничениями. Некоторые мосты публикуются в открытых реестрах, но другие предоставляются пользователям вручную, например, через почту или Telegram. Это создаёт дополнительные проблемы для провайдеров, пытающихся блокировать Tor, поскольку мосты не так легко обнаружить.

Когда мосты становятся известными, они могут быть заблокированы по IP-адресам. Также можно использовать DPI для выявления использования обфускации через obfs4. В ответ на это Tor постоянно обновляет список мостов, а также использует встроенные мосты в браузерах, таких как Tor Browser. Также развивается новый протокол Snowflake, который децентрализует узлы, делая их более трудными для блокировки.

6.4 Блокировка Pluggable Transports

В странах с особенно жёсткой цензурой, таких как Китай и Иран, могут блокировать и сами Pluggable Transports. Например, обфускационные протоколы, такие как meek и obfs4, могут быть обнаружены с помощью анализа handshake-паттернов. Также могут блокировать домены CDN, через которые работает meek (например, Google AppEngine или CloudFront), а также анализировать JA3 TLS fingerprint соединений для определения Tor-трафика.

В ответ на это Tor постоянно обновляет свои обфускационные протоколы, а также развивает Snowflake, который использует WebRTC для создания децентрализованных узлов.

6.5 Блокировка по ключевым DNS-запросам и SNI

Некоторые узлы Tor могут использовать специфические доменные имена или ключи в DNS-запросах, что может быть использовано для выявления попытки подключения. Кроме того, возможна фильтрация по SNI (Server Name Indication), если используется протокол meek или другие CDN-туннели.

Для обхода этих блокировок Tor применяет методы шифрования, такие как ECH (Encrypted Client Hello), чтобы скрыть информацию о целевом сервере. Также используется технология

для перехода на нестандартные домены и туннели, что затрудняет определение, что это трафик Tor.

6.6 Принудительный контроль над TLS (MITM)

В теории возможна атака MITM (man-in-the-middle), когда цензор может установить поддельные сертификаты для перехвата TLS-трафика. Однако Tor защищён встроенной цепочкой доверия, которая сложна для подделки. Это затрудняет успешное выполнение MITM-атаки, так как Tor использует проверенные сертификаты и цепочку доверия, что делает перехват и дешифровку трафика практически невозможным.

7. МЕТОДЫ БОРЬБЫ С DoH, DoT, ECH И DOMAIN FRONTING

Технологии DoH (DNS over HTTPS), DoT (DNS over TLS), ECH (Encrypted Client Hello) и domain fronting делают возможным шифрование данных, которые обычно используются для цензуры. С помощью этих технологий скрываются DNS-запросы и TLS-заголовки, что осложняет блокировку веб-сайтов. Однако для подавления этих технологий требуются более сложные и ресурсоёмкие методы.

7.1 DoH (DNS over HTTPS) и DoT (DNS over TLS)

Обе эти технологии шифруют DNS-запросы, скрывая от провайдера, какие домены запрашивает пользователь. Это делает невозможным использование традиционной DNS-фильтрации, которая является основным методом цензуры.

Методы борьбы с DoH и DoT:

1. Блокировка известных серверов DoH/DoT. Провайдеры могут блокировать публичные DNS-серверы, такие как Cloudflare (1.1.1.1) и Google (8.8.8.8). Однако этот метод не всегда эффективен, поскольку пользователь может выбрать нестандартный сервер.
2. DPI-выявление и блокировка трафика DoH/DoT. Некоторые системы могут обнаружить характерный трафик DoH/DoT, даже если используется CDN или прокси.
3. Принудительное использование локального DNS. Провайдеры могут перенаправить все DNS-запросы через контролируемый DNS-сервер.

7.2 ECH (Encrypted Client Hello)

ECH — это новая технология, которая шифрует часть данных в ClientHello пакете в TLS 1.3, включая SNI (Server Name Indication). Это позволяет скрыть информацию о сервере, с которым устанавливается соединение, что делает блокировку сайтов сложнее.

Методы борьбы с ECH:

1. Блокировка хостов, поддерживающих ECH. Для этого создаются списки серверов, которые поддерживают ECH, и блокируются их IP-адреса. Однако это может повлечь за собой блокировку популярных CDN, таких как Cloudflare.
2. Снижение версии TLS. Провайдеры могут принудительно ограничивать поддержку TLS 1.3 или блокировать соединения с непонятным ClientHello.

Таким образом, несмотря на все усилия цензоров, технологии шифрования, такие как DoH, DoT и ECH, продолжают развиваться, предоставляя пользователям инструменты для обхода цензуры и обеспечения конфиденциальности.

7.3 Domain Fronting:

Техника domain fronting представляет собой способ обхода интернет-цензуры, при котором реальный домен соединения скрывается за другим, разрешённым доменом. Это позволяет обойти блокировки, маскируя истинный адрес сайта или сервиса, с которым устанавливается соединение, под домен, который не вызывает подозрений у провайдеров или государственных органов.

Когда пользователь пытается подключиться к заблокированному сайту, например hidden.site.com, он может использовать разрешённый домен, такой как www.google.com, для маскировки этого запроса. В момент установления соединения через SNI (Server Name Indication) и TLS передаётся именно домен www.google.com, что делает его видимым для провайдера и системы фильтрации, однако внутри самого HTTPS-запроса скрывается настоящий домен — hidden.site.com.

Инфраструктура CDN (Content Delivery Network), такая как Google, Cloudflare или Amazon CloudFront, принимает запрос и, согласно внутренним правилам маршрутизации, пересылает его на нужный сервер, не обращая внимания на то, что скрыто внутри запроса. Такой подход

эффективно скрывает реальный адрес ресурса и помогает пользователю обойти блокировки, установленные на уровне DNS или IP.

Методы борьбы с Domain Fronting

1. Блокировка фронтирующих CDN:
   Некоторые страны, в частности Иран и Китай, пошли на радикальные меры, блокируя весь трафик, который проходит через CDN, поддерживающие domain fronting. Этот метод предотвращает использование технологии для обхода блокировок, ведь все запросы через эти CDN начинают блокироваться. Однако такая мера имеет свои ограничения и последствия.

   Недостатки:

   - Массовые сбои сервисов: Блокировка трафика через все CDN, которые поддерживают domain fronting, может привести к массовым сбоям в работе популярных сервисов, таких как Google, Amazon или Cloudflare, что затруднит доступ пользователей к множеству легитимных и востребованных ресурсов.
   - Закрытие поддержки domain fronting: Некоторые крупные компании, например Google и Amazon, уже в 2018 году закрыли возможность использования domain fronting на своей инфраструктуре, что снизило её эффективность как метода обхода блокировок.

2. DPI-анализ поведения TLS/HTTPS:
   Несмотря на использование domain fronting, трафик всё же можно идентифицировать по характерным признакам. Например, в запросах может наблюдаться несоответствие между доменом в SNI и заголовке Host. Такое несоответствие можно зафиксировать с помощью DPI (глубокой инспекции пакетов), анализируя такие паттерны, как различные домены в этих заголовках или специфические пути запроса.

   Ответные меры:

   - Для обхода этой фильтрации используется технология ECH (Encrypted Client Hello), которая полностью шифрует handshake и скрывает такие данные, как SNI, в процессе установки соединения. Это усложняет задачу для цензоров и провайдеров, которые пытаются распознать и заблокировать domain fronting.

В результате, несмотря на существующие методы борьбы, domain fronting остаётся важным инструментом для пользователей, стремящихся обойти блокировки, хотя его эффективность зависит от того, насколько активно цензоры применяют новые методы анализа и блокировки трафика.

ЗАКЛЮЧЕНИЕ

В ходе проведённого исследования была рассмотрена актуальная проблема цифровой цензуры и способов её обхода. Мы подробно проанализировали ключевые технологии, применяемые для обхода региональных блокировок, включая VPN, Tor, DoH/DoT, ECH и domain fronting. Наряду с этим была представлена система методов, применяемых для их блокирования.

Современные технологии обхода блокировок развиваются в сторону повышения анонимности, маскировки трафика и шифрования служебной информации. Это существенно снижает эффективность традиционных методов фильтрации.

Наиболее распространёнными средствами обхода являются VPN-сервисы, сеть Tor и шифрованные DNS-технологии (DoH, DoT). Все они отличаются устойчивостью к простым методам блокировки.

Цензоры применяют комплексные технологии противодействия, включая блокировку IP-адресов, глубокую инспекцию пакетов (DPI), фильтрацию SNI и DNS-запросов, а также поведенческий анализ трафика.

Выводы практического характера:

1. Блокировка IP-адресов и DNS-фильтрация являются базовыми, но недостаточно надёжными методами в современных условиях.
2. Применение DPI и поведенческого анализа требует серьёзных ресурсов, но обеспечивает более высокую эффективность, особенно против Tor и обфусцированных прокси.
3. Эффективное противодействие должно строиться на комбинации техник, включая централизованную регистрацию устройств, принудительное использование локального DNS и интеллектуальный анализ сетевой активности.

СПИСОК ЛИТЕРАТУРЫ

1. Аверченков В.И. Основы научного творчества [Электронный ресурс]: учеб. пособие / В.И. Аверченков, Ю.А. Малахов. — Брянск: Брянский государственный технический университет, 2012. — 156 с. — Режим доступа: http://www.iprbookshop.ru/7004.
2. Астанина С.Ю. Научно-исследовательская работа студентов (современные требования, проблемы и их решения) [Электронный ресурс]: монография / С.Ю. Астанина, Н.В. Шестак, Е.В. Чмыхова. — М.: Современная гуманитарная академия, 2012. — 156 с. — Режим доступа: http://www.iprbookshop.ru/16934.
3. Афанасьев С. В. Deep Packet Inspection и его применение в современных сетях [Электронный ресурс] // Хакер. — 2020. — № 8. — Режим доступа: https://xakep.ru/2020/08/12/dpi-deep-packet-inspection.
4. Комлацкий В.И. Планирование и организация научных исследований [Электронный ресурс]: учебное пособие / В.И. Комлацкий, С.В. Логинов, Г.В. Комлацкий. — Ростов-на-Дону: Феникс, 2014. — 205 с. — Режим доступа: http://www.iprbookshop.ru/58980.
5. Мокий М.С. Методология научных исследований: учебник / М.С. Мокий, А.Л. Никифоров, В.С. Мокий. — М.: Юрайт, 2015. — 255 с.
6. Рыжков И.Б. Основы научных исследований и изобретательства [Электронный ресурс]: учеб. пособие / И.Б. Рыжков. — СПб.: Лань, 2013. — 224 с. — Режим доступа: http://e.lanbook.com/book/30202.
7. Требования, правила выполнения и защиты магистерской диссертации [Электронный ресурс]: методические указания / Н.Ю. Донец. — СПб.: СПбГАУ, 2012. — 13 с. — Режим доступа: http://biblioclub.ru/index.php&?page=book&id=364366.
8. Cahn A., Alfeld S., Barford P., Miskovic S. An Empirical Study of Tor Hidden Services Discoverability [Электронный ресурс] // arXiv.org. — 2017. — Режим доступа: https://arxiv.org/abs/1709.01436.
9. Cloudflare. Understanding Encrypted Client Hello (ECH) [Электронный ресурс]. — 2022. — Режим доступа: https://blog.cloudflare.com/encrypted-client-hello.
10. Ensafi R., Winter P., Mueen A., Crandall J. Detecting Intentional Packet Drops on the Internet via TCP Inconsistencies [Электронный ресурс] // Passive and Active Measurement

Conference. — 2014. — Режим доступа: https://cs.unm.edu/~crandall/papers/ensafi14pam.pdf.

11. Fifield D. Domain Fronting for Circumvention [Электронный ресурс]: whitepaper / D. Fifield, R. Ensafi, P. Winter. — 2015. — Режим доступа: https://www.bamsoftware.com/papers/fronting.

12. Mozilla. DNS-over-HTTPS (DoH) [Электронный ресурс]. — 2023. — Режим доступа: https://wiki.mozilla.org/Trusted_Recursive_Resolver.

13. OpenNet Initiative. Internet Filtering in Iran [Электронный ресурс]: Country Profile. — 2013. — Режим доступа: https://opennet.net/research/profiles/iran.

14. Tor Project. Pluggable Transports [Электронный ресурс]. — 2023. — Режим доступа: https://2019.www.torproject.org/docs/pluggable-transports.html.

15. Winter P., Lindskog S. How China Is Blocking Tor [Электронный ресурс] // Free and Open Communications on the Internet (FOCI). — 2012. — Режим доступа: https://www.cs.kau.se/philwint/pdf/foci2012.pdf.

16. Xu H., Narayanan A. ECH and the Future of TLS Privacy [Электронный ресурс] // Princeton University. — 2021. — Режим доступа: https://freedom-to-tinker.com/2021/06/10/ech-and-the-future-of-tls-privacy.