Анализ существующих методов управления доступом к интернет-ресурсам и рекомендации по их применению.

Москва

Апрель 2013 г.

РЕФЕРАТ

Отчет «Анализ существующих методов управления доступом к интернет-ресурсам и рекомендации по их применению» содержит 109 страниц, 7.разделов, 18 рисунков.

Цель работы заключается в исследовании круга проблем, связанных с обеспечением безопасного публичного использования сети Интернет, и определении сбалансированных подходов, обеспечивающих решение соответствующих задач, входящих в сферу полномочий Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - Роскомнадзор).

В ходе выполнения работы решаются следующие задачи:

- Описание основных сфер управления Интернетом и ключевых органов, участвующих в управлении доступом к интернет-ресурсам;

- Анализ основных механизмов и инструментов реализации функции управления доступом к интернет-ресурсам

- Выработка предложений по использованию наиболее эффективных механизмов и инструментов реализации функции управления доступом к интернет-ресурсам с учетом передовой практики зарубежных стран и правовых норм Российской Федерации.

Краткое изложение

Цель настоящего исследования заключается в сравнительном анализе и оценке методов блокирования противоправного контента в сети Интернет и формировании предложений по использованию наиболее эффективных из них (или комбинаций нескольких методов) на основе набора отобранных для настоящего исследования качественных критериев технологического и экономического характера, а также передовой практики зарубежных стран.

В рамках работы также рассматриваются следующие вопросы:

- Модели и технологии блокирования, их воздействие и последствия для сети Интернет;
- Эффективность различных методов и технологий блокирования, оценка возможностей обхода блокирования с точки зрения обеспечения желаемого эффекта и возможностей для большинства операторов веб-сайтов обойти указанное блокирование;
- Возможность использования интернет-провайдерами мер по предотвращению обхода блокирования;
- Возможность «точного» блокирования части веб-сайтов, оценка эффективности применения этого метода;
- Оценка текущих подходов к блокированию интернет-ресурсов в рамках действующего законодательства.

Таким образом, в настоящей работе упор сделан на представление обзора доступных методов блокирования и оценке эффективности их реализации с технической точки зрения. Оценка пропорциональности применения инструмента блокирования веб-сайтов и эффективность этой меры для решения задач в социальной сфере, духовно-нравственной и воспитательной целях в цели настоящей работы не входят.

О блокировании интернет-ресурсов

Учитывая специфику построения Интернета, подходы к блокированию рассматриваются на базе трех моделей блокирования: сетевого блокирования, инфраструктурного блокирования и блокирования в точке подключения (со стороны пользователя).

На данный момент преобладающим является сетевой подход к блокированию. Существует несколько первичных технологий, обеспечивающих сетевое блокирование доступа к интернет-ресурсам:

• Блокирование по IP адресу: настройка сетевого оборудования ISP-поставщика для запрета Интернет-трафика к/от заблокированного сайта;

• Блокирование с помощью изменений системы доменных имен (DNS): путем настройки DNS серверов интернет-провайдеров;

• Блокирование по URL: блокирование определенных элементов веб-сайтов, например, http://www.example.com/zapretinfo.html;

• Блокирование с использованием анализа пакетов: блокирование с помощью решений с анализом трафика, либо на верхнем уровне (поверхностная проверка пакетов, заголовков пакетов (SPI)), либо на более детальном уровне (углубленная проверка содержания пакетов информации (DPI)).

Для сетевого подхода к блокированию также были рассмотрены смешанные варианты:

1. блокирование DNS совместно с поверхностной проверкой пакетов;
2. блокирование DNS совместно с URL-блокированием;
3. блокирование DNS совместно с углубленным анализом пакетов;
4. блокирование с выделением по IP адресам и URL блокированием.

На инфраструктурном уровне были рассмотрены блокирование на уровне авторитетных серверов DNS и в реестрах DNS и IP-адресов.

При оценке каждого метода использовались следующие критерии: быстрота реализации; стоимость; эффективность блокирования; сложность

обхода; масштабируемость; влияние на производительность сети; а также воздействие блокирования на законные сервисы.

Результаты оценки позволяют утверждать, что ни один из вышеуказанных методов не является на 100% эффективным; каждый из них требует определенных затрат на его реализацию и оказывает влияние на производительность сети, а большинство также несет в себе риск избыточного блокирования «невиноватых» ресурсов.

Для квалифицированных пользователей в большинстве случаев остается возможным обход блокирования. Не имеет смысла рассматривать вариант блокирования защищенного трафика, так как его реализация приводит к полному обесцениванию Интернета как среды, обеспечивающей инновации, реализацию бизнес-проектов или значимых сервисов.

Результаты проведенного анализа и оценки эффективности использования отдельных методов (комбинаций нескольких методов) блокирования позволяют сделать следующие выводы:

- Ни один из исследованных методов блокирования не является абсолютно эффективным;
- Для каждого из них характерны определенные издержки: финансовые (стоимость внедрения и дальнейшей поддержки), производственно-технологические (степень влияния на производительность Сети), специфические издержки в виде риска избыточного блокирования легитимных ресурсов, а также репутационные издержки для страны в целом;
- Наиболее адекватным архитектуре Интернета методом блокирования следует признать блокирование в точках подключения;
- С практической точки зрения, с учетом быстроты, стоимости реализации и минимума негативных последствий, оптимальным методом следует признать блокирование по URL с предварительным выделением запросов по IP адресам;

- Блокирование должно осуществляться на уровне провайдеров доступа в Интернет, непосредственно обслуживающих конечных клиентов.

Необходимо оговориться, однако, что, учитывая сложившуюся практику управления использованием сети Интернет, членство Российской Федерации в ряде авторитетных международных организаций и «клубов» развитых стран, а также перспективу вступления в другие подобного рода объединения, рекомендуется сделать, - по крайней мере, формально - вопросы возможности, допустимости, адекватности и пропорциональности реализации тех или иных методов блокирования предметом широкой общественной дискуссии с учетом всех ключевых заинтересованных сторон: государства, бизнеса, гражданского общества, науки и интернет-пользователей.

Содержание

Краткое изложение 3

1. Введение 8

2. Архитектура сети Интернет и основные принципы ее функционирования 11

2.1 Общие сведения 11

2.2 Управление Интернетом 16

2.3 Основные принципы архитектуры Интернета 21

2.3.1 Сквозное подключение и “прозрачность” 21

2.3.2. Иерархичность 22

2.3.3 Распределенность и мобильность 23

2.3.4. Локальность и автономность 24

3. Модели и технологии блокирования ресурсов Интернет 26

3.1. Сетевое блокирование 27

3.1.1 Блокирование по IP-адресам 36

3.1.2 Блокирование с помощью DNS 41

3.1.3 Блокирование сайтов по URL 46

3.1.4 Блокирование с помощью анализа содержимого пакетов 53

3.1.5 Комбинированное блокирование 57

3.2. Инфраструктурное блокирование 58

3.3. Блокирование в точке подключения 68

4. Анализ практики блокирования и оценка перспектив сети Интернет 72

4.1. Опыт и практика борьбы с незаконными сервисами 72

4.2. Анализ последствий применяемых технологий 74

4.3 Новые внедряемые технологии и их влияние на блокирование сайтов 74

4.4 Заключение о методах блокирования 82

5. Регулирование доступа к запрещенной информации в Интернете на территории Российской Федерации 83

6. Сопутствующие аспекты, связанные с блокированием 92

7. Рекомендации по организационным и техническим решениям 97

8. Заключение 99

Обозначения и сокращения 102

Технический глоссарий 105

Список использованной литературы 108

1. Введение

Исследование методов ограничения доступа к интернет-ресурсам, на которых располагается противоправный контент, - сложная задача, подразумевающая комплексный анализ набора юридических, организационных, технических и правоприменительных практик – как специфических для Российской Федерации, так и зарубежных государств, - а также ряда международных органов и организаций.

Настоящее исследование подготовлено в развитие идей, методологии и результатов следующих работ и материалов [OFCOM] [SAC056] [IETFILTERING], обсуждений с их авторами, по итогам рабочего семинара 180 Форума по управлению Интернет при ООН [IGF2012WS180], а также личных дискуссий с рядом известных зарубежных экспертов отрасли.

Цель настоящей работы заключается в исследовании круга проблем, связанных с обеспечением безопасного публичного использования сети Интернет, и определением сбалансированных подходов, обеспечивающих решение соответствующих задач, входящих в сферу полномочий Роскомнадзора.

В ходе выполнения работы решаются следующие задачи:

- Описание основных сфер управления Интернетом и ключевых органов, участвующих в управлении доступом к интернет-ресурсам;

- Анализ основных механизмов и инструментов реализации функции управления доступом к интернет-ресурсам;

- Выработка предложений по использованию наиболее эффективных механизмов и инструментов реализации функции управления доступом к интернет-ресурсам с учетом передовой практики зарубежных стран и правовых норм Российской Федерации.

Для целей настоящей работы ограничение доступа к интернет-ресурсам, на которых размещается противоправный контент, понимается как блокирование указанных ресурсов. В этой связи следует отметить, что в

отсутствие единого общепризнанного определения под блокированием интернет-ресурсов (далее - блокирование) в данной работе понимается набор законодательно установленных государством и/или добровольно имплементируемых – совместно или по отдельности - техническим, бизнес-сообществом или сообществом интернет-пользователей организационно-технических мер, призванных ограничить доступ к определенной информации или интернет-ресурсам.

Очевидно, что вне зависимости от избранного метода блокирования (их число сегодня невелико, и все они хорошо известны), масштабов и интенсивности его применения в национальном сегменте сети Интернет это предполагает наличие определенных исполнителей самой функции блокирования, инструментария и технологии ее реализации, а также эффектов от его применения для всех ключевых заинтересованных сторон процесса (включая и нарушителей правил).

В этой связи следует отметить специфические проблемы и риски, возникающие на уровне государства как участника этого процесса.

С точки зрения концептуальной, это, в первую очередь, возможная недооценка сложности и многомерности архитектуры сети Интернет, принципов, лежащих в ее основе и роли в ней ключевых органов и организаций глобальной системы управления Интернетом. В этой связи следует также отметить и трансграничный характер Интернета, который порождает известную неопределенность в процессе принятия решений в правовой, организационной, структурной и технологической областях.

С экономической точки зрения, процесс принятия решений по блокированию тех или иных интернет-ресурсов требует постоянного учета баланса выгод и затрат: поскольку общепризнанно, что Интернет сегодня – один из ключевых движителей экономического развития, непродуманные действия по блокированию ресурсов в нем могут иметь крайне неблагоприятные социально-экономические последствия даже в

краткосрочной перспективе и к тому же оказаться неэффективными в средне- и долгосрочной перспективе.

Наконец, Правительству Российской Федерации следует оценивать не только экономическую эффективность тех или иных мер по блокированию интернет-ресурсов, но и потенциальные репутационные риски: учитывая стремление России к членству в различных «клубах» развитых стран, в большинстве своем с уже устоявшимися и формализованными в соответствующих программных документах принципами управления Интернетом, правительство страны вынуждено руководствоваться передовой практикой этих организаций и их членов в указанной сфере или, по крайней мере, обеспечивать проверку тех или иных действий по блокированию интернет-ресурсов на адекватность/пропорциональность их воздействия на Сеть.

Исходя из этих соображений, в первом разделе настоящей работы представлен краткий обзор специфики архитектуры Интернета и управления его развитием, основных механизмов и инструментов хранения и передачи данных в нем, а также участников этих процессов.

В следующем разделе рассматриваются основные способы блокирования интернет-ресурсов с учетом ряда предложенных нами качественных критериев.

Далее в анализ также включен краткий обзор существующего законодательства, обеспечивающего возможность блокирования интернет-ресурсов.

В заключение предлагается ряд рекомендаций по техническим решениям и организационно-техническим мероприятиям, которые необходимы для обеспечения должного баланса между законными интересами государства и задачей развития Интернета как трансграничной среды и ключевого фактора социально-экономического развития России.

2. Архитектура сети Интернет и основные принципы ее функционирования

2.1 Общие сведения

Прежде чем рассмотреть методы, используемые для ограничения доступа к интернет-ресурсам, на которых располагается нелегальный контент, следует коротко остановиться на архитектуре Интернета, используемых интернет-протоколах и структуре системы управления Интернетом.

Интернет – это общедоступная сеть глобально взаимоподключенных сетей, которые обмениваются данными с использованием стандартизированного набора протоколов, называемого стеком протокола управления передачей и Интернет-протокола (TCP/IP-стек).

Для описания работы сети часто используется семиуровневая модель OSI (Open System Interconnect Model). Для целей настоящего исследования интерес представляют четыре уровня этой модели в интерпретации, принятой по отношению к протоколам Интернет. Чем ниже уровень, тем ближе его функциональность находится к работе физической сети.

Сетевой уровень в нашем случае включает в себя также и нижележащие уровни аппаратного интерфейса и интерфейса среды передачи данных, например, волоконную оптику или Ethernet.

Уровень IP (Internet Protocol – Интернет протокола) связан, прежде всего, с созданием пакетов данных, маршрутизацией и пересылкой пакетов к месту назначения в соответствии с IP-адресом, указанным в заголовке пакета.

Транспортный уровень определяет требования к подключению и надежность данных, передаваемых по сети.

Наконец, уровень приложения определяет взаимодействие с функциональностью нижнего транспортного уровня и осуществляюшей запрос внешней программой конечного пользователя, например, веб-браузером или почтовым клиентом.

Каждый из методов сетевого блокирования, которые мы рассмотрим, действует на определенном уровне в стеке. Чем ниже в стеке действует метод блокирования, тем менее точен этот метод блокирования.

Таблица 2.1.1: Применение методов блокирования в наборе протоколов Интернет

TCP/IP-модель	Пользователи	Блокирование	
Приложение	Веб-страницы (http) Система доменных имен (DNS) Протокол передачи файла (ftp)	URL DNS Углубленный анализ пакета	Наиболее точный
Транспортный	Протокол управления передачей Протокол дейтаграмм	IP/Порт (сервис) Простая проверка пакетов	
Интернет протокола/межсетевой	Адрес Интернет-протокола	IP-блокирование	Наименее точный
Сетевой	Ethernet, ATM		

Следует отметить, что к сервисам Интернет относятся не только WWW сайты, но и многие другие ресурсы сети доступные по отличным от http протоколам. Доступ же к веб-серверам, которые обслуживают страницы, осуществляется через веб-браузеры. В пределах веб-браузера веб-страницы

отображаются/исполняются, показывая текст, изображения, анимацию и ссылки на другие веб-страницы.

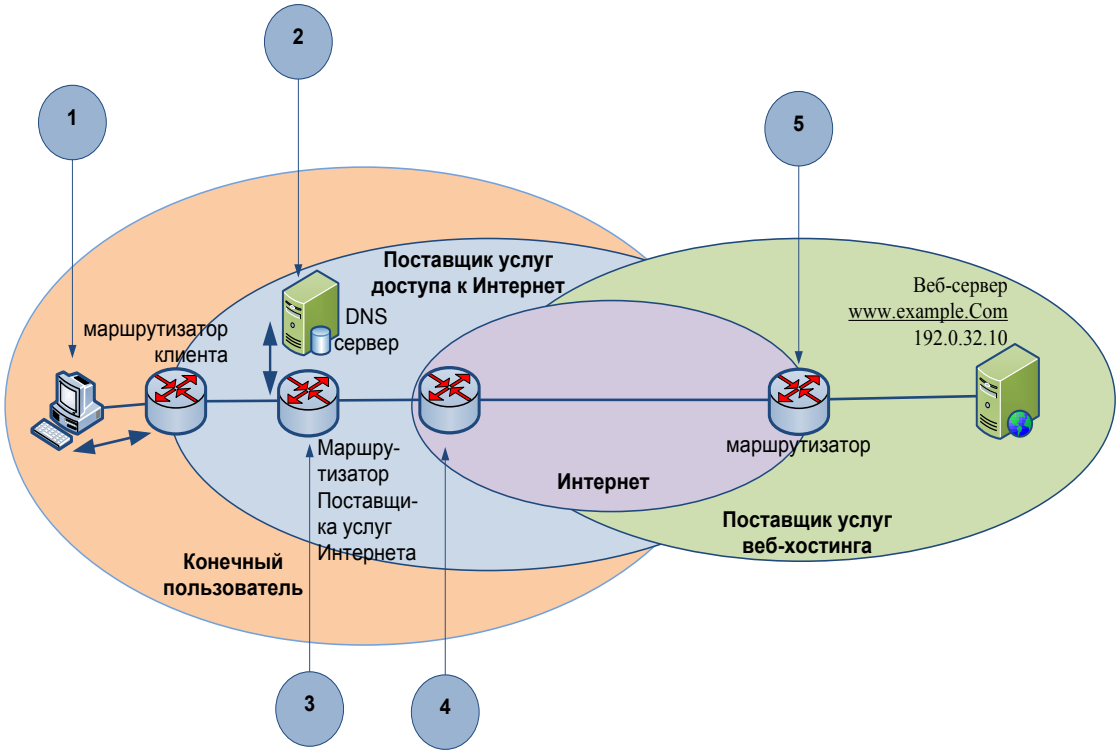
Когда пользователи запрашивают и получают веб-страницу – они полагаются на ряд связанных между собой интернет-услуг (см. Рисунок 2.1.1), которые включают в себя следующее:

• подключение (широкополосное) поставщика услуг Интернета;

• систему доменных имен (перевод доменных имен в IP-адреса);

• сетевую маршрутизацию/трансляцию адресов;

• веб-сервер.



Обозначение	Пояснение
1	Какой IP-адрес для www.example.com?
2	IP-адрес www.example.com - 192.0.32.10
3	Положение IP-адреса 192.0.32.10 – этот путь
4	Положение IP-адреса 192.0.32.10 – этот путь
5	IP-адрес 192.0.32.10 находится в моей сети

Рисунок 2.1.1 Общий обзор запроса веб-страницы

Операторы Интернета, известные также как интернет-провайдеры, обеспечивают конечным пользователям доступ в Интернет, и в основном де-факто работают в рамках неформальной иерархии, (см. Рис. 2.1.2) Как правило выделяют три уровня интернет-операторов, каждый из которых обычно использует и пиринг (т.е. обмен трафиком клиентов без оплаты) и платные подключения к другим интернет-операторам. Пиринг осуществляется интернет-операторами одного и того же уровня. В то же время интернет-операторы более высокого уровня продают подключение к Интернету тем, кто имеет более низкий статус. Интернет-провайдеры первого (высшего) уровня, представленные крупнейшими телекоммуникационными компаниями, в основном, не платят другим операторам за трафик, передаваемый через другие сети (то есть используют пиринг). Операторы второго уровня осуществляют пиринг с некоторыми сетями (как правило, другими операторами второго уровня), но, как правило, приобретают IP-транзит и другие услуги у операторов первого уровня для доступа в Интернет. Операторы третьего уровня, как правило, приобретают все необходимые услуги у операторов либо первого, либо второго уровня.

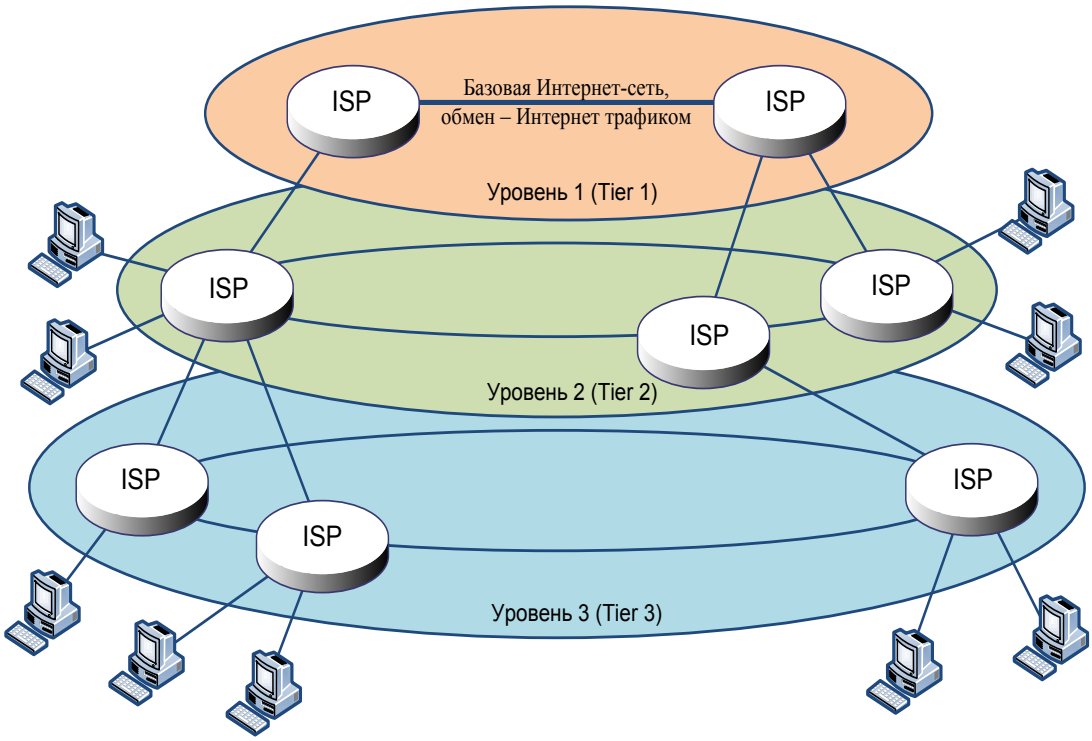


Рисунок 2.1.2 Схема взаимодействия интернет-провайдеров различных уровней

2.2 Управление Интернетом

Чтобы понять некоторые проблемы, появляющиеся при разработке и выборе методов блокирования ресурсов, необходимо иметь представление о системах управления и администрирования, которые делают возможной бесперебойную работу Интернета.

Администрирование и управление Интернетом является глобальным процессом с участием национальных и международных организаций (государственных и негосударственных).

Таблица 2.2.1: Основные органы управления Интернетом

Управление Интернетом					
Стандарты Интернет-технологий			**Ресурсы Интернет-адресации**		
МСЭ (ITU)	**Консорциум W3C**	**IETF**	**Международные** ICANN	**Региональные** Региональные Интернет-реестры	**Национальные** Национальные реестры DNS
	·	· Включает - IAB - IRTF - IESG	- IANA	- AfrlNIC - APNIC - RIPE NCC - LACNIC - ARIN	· КЦ (Россия) ·DENIC (Германия) ·AUDA (Австралия)

Мы не пытаемся показать здесь, как управление Интернетом структурировано в полном объеме, - скорее, концентрируем внимание на аспекте администрирования, который является наиболее релевантным для данного исследования, а именно на системе регистрации данных права использования как на доменные имена, так и на блоки IP-адресов.

В рамках настоящего исследования интерес представляют следующие участники процесса:

- ICANN;
- Реестры и регистраторы DNS;
- Реестры IP адресов.

Корпорация по присвоению имен и номеров в Интернете (ICANN) - образованная в 1998 году некоммерческая организация, которая отвечает за широкий спектр задач, изначально подпадавших под мандат Правительства США. Среди прочего, она отвечает за координацию и делегирование распределения и управления ресурсами Интернета и DNS-администрирование, выполняя по контракту с Министерством торговли США функции IANA, по администрированию корневой зоны DNS и распределению IP-адресов.

Администрирование системы доменных имен

ICANN делегирует администрирование общих доменов верхнего уровня (т.е. суффиксы домена без конкретного кода страны, например .com, .net, .info и т.д.) сторонним организациям (реестрам) сохраняя контроль за их деятельностью. В свою очередь реестр позволяет коммерческим компаниям предлагать услуги регистрации доменных имен физическим лицам или организациям, желающим обеспечить доменное имя. Эти компании известны как регистраторы.

Национальные домены верхнего уровня (ccTLD-домены), такие как «.ru» или «.рф», находятся в ведении национальных независимых реестров. Так Координационный Центр Национального Домена Интернет (КЦ НДИ) является оператором реестров Российской Федерации, ответственным за администрирование доменов «.ru» и «.рф». КЦ НДИ является некоммерческой организацией, финансируемой за счет регистрационных сборов за услуги регистрации доменов второго уровня в указанных национальных доменах.

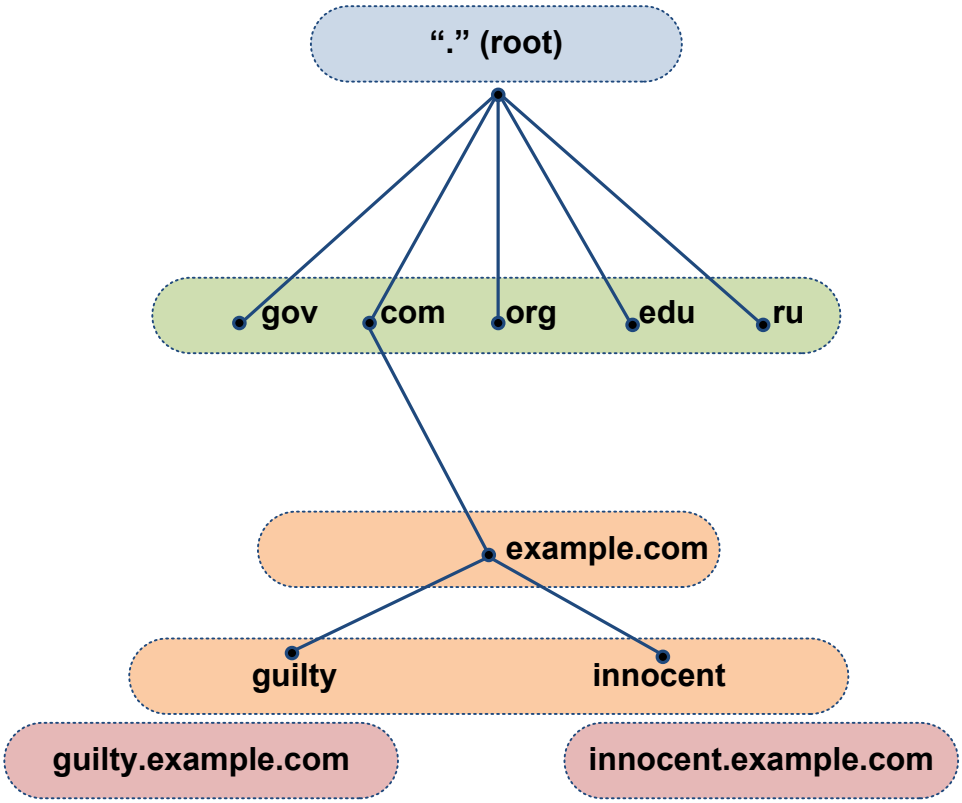


Рисунок 2.2.2 Схема регистрации доменных имен

Когда физическое лицо или компания покупает доменное имя у регистратора, их просят заполнить контактные данные по домену, включая электронную почту и почтовый адрес. Эти данные затем вносятся в базу данных реестра и они находятся в публичном доступе через сервис WHOIS DNS. WHOIS DNS – это сервис, предоставляемый реестром по протоколу WHOIS, который делает возможным запросы к базе данных доменных имен, чтобы можно было установить право «собственности» на конкретный домен.

Существуют проблемы, связанные с надежной идентификацией владельцев отдельных сайтов, что затрудняет процесс идентификации и увязке доменного имени с личностью владельца сайта.

В частности, не следует ожидать точности предоставления контактных данных администратора домена через сервер WHOIS, (например, по сравнению с адресом биллинга - выставления счетов по кредитной карте). Кроме того, реестры позволяют частным лицам отказаться от отображения полной контактной информации, если сайт или сервис используется для

некоммерческих целей (например, сайты для хобби). Если лицо приняло решение о сохранении “анонимности”, запрос в базы данных реестра относительно контактных данных о праве собственности выдает только условный идентификатор администратора домена. Еще более усложняет проблему то, что некоторые администраторы доменов и регистраторы доменных имен используют прокси-сервисы, которые хранят данные администратора домена, предоставляя общий контакт для депонирования запросов к администратору домена или сервиса передачи сообщений.

На рисунке 2.2.3 ниже приведен пример ответа на WHOIS-запрос для домена zniis.ru.

```
% By submitting a query to NETFOX Whois Service
% you agree to abide by the following terms of use:
% http://netfox.ru/whois/conditions/

domain:         ZNIIS.RU
nserver:        dns1.zenon.net.
nserver:        dns2.zenon.net.
state:          REGISTERED, DELEGATED, UNVERIFIED
org:            Central Science Research Telecommunication
Institute
registrar:      NAUNET-REG-RIPN
admin-contact: https://client.naunet.ru/c/whoiscontact
created:        1998.08.05
paid-till:      2013.09.01
free-date:      2013.10.02
source:         TCI

Last updated on 2013.03.13 16:21:37 MSK
```

Рис. 2.2.3. Результат WHOIS-запроса для домена zniis.ru

Распределение ресурсов Интернета

Там, где трудно идентифицировать администратора домена по базе данных WHOIS DNS, может оказаться возможным, по крайней мере, определить поставщика услуг хостинга, которому были выделены конкретные IP-адреса. В то время как доменные имена распределяются

реестрами DNS, другие Интернет-ресурсы, такие, как блоки IP-адресов, находятся в ведении пяти региональных реестров:

- AfriNIC – Африканский;
- APNIC – Азия и Тихий океан;
- ARIN – Северная Америка;
- LACNIC – Латинская Америка;
- RIPE NCC – Европа и Ближний Восток.

Эти пять региональных реестров для Интернет-ресурсов поддерживают базы регистрационных данных с возможностью поиска для информации об IP-адресах и сетевой маршрутизации с доступом через протокол WHOIS. Иногда этот сервис для простоты тоже называют WHOIS. В то время как DNS-реестры содержат информацию о владельцах доменных имен, реестры Интернет-ресурсов предоставляют контактную информацию о владельце сети/операторе.

2.3 Основные принципы архитектуры Интернета

Для понимания последствий применения разных стратегий блокирования важно представлять себе основные принципы, которые легли в основу архитектуры Интернета. Хотя в основном эта область уже хорошо описана, данный раздел посвящен четырем основным архитектурным принципам, которые имеют прямое влияние на результативность блокирования контента: возможности сквозного соединения и обеспечения “прозрачности”, иерархичности, распределенности и мобильности, локальности и автономности.

2.3.1 Сквозное подключение и “прозрачность”

Принцип сквозного подключения является «основным архитектурным принципом Интернета» [RFC3724]. Соблюдение принципа наделения точек подключения функциональностью для выполнения «сквозных» задач приводит к созданию «прозрачной» сети, в которой пакеты не фильтруются и не изменяются при передаче по маршруту [RFC2775]. Эта прозрачность, в свою очередь, является одним из ключевых требований для обеспечения сквозной связности элементов сети. Современные механизмы безопасности, которые полагаются на доверенные хосты, связывающиеся между собой по защищенным каналам без промежуточного вмешательства, позволяют сетям поддерживать электронную коммерцию, конфиденциальную связь, и множество других подобных услуг.

Принцип сквозного подключения является фундаментальным для безопасности в Интернете, и основой, на которой построены протоколы безопасности в Интернете. Такие протоколы, как TLS и IPsec [RFC5246] [RFC4301], были разработаны так, что каждая из сторон гарантированно идентифицировала другую, а доступ к защищенному содержанию соединения имели только участники данного соединения. Например, когда пользователь подключается к вебсайту банка, TLS гарантирует, что

финансовые данные пользователя передаются именно в банк и никуда больше.

Для некоторых стратегий блокирования требуются посредники, внедряющиеся на маршруте в сквозную коммуникацию (сетевые системы веб-фильтрации), что может нарушать безопасность интернет-протоколов. В таких случаях в точках подключения будет сложно или невозможно отличить внедрение хакеров от лиц, осуществляющих блокирование.

2.3.2. Иерархичность

Интернет-приложения построены из набора слабо связанных компонент различных «уровней». Эти уровни выполняют разные функции, например, маршрутизации, транспорта и именования (см. [RFC1122], раздел 1.1.3). Функции этих уровней развивались независимо друг от друга, практически всегда ими пользуются различные субъекты сети. Например, во многих сетях физический уровень связи и канал предоставляет «провайдер доступа», а IP-маршрутизацию осуществляет «провайдер интернет-услуг». Услуги на уровне приложений могут предоставляться совершенно другим юридическим лицом (например, владельцем веб-сервера). Протоколам верхнего уровня и приложениям для работы необходима вся совокупность функций более низкого уровня. Многочисленные специализированные приложения верхнего уровня могут использовать одни и те же базовые сетевые функции.

Результатом такой структуры является то, что действия, предпринятые на одном из нижних уровней, могут повлиять на функциональность или приложения более высоких уровней. Например, вмешательство в функции маршрутизации или DNS с целью ограничения доступа к ограниченному набору ресурсов с помощью отдельных приложений наверняка повлияет на все приложения, которые зависят от этих функций.

2.3.3 Распределенность и мобильность

Интернет построен как географически и топологически распределенная система. Ресурсы могут быть доступны из любой точки мира независимо от физического места нахождения или оператора доступа. Ресурсы также очень мобильны – их очень легко переместить с одного физического или логического адреса на другой.

Эта распределенность и мобильность лежит в основе отказоустойчивости Интернета. Маршрутизация в Интернете устойчива к серьезным авариям - таким, как разрывы подводных оптических кабелей, так как распределенная система маршрутизации Интернета позволяет отдельным сетям быстро перенаправить трафик по альтернативным маршрутам. Службы приложений, как правило, защищены от отказов при помощи распределенных серверов.

Нежелательные коммуникации также выигрывают от этой надежности - ресурсы, запрещенные или блокированные в одной части Интернета, могут быть воссозданы в другой[Dagon]. Если вебсайту запрещено использовать доменное имя или некоторые IP адреса, он может легко перейти на другое доменное имя или в другую сеть.

Распределенный и мобильный характер интернет-ресурсов ограничивает эффективность акций по блокированию. Доступ к интернет-сервису возможен из любого места в Интернете; сервис, который заблокирован в одной стране, часто может быть перемещен или восстановлен в другой юрисдикции. Кроме того, услуги, которые зависят от заблокированных ресурсов, часто можно быстро перенастроить на использование незаблокированных ресурсов. Например, часто отправители спама используют адреса в различных сетях в для отправки спама. Такой подход широко используется для распределения источников спам-рассылки по различным ресурсам и разным юрисдикциям для предотвращения эффективного блокирования спама. Кроме того, пользователи для получения требуемой услуги могут использовать различные типы протоколов. В случае

попытки блокировании голосовой связи на базе SIP [RFC3261], пользователи, скорее всего, воспользуются защищенными протоколами, которые позволят им общаться друг с другом. Таким образом, распределенность и мобильность могут свести к нулю усилия по блокированию коммуникаций.

2.3.4. Локальность и автономность

Базовым элементом маршрутизации в Интернете является «автономная система» - сеть, управляющая своей маршрутизацией. Концепция автономности широко используется в дизайне Интернета, как и родственная ей идея принципа локальности, в соответствии с которой «Автономная система» - сеть, управляющая своей маршрутизацией самостоятельно и независимо от других сетей. (Автономная система может включать в себя конкретного оператора сети или географическую местность).

Эти идеи играют важную роль в обеспечении стабильности, масштабируемости и способности к инновациям в Интернете. Если бы каждое изменение, производимое миллионами администраторов в различных сетях, оказывало бы влияние на весь Интернет, в нем воцарился бы хаос.

В контексте проблемы блокирования принцип локальности означает, что результат технических изменений, при помощи которых будет осуществляться блокирование, может работать только в пределах ограниченной области. Например, в случае изменений в сети доступа оно затрагивает только относительно небольшое, определенное количество пользователей, подсоединенных к этой сети, но при этом может также повлиять и на все приложения используемые этими пользователями. В свою очередь, изменения в конкретном сервисе приложений могут повлиять на пользователей в масштабах всего Интернета, но только для случая использования данного приложения. Таким образом, в одном случае последствия могут быть ограниченными (группа пользователей или набор приложений), а в другом – иметь эффект в масштабах всего Интернета. В некоторых случаях приложения и/или услуги инфраструктуры настолько

переплетены друг с другом, что фильтрация одного сервиса или в одной точке сети может породить глобальные последствия в разных местах и для разных приложений.

Действия по блокированию, как правило, изначально направлены на применение их в определённой зоне, но часто приводят к блокированию за ее пределами. Так, например, активация систем веб-фильтрации в Индии и Китае стали причиной блокирования вебсайтов в Германии и Корее для пользователей в Омане и США[Citizen][SIGCOMM].

3. Модели и технологии блокирования ресурсов Интернет

Вообще говоря, в типовой сквозной интернет-коммуникации участвуют три вида сущностей, каждая из которых имеет различные возможности для блокирования коммуникаций. Так, конечный пользователь инициирует соединение с другим конечным пользователем или оператором сервисов приложений на другом конце сети. В этих точках подключения системы аутентификации и репутационные системы дают возможность устройствам и их пользователям принимать решения о блокировании тех или иных соединений.

Конечные точки, в свою очередь, связаны через ряд сетей, операторы которых также могут выполнять функцию блокирования. Средства сетевого блокирования обычно включают в себя промежуточные устройства в сети для анализа трафика и принятия решения о блокировании.

И, наконец, сам транспорт и коммуникации зависят от общих «инфраструктурных» сервисов, которые глобально поддерживают множество различных приложений. Среди них система доменных имен, инфраструктура маршрутизации, и поддерживающих их информационных сервисов - таких, как реестры адресации. Операторы этих услуг могут блокировать соединения, изменяя информацию, которую они хранят в своих соответствующих базах данных или предоставляют конечным точкам (участникам коммуникации).

В этом разделе мы рассмотрим указанные три модели блокирования, а также их соответствие изложенным выше принципам архитектуры Интернета.

На рисунке ниже приведена упрощенная схема моделей блокирования с указанием основных инструментов и участников.

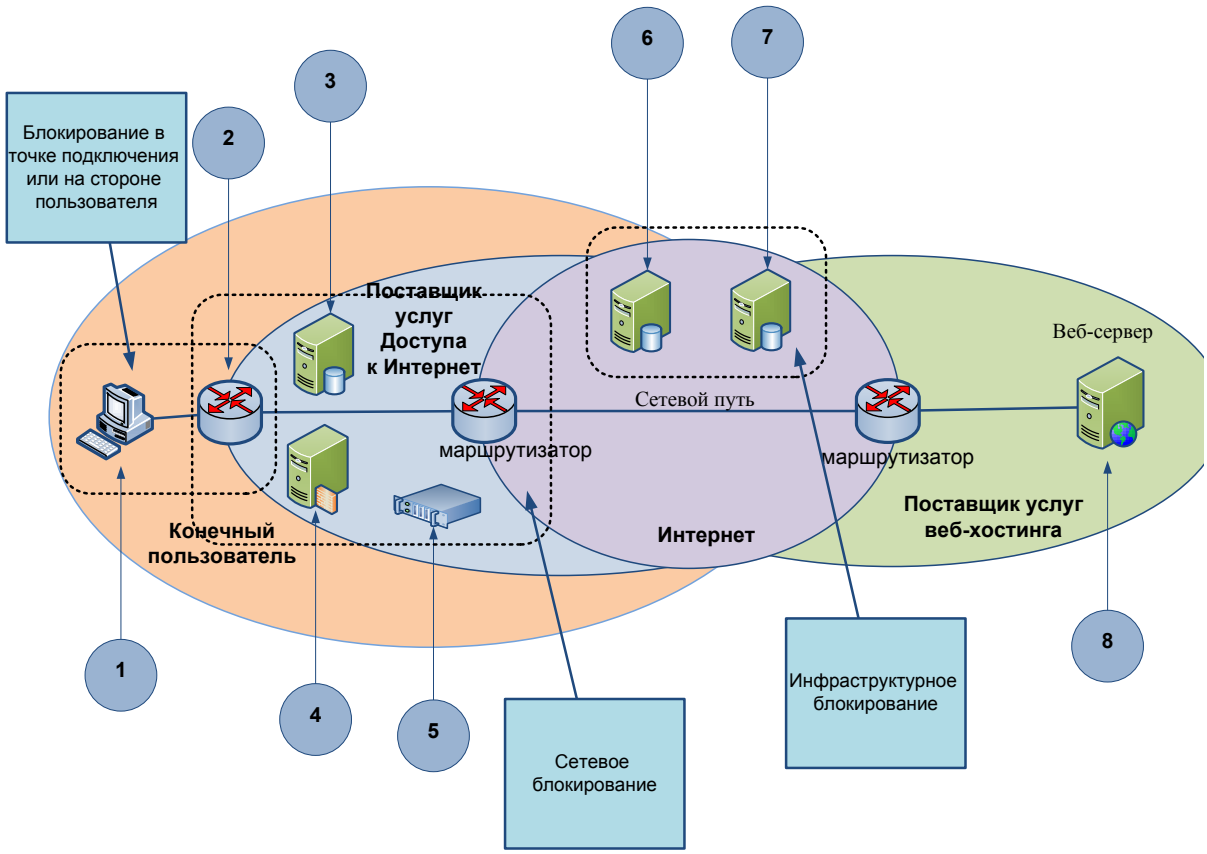


Рис. 3.1 : Блокирование. Модели.

Обозначение	Наименование
1	Веб-браузер конечного пользователя
2	Маршрутизаторы сети
3	Рекурсивный DNS-сервер
4	Прокси-серверы, управляемые Интернет провайдером
5	DPI - устройство, представляющее собой сетевое оборудование, способное провести детальный анализ незашифрованного контента сетевого трафика.
6	Реестры IP-адресов
7	Авторитативные DNS-серверы и реестры DNS
8	Веб-серверы

3.1. Сетевое блокирование

Возможность блокирования доступа к ресурсам в одностороннем порядке без согласия или взаимодействия с участниками коммуникаций как правило является обязательным требованием инициаторов создания систем блокирования. Системы с данными возможностями часто реализованы с использованием промежуточных устройств в сети, таких как брандмауэры или фильтрующие системы. Эти системы анализируют проходящий через сеть трафик, принимают решения на основе тех или иных параметров или содержания данной коммуникации, а затем блокируют или разрешают передачу, в зависимости от требований.

Типичными примерами сетевого блокирования являются брандмауэры и сетевые системы фильтрации веб-контента. Например, устройства веб-фильтрации, обычно анализируют HTTP запросы для определения запрашиваемого URL, сравнивают его с «черным» или «белым» списком адресов и разрешают перейти на него в том случае, если он разрешен выбранной политикой. Брандмауэры выполняют ту же функцию и для других типов трафика помимо HTTP. Некоторые системы блокирования ориентированы на конкретный трафик прикладного уровня, в то время как другие фильтруют трафик по параметрам нижних уровней (транспортного протокола и по адресам/портам источника или назначения).

В дополнение к блокированию связи по адресу назначения или источника сетевое блокирование может применяться в отношении других сервисных компонент, предоставляющих информацию, необходимую для запуска сервисных приложений и установления необходимых соединений, но непосредственно не участвующих в коммуникациях. Например, чтобы установить голосовое SIP-соединение, конечным узлам (терминалам) необходима информация о присутствии в сети и другая информация от SIP-серверов. Сетевые операторы могут блокировать использование SIP-услуг путем блокирования доступа к SIP-серверам.

Следует отметить, что эти используемые для блокирования «промежуточные» системы во многих случаях располагаются недалеко

от границы сети. Например, во многих корпоративных сетях установлены брандмауэры, которые блокируют определенные веб-сайты, как это делают и некоторые провайдеры ШПД для населения. В некоторых случаях эта фильтрация осуществляется с согласия пользователей или при взаимодействии с ними. ПК на предприятии: например, может быть настроен для работы через прокси-сервер компании, провайдер для населения может предлагать услуги "безопасного серфинга" или в почтовых клиентах пользователей может быть включена настройка фильтрации спама на почтовых серверах. Эти случаи имеют некоторые общие черты с рассматриваемыми далее по тексту сценариями блокирования в точках подключения, так как пользователь осознанно уполномочивает посредника осуществлять блокирование от своего имени. Маловероятно, что в этой ситуации он попытается обойти блокирование. С архитектурной точки зрения, однако, это может приводить к тем же проблемам, что и в случае принудительной сетевой фильтрации.

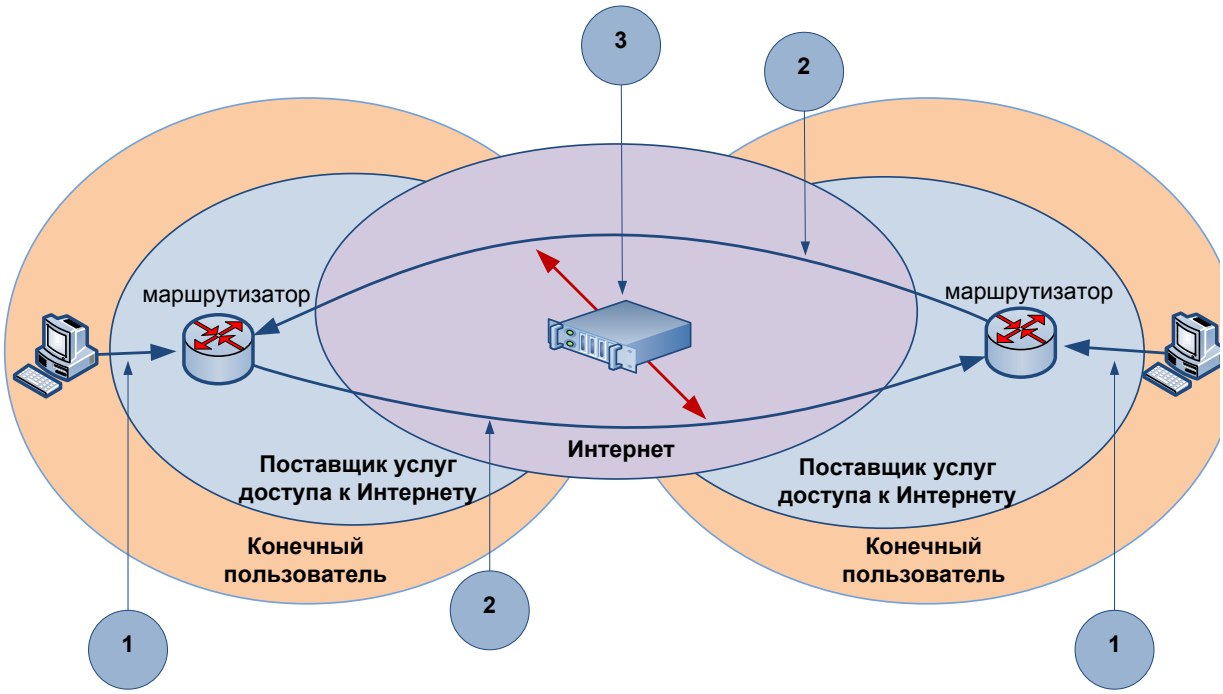


Рис. 3.1.1. Организация сетевого блокирования

Обозначение	Пояснение

Обозначение	Пояснение
1	Трафик пользователя, в том числе защищенный: кодирование (IPsec и TLS), организация VPN, туннелирование
2	Ассимметричный режим маршрутизации, при передачи трафика между конечными пользователями
3	Промежуточное фильтрующее устройство (DPI, брандмауэр), имеющее доступ ко всем маршрутам, на которых должно осуществляться блокирование трафика, а также взаимодействие с внешними ресурсами при использовании пользователями защищенных протоколов

Соответствие архитектурным принципам

Блокирование с использованием промежуточных устройств в сети вступает в конфликт с описанными выше принципами сквозного подключения и прозрачности. Сама цель блокирования в таком виде заключается в нарушении прозрачности для случаев определённого контента или соединения. Поэтому такое блокирование всегда сталкивается с рядом технических сложностей, ограничивающих его применимость на практике. В частности, множество проблем возникает в результате того, что для принятия блокирующих решений посреднику необходимо получить доступ к достаточному объему трафика.

Первая сложность в получении доступа к этому трафику заключается именно в получении доступа к соответствующим пакетам. Интернет разработан для доставки пакетов через промежуточные узлы от источника по адресу назначения, пакеты данных доставляются от источника к получателю, а не к некоторому находящемуся между ними узлу. На практике маршрутизация в Интернете часто бывает асимметричной, а для достаточно сложных локальных сетей внутрисетевой трафик также может быть асимметричным – то есть проходить в разных направлениях соединения по разным маршрутам.

Эта асимметрия означает, что промежуточному устройству часто будет доступна только половина данной соединения/коммуникации (если оно увидит ее вообще), что может ограничить его способность к эффективной фильтрации. Например, фильтр по запросам на конкретные URL-адреса не сможет принять решений по блокированию, если он размещен только на пути передачи HTTP ответов, а не запросов. Маршрутизация может быть иногда принудительно сделана симметричной в пределах конкретной сети с помощью настройки маршрутизации, NAT, или технологий 2 уровня (например, MPLS), но эти механизмы часто являются ненадежными, сложным и дорогостоящими и их использование нередко приводит к снижению производительности сети по сравнению с использованием асимметричной маршрутизации.

После того как промежуточная система получила доступ к трафику, она должна определить, какие пакеты подлежат фильтрации. Это решение обычно основывается на некоторой комбинации информации сетевого уровня (например, IP-адреса), транспортного уровня (порты), или уровня приложений (URL или другой контент). Блокирование с использованием атрибутов прикладного уровня потенциально может быть более детальным и имеет меньше шансов вызвать побочный ущерб, чем блокирование всего трафика по определенному адресу, которое может повлиять на не имеющие к этому отношения сервисы, использующие тот же адрес.

Обход блокирования

Независимо от уровня, на котором происходит блокирование, оно может быть обойдено, особенно в тех случаях, когда участники коммуникации не заинтересованы в блокировании и не давали на него разрешения. Соединение может быть закрыто и защищено от вмешательства промежуточных систем на любом уровне с использованием защиты (шифрования - см. ниже). IP-адреса могут быть видны, даже если пакет защищен IPsec, но блокирование на основе IP-адресов является простейшей

формой фильтрации, которую легко обойти. Фильтруемые сайты, могут быстро изменить свой IP-адрес, используя простейший алгоритм: изменение одной записи DNS и назначение нового адреса серверу или просто перемещение своих услуг на новый адрес. Так в условиях блокирования по IP в некоторых сетях, такие сервисы, как The Pirate Bay, теперь используют «облака» для хостинга, и промежуточным системам стало трудно выявлять их IP-адреса. [BT] [TPB].

Если содержимое приложения защищено с помощью протоколов безопасности - таких, как IPsec и TLS, - то промежуточной системе потребуется расшифровка пакетов для изучения содержимого приложения. Так как защищенные протоколы предназначены для обеспечения сквозной безопасности (для предотвращения перехвата содержимого), такая система может пытаться маскироваться под один из концов соединения, взломав аутентификацию в протоколе безопасности, при этом снижая безопасность пользователей и сервисов и вмешиваясь в законные частные коммуникации. Кроме того, различные методы, например, общедоступные базы данных с «белыми» списками ключей, позволяют пользователям обнаруживать системы этого типа. Пользователи затем вероятно будут относиться к данной услуге как заблокированной и использовать пути обхода.

Если посредник не в состоянии расшифровать защищенный протокол, то решение о блокировании защищенных сессий может быть принято лишь на основе таких незащищенных атрибутов, как IP-адрес, идентификатор протокола и номера портов. Некоторые системы блокирования сегодня все еще пытаются осуществлять блокирование, основываясь на этих атрибутах, например, блокируют TLS-трафик на известные прокси-серверы, которые могут использоваться как туннели через блокирующую систему.

Однако для защищенного трафика в большинстве ситуаций затруднительно будет отличить легитимный трафик, например, к банковской системе от доступа к блокируемым ресурсам.

Таким образом, в принципе невозможно заблокировать конкретный туннелированный трафик на промежуточной системе (за исключением случаев установки специального программного обеспечения у клиента), не блокируя весь защищенный трафик.

В большинстве случаев блокирование всего защищенного трафика является неприемлемым, так как обеспечение безопасности необходимо для многих систем - таких как электронная коммерция, промышленные VPN и управление критической инфраструктурой. Если для более эффективного блокирования правительство или сетевые операторы попытаются заставить пользователей использовать незащищенные протоколы для этих услуг, они подвергнут их риску различных атак, от которых должны защищать эти протоколы безопасности.

Следует отметить, что может быть достаточно и блокирования доступа к ресурсам только через незащищенные каналы – исходя из того, что пользовательская база, которая будет использовать защищенные туннели и/или специальное программное обеспечение для обхода блокирования, в настоящее время может считаться незначительной. В такой ситуации можно отказаться от попыток контроля защищенного трафика. Тогда применение отдельных технологий сетевого блокирования может быть признано целесообразным.

Но, чем дольше используются сетевые системы блокирования, тем больше появляется эффективных и простых в использовании систем туннелирования. Распространение сети Tor, например, и применяемые в ней все более сложные методы обхода блокирования демонстрируют потенциал данного направления [TOR]. Таким образом, малоэффективное и сейчас, сетевое блокирование со временем будет становиться все менее эффективным.

Сетевое блокирование является ключевым фактором в “гонке вооружений”, которая привела к развитию этих видов инструментов и технологических решений, результатом которого стало создание ненужных,

избыточных уровней сложности в Интернете. В период до широкого распространения блокирования контента для сетевых операторов предпочтительным вариантом оставалось блокирование по портам, широкое использование которого заставило перейти многие приложения и услуги на использование портов (в первую очередь, 80), которые вряд ли могут быть заблокированы. В свою очередь, операторы сетей перешли на более детальный анализ содержимого трафика через порт 80. Контент-провайдеры в свою очередь перешли на защищенные каналы, и операторы занялись выявлением этих каналов. Сетевое блокирование неизбежно стимулирует поиски его обхода со стороны участников коммуникаций, эта игра в «кошки-мышки» стала неизбежным побочным продуктом данного вида блокирования.

В целом, сетевое блокирование эффективно только при довольно ограниченных условиях:

- Во-первых, трафик должен проходить через сеть таким образом, чтобы промежуточное устройство имело доступ к любому соединению, которое оно намерено блокировать;
- Во-вторых, системе блокирования необходимы внешние ресурсы при использовании пользователями защищенных протоколов (например, аналитиков для определения IP-адреса конечных точек туннеля), что может оказаться высокозатратным, особенно, если точки терминации туннеля начинают часто меняться.

Если сеть достаточно сложна или вероятность использования туннелирования высока, то сетевое блокирование не будет эффективным и в любом случае этот тип блокирования быстро приведет к развитию более сложных вариантов и технологий его обхода.

Технологии сетевого блокирования

Существует ряд технических решений, которые могут быть использованы для ограничения доступа к сайтам в Интернете. В этом разделе

рассмотрены основные методы, которые в настоящее время доступны операторам фиксированного доступа в Интернет.

К основным методам сетевого блокирования сайтов, применяемым во всем мире, относятся следующие:

- по IP-адресу;
- по DNS;
- по URL;
- с применением анализа пакетов – DPI (deep packet inspection).

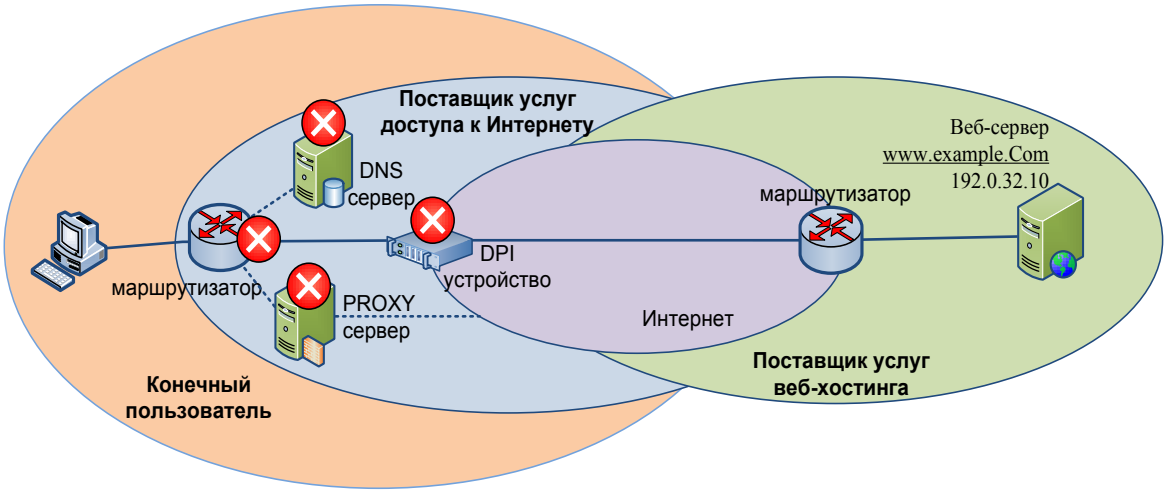


Рисунок 3.1.2: Возможные места применения различных методов сетевого блокирования ресурсов

Обозначение	Пояснение
	Блокирование с помощью выделенного устройства или путем изменения существующей системы
	Прокси-сервер, под управлением Интернет провайдера
	Устройство Интернет провайдера, для анализа пакетов

Представляется, что приведенный список сетевых подходов к блокированию сайтов на данный момент носит исчерпывающий характер и никаких других альтернативных подходов не предлагается.

При анализе методов блокирования мы оценим влияние каждого на общие эксплуатационные расходы на управление и уровень технической сложности реализации для интернет-провайдеров.

В данном разделе также анализируется, степень легкости, с которой как пользователи, так и операторы заблокированного сайта могут обойти блокирование сайта и какие контрмеры поставщик услуг Интернета может предпринять для снижения вероятности или прекращения практики использования таких обходов.

3.1.1 Блокирование по IP-адресам

Описание решения

Основу Интернета составляет набор сетевых технологий, основанных на Интернет-протоколе (IP), который является стандартизированным форматом для передачи данных через Интернет. В наиболее широко используемой версии IP, IP-версии 4 (IPv4), адрес отображается в виде четырех чисел, разделенных точкой, его иногда называют адресом с точками-разделителями. Например, веб-сайт zniis.ru имеет общедоступный IP-адрес 213.189.197.12.

IP позволяет передавать данные с компьютеров по всему миру в виде пакетов. IP-пакет содержит IP-адрес источника и IP-адрес назначения, а также полезную нагрузку/данные. Каждый отдельный пакет может использовать различный маршрут к адресу назначения. Устройство-адресат в состоянии восстановить оригинальные данные, основываясь на информации, содержащейся в каждом пакете, будь то сообщение по электронной почте или веб-страница. Последовательность сетей, составляющих Интернет, соединена через маршрутизаторы, которые,

используя динамические таблицы о маршрутах для сетей, доступных в Интернете, передают каждый из пакетов по назначению.

Маршрутизаторы могут быть настроены для отправки IP-пакетов, предназначенных для указанного IP-адреса назначения, по несуществующим или пустым (NULL) маршрутам, блокируя, таким образом, доступ к конечному сайту. Аналогичным образом весь диапазон адресов той или иной сети может быть заблокирован путем назначения «лучшего» маршрута для данной сети, а также путем направления пакетов по NULL-маршрутам.[1]

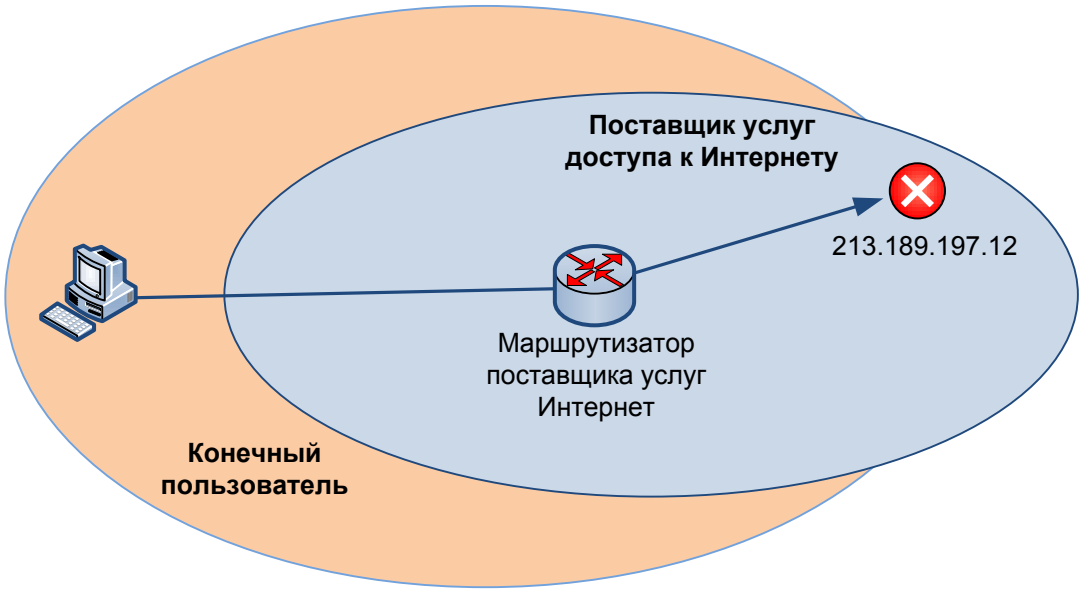


Рис. 3.1.1.1 Блокирование IP-адресов на маршрутизаторах

Эффективность блокирования и сложность обхода.

Обход блокирования IP-адресов технически прост.

Оператор заблокированного сайта может:

- изменить IP-адрес, но остаться в той же сети (например, на том же хостинг-провайдере);
- перейти на новую сеть (на ранее незафиксированный IP-адрес);

[1] Другие сетевые устройства - такие, как оборудование управления/формирования трафика и устройства

- предложить защищенные услуги доступа, которые скрывают истинный сетевой адрес/назначение, например, доступ через виртуальные частные сети (VPN);
- операторы сервера могут использовать разновидности DNS-техники типа Fast Flux {HONEY] (быстрые и частые переходы на новые адреса - затрудняющие выявление истинного сетевого адреса блокируемого сайта).

У операторов сайтов есть и другие способы. При переходе на новый IP-адрес оператор сайта может зарегистрировать несколько IP-адресов для данного сайта для поддержания сервиса в том случае, если некоторые из этих отдельных IP-адресов будут заблокированы. Этот подход также часто используется и в легальных целях.[2] Кроме того, устанавливая низкое значение «времени существования» (TTL – time to live) в системе доменных имен (DNS), определяющее продолжительность времени, в течение которого IP-адрес для конкретного домена остается в кэше серверов имен (выражается в секундах), оператор сайта может с большей легкостью заменять IP-адреса сайта без потери доступа для конечных пользователей. Когда установлен низкий TTL, кэши серверов DNS интернет-оператора быстро очищаются, предоставляя обновленные IP-адреса сайта от авторитативного сервера имен и сохраняя доступность сайта.

Пользователи Интернета могут использовать также анонимные прокси-серверы (серверы-посредники между конечным пользователем и оператором сайта) или другие службы-анонимайзеры; в этом случае интернет-оператор и не знает, что конечный пользователь пытается получить доступ к заблокированному сайту.

Технические ответные меры Интернет провайдеров на обход клиентом блокирования сайта

[2] Для повышения доступности сервисов операторы сайтов часто используют несколько IP-адресов.

Если применяемые средства обхода не используют шифрования, оператор доступа в Интернет для повышения эффективности блокирования IP-адреса может проанализировать IP-пакеты. Например, можно проверять весь трафик, предназначенный для незащищенных веб-прокси, и заблокировать любой трафик, который соответствует набору заданных правил или конкретной сигнатуре пакетов. Когда пакет, соответствующий IP-адресу заблокированного сайта, или содержащий определенное ключевое слово, проходит через устройство анализа пакетов (не обязательно DPI), оно может сравнить содержимое заголовка пакета и IP-адреса источника и назначения и сетевое соединение может быть разорвано.

Блокирование с использованием методов DPI будет рассмотрено ниже.

Последствия блокирования для пользователей, провайдеров Интернета

Блокирование по IP-адресам является очень грубым методом блокирования Интернет-сайтов. В ситуации хронической нехватки IPv4-адресов и необходимости оптимизации использования этого ограниченного ресурса для повышения эффективности бизнеса веб-хостинга, хостинговые компании размещают по несколько сайтов на общем оборудовании, которые имеют один общий IPv4-адрес. В результате блокирование одного IP-адреса может приводить к блокированию доступа к нескольким сотням сайтов (непреднамеренное блокирование). Только хостинг-провайдеру известно, сколько веб-сайтов в конкретный момент времени используют данный IP-адрес.

Оценки масштабов совместного использования IP-адреса веб-сайтами варьируются. Согласно некоторым оценкам в доменных зонах COM, NET и ORG 80-90% веб-сайтов имеют общий IP-адрес. Совместное использование IP-адресов является общепринятой практикой для хостинга веб-сайтов. Типичное число сайтов, совместно использующих один IP-адрес в системах виртуального хостинга, в настоящее время колеблется от нескольких

десятков до полутора тысяч. Некоторые нелегальные сайты могут быть размещены и на выделенном оборудовании или монопольно использовать один IP-адрес, но это нетипично.

Таким образом, при организации блокирования единичного ресурса по IP-адресу практически будет заблокировано как минимум несколько сотен(!) полностью легитимных сайтов.

Оценка затрат, масштабируемость и влияние на производительность сети

Для операторов Интернета есть проблемы и с администрированием блокирования по IP-адресам на маршрутизаторах. Среди них:

- снижение производительности маршрутизатора, связанное с ростом размера списков заблокированных IP-адресов сайтов;
- технические ограничения на максимальный размер списков;
- продолжительность постановления о блокировании и требование поддерживать эти списки на оборудовании маршрутизации;
- возрастание вероятности ошибок при изменениях в списках;
- невозможность точно спланировать расходы, поскольку количество сайтов, которые могут быть заблокированы, неизвестно заранее.

Блокирование по IP-адресам требует дополнительных инвестиций в сетевое аппаратное обеспечение и ведет к росту эксплуатационных накладных расходов, в том числе, росту численности персонала. Если игнорировать данный экономический фактор и темпы роста трафика в Интернет, то теоретически это решаемые вопросы, и формально сами по себе они не являются непреодолимым препятствием для использования блокирования IP-адресов.

Применение блокирования по IP может происходить в рамках заранее запланированных работ по изменениям в системе управления сетью. Различные режимы управления изменениями интернет-провайдерами могут приводить к блокированию сайта в разное время и через различные

промежутки времени после поступления запросов на блокирование у различных операторов Интернета.

Соответствие архитектуре Интернета

Как указывалось выше, интернет-провайдеры, как правило, приобретают услуги доступа и транзита у оптовых поставщиков более высокого уровня. Могут возникать ситуации, когда интернет-провайдеры заинтересованы в получении от вышестоящего оператора услуг блокирования. С другой стороны, следует учитывать трансграничный характер Интернета, когда блокирование на магистральной сети оператора приводит к блокированию доступа за пределами национальной юрисдикции. Такое уже происходило в Пакистане, Китае и происходит в России. В случае России избыточное блокирование в Ростелекоме и Вымпелкоме сказалось на операторах Армении, Азербайджана, Белоруссии, Украины и ряда других стран, что следует рассматривать как недопустимое последствие.

Хотя эти оперативные вопросы и не являются неразрешимыми, они дают представление о сложностях, возникающих в процессе реализации кажущегося простым блокирования по IP-адресам.

3.1.2 Блокирование с помощью DNS

Описание решения

Распределенный характер DNS и ее ключевая роль в доступе к Интернет-хостам на первый взгляд делают ее очевидным кандидатом для использования при блокировании сайтов. Интернет оператор может выполнять блокирование через серверы имен DNS поставщика с помощью следующих методов:

- жестко прописать доступ к указанному IP-адресу или к специальному «локальному» адресу 127.0.0.1;

- настроить сервер DNS так, чтобы он отказывался выполнять запрос;
- настроить сервер DNS так, чтобы в ответ на запрос выдавалась информация, что домен не существует (ответ NXDOMAIN).

На рисунке 3.1.2.1 показано, как DNS-блокирование работает на практике.

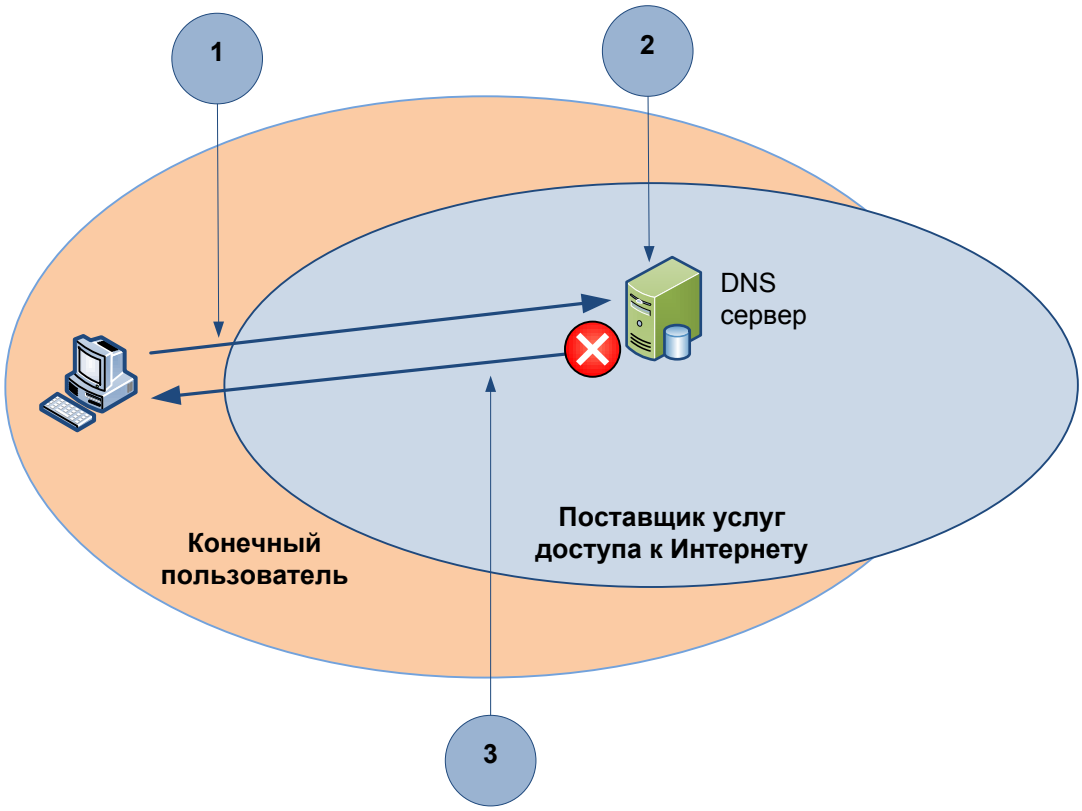


Рис. 3.1.2.1 DNS-блокирование

Обозначение	Пояснение
1	Какой IP-адрес для www.example.com?
2	DNS-сервер поставщика услуг доступа к Интернет
3	www.example.com не существует

Эффективность блокирования и сложность обхода

Обойти DNS-блокирования так же, как и другие методы блокирования, относительно легко:

- заблокированный сайт может предложить такие сервисы, как доступ через виртуальные частные сети, защищенные от доступа третьих лиц (преобразование имен DNS будет происходить в сети VPN-оператора в обход DNS-блокирования сайта у основного интернет-провайдера);
- конечный пользователь может настроить свой резолвер по умолчанию на сервер DNS третьего лица;
- пользователи могут использовать анонимные прокси-серверы или другие услуги-анонимайзеры, которые не зависят от DNS-серверов интернет-провайдера;
- преобразование имен может быть выполнено локально путем добавления записи в хост-файл (информация о преобразовании IP-адреса может быть получена с веб-сайтов, поддерживающих сетевой эквивалент команды «nslookup»).

Для конечных пользователей, которые хотят обойти блокирование, есть несколько вариантов. Например, существует много альтернативных, в том числе коммерческих, DNS-провайдеров сервисов DNS, например, Google DNS, Verisign, Neustar. Перенастройка DNS на альтернативных поставщиков не требует особой технической подготовки, так как сервис-провайдеры предоставляют четкие инструкции, используя доступный для неподготовленного пользователя язык.

Доступ к сайту можно получить даже при ограниченном знании интернет-технологий, введя IP-адрес сайта (если несколько веб-сайтов размещены на том же IP-адресе, у пользователя будет отображаться по умолчанию веб-сайт или страница данного веб-сервера). Операторы сайтов могут предоставлять информацию об альтернативных онлайн-источниках преобразования имен DNS через рассылку по электронной почте или на интернет-форумах.

Среди других каналов, которые операторы сайтов могут использовать для широкого распространения информации о том, как обойти DNS-блокирование следует указать такие, как: размещение ее на интернет-форумах, каналы рассылки новостей обновлений сайтов (RSS) или обновления через сайты микроблогов - таких как Twitter. Рекомендации могут включать как предложения настроить резолвер на сервер DNS с исходной информацией, так и использовать виртуальные частные сети, прокси-серверы или другие системы-анонимайзеры.

Кроме того, операторы сайтов могут быстро создать зеркала (копии) заблокированного сайта в другом домене высшего уровня или страновом домене, указав новые IP-адреса, например, www.blockedsite.cc; www.blockedsite.ru; www.blockedsite.vn; www.blockedsite.net.

Технические ответные меры поставщиков услуг Интернета на обход блокирования

Для предотвращения запросов к другим операторам DNS интернет-провайдеры могут использовать такие меры, как блокирование DNS-запросов к сторонним серверам DNS. Этот подход требует использования анализа заголовков IP-пакетов и является разновидностью фильтрации по содержимому IP-пакетов.

К нежелательным побочным эффектам блокирования стороннего DNS-трафика следует отнести то, что будут заблокированы провайдеры легальных DNS-услуг для третьих лиц (некоторые из которых фильтруют запросы по категориям, например, для взрослых, азартные игры и т.д., для родительского контроля или осуществляют фильтрацию для корпоративных сетей, осуществляют защиту DNS) или компании, которые имеют свои собственные DNS-сервисы.

Если пользователь использует предоставленный провайдером маршрутизатор, технически возможно «заблокировать» настройки IP-адреса сервера имен DNS в маршрутизаторе, чтобы не допустить запросы к

сторонним серверам DNS. Это требует соответствующих изменений в договорах с пользователями и исключение использования сторонних поставщиков DNS, в том числе и для защиты DNS. Неизвестно, сколько сервис-провайдеров и конечных пользователей могут затронуть подобные меры. Количество абонентов с собственными маршрутизаторами, подключенными к сети провайдера Интернета, также неизвестно, но в России таких большинство, и стороннее ограничение или блокирование конфигурации маршрутизатора пользователя, в России практически нереализуемо.

Последствия блокирования для пользователей, провайдеров Интернета

DNS-блокирование выполняется на уровне запрещенного домена. В этом случае также будут заблокированы все сервисы, работающие в данной доменной зоне и использующие поддомены данного домена. Сам факт запрета доступа ко всем сервисам в доменной зоне не создает технических проблем, однако следует учитывать, что могут существовать и легальные сервисы, которые предоставляются в пределах той же зоны , что и запрещенные сервисы. Так блокирование, осуществленное в отношении домена «example.com», заблокирует как «guilty.example.com», который является целевым сайтом, так и «innocent.example.com», который не является предполагаемым объектом блокировки.

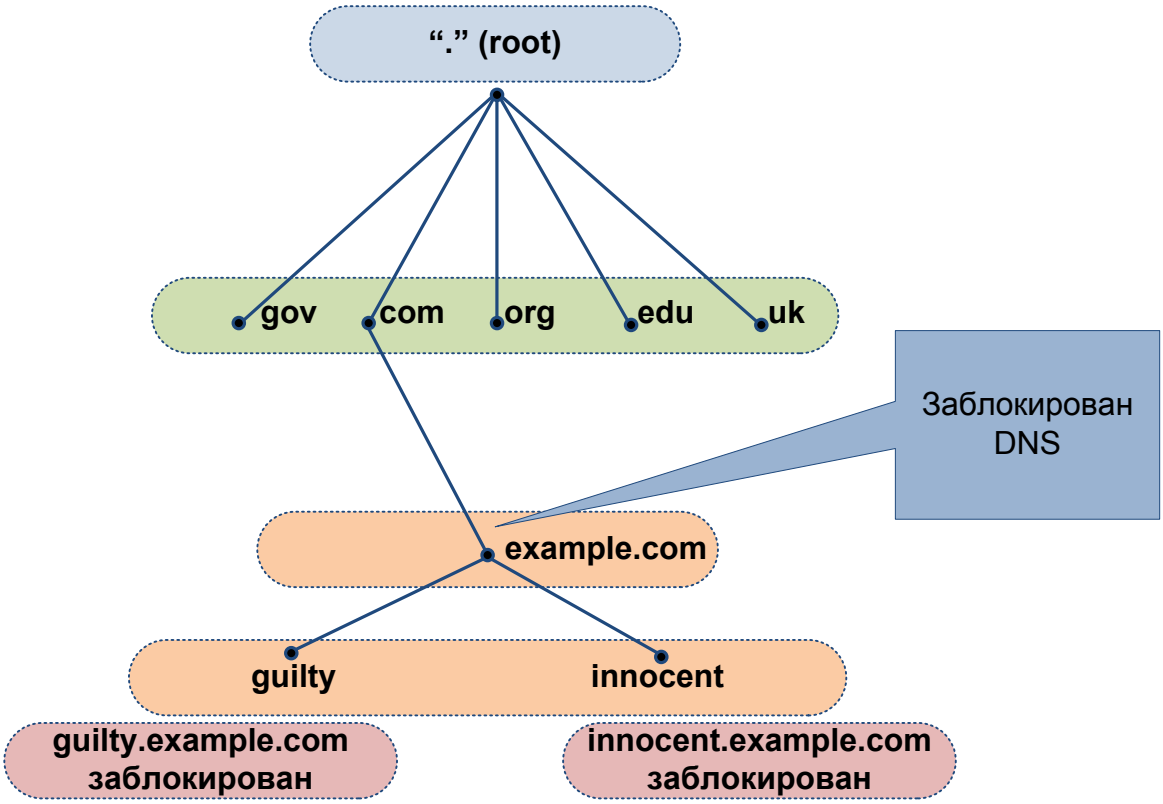


Рис. 3.1.2.2 Иллюстрация риска чрезмерного DNS-блокирования

Оценка затрат, масштабируемость и влияние на производительность сети

Расходы при применении DNS-блокирования в настоящее время не являются значительными и будут нарастать постепенно. Также существуют коммерческие решения в виде расширений к системам DNS, блокирующие вредоносные или нелегальные домены.

3.1.3 Блокирование сайтов по URL

Описание решения

Наиболее известный пример использования URL – это доступ к веб сайтам (WWW). URL может указывать на конкретный файл, каталог или сервер.

На рисунке ниже приведены примеры веб-URL по HTTPS, веб-URL веб-сервера, работающего через нестандартный сетевой порт (1491), и URL-протокола передачи файлов (FTP) с доступом через IP-адрес хоста. Есть и другие сервисы, которые используют формат URL, включая группы новостей, SIP и так далее.[3][URL]

Протокол	*FQDN*	Каталог	*Файл*
https://	*www.example.com* /	*downloads /*	*zapretinfo.zip*
Протокол	*IP адрес*	*Порт*	
http://	*192.0.43.10:2322/*		
Протокол	*IP адрес*	*Каталог*	
ftp://	*192.0.43.10 / prohibition /*		

FQDN - Fully Qualified Domain Name	Полностью квалифицированное доменное имя

Рис. 3.1.3.1: Примеры URL

[3] RFC 1738 - http://www.ietf.org/rfc/rfc1738.txt

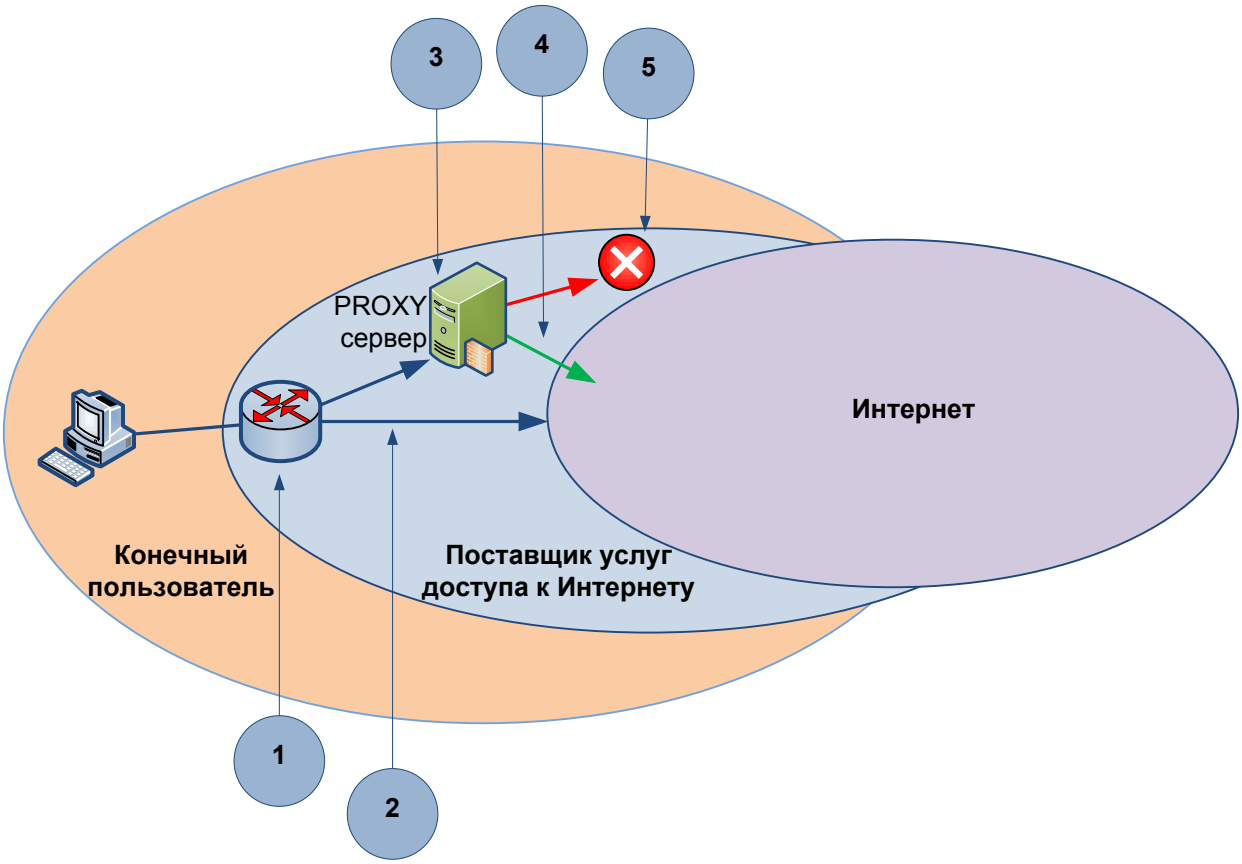


Рис. 3.1.3.2 Модель «прозрачного» прокси-блокирования с помощью URL

Обозначение	Пояснение
1	Трафик для сайта x, отделяется от остального трафика и пересылается через блокирующий прокси-сервер
2	Обычный путь следования интернет-трафика
3	Прозрачный прокси-сервер поставщика услуг Интернет, осуществляющий проверку URL на принадлежность к заблокированным значениям
4	Совпадение отсутствует, трафик пропускается
5	URL совпал, трафик блокируется

Прокси-сервер является промежуточным сервером, который обрабатывает запросы на подключение от имени запрашивающего. Прокси-серверы являются обычным явлением в школах и на предприятиях, выполняя ряд функций, включая кэширование контента, блокирование

нежелательных сайтов и предоставление элементарной защиты. До появления широкополосного доступа прокси-серверы были обычным явлением в инфраструктуре предоставления коммутируемого доступа Интернет провайдеров и весь трафик, как правило, проходил через них.

Эффективность блокирования и сложность обхода

Блокирование с помощью URL может быть осуществлено либо на уровне домена (например, www.example.com), либо для случая конкретного URL (например, http://www.example.com/files/zapret.zip). При применении на уровне домена URL-блокирование эквивалентно DNS-блокированию.

URL-блокирование ограничено, так как может блокировать только незащищённый веб-трафик (WWW). Оно не подходит для работы с контентом в группах новостей USENET или передаваемым по протоколу передачи файлов (FTP).

Факторы, которые могут значительно снизить эффективность URL-блокирования:

- Использование защищенного доступа к веб-сайтам с помощью протоколов безопасных соединений/защиты транспортного уровня, т.е. https-подключение https://www.example.com/downloads/zapretinfo.zip;
- оператор сайта может запустить доступ к веб-сайту через сетевой порт, отличный от порта 80;
- оператор сайта, может изменить IP-адрес;
- оператор сайта может организовать доступ с использованием нового доменного имени, например, www.example.net или www.example.org;
- оператор сайта может организовать доступ к заблокированному сайту по VPN;
- пользователи могут использовать анонимные прокси-серверы или других службы-анонимайзеры;

- реорганизация структуры сайта оператором, если блокирование осуществляется в отношении конкретных URL;
- оператор сайта или конечный пользователь может закодировать URL (или организовать доступ по «одноразовым» URL) для обхода блокирования.

Технические ответные меры интернет-провайдера на обход блокирования

Могут быть использованы специализированные сетевые устройства для блокирования трафика по комбинации IP/порт – такие, как брандмауэры и DPI-устройства. Но подобные методы технически легко обойти, используя VPN, анонимные прокси и другие службы-анонимайзеры.

Последствия блокирования для пользователей, провайдеров Интернета

URL-блокирование может обладать высокой степенью детализации, иметь низкий порог чрезмерного блокирования. В целом URL-блокирование эффективно только против незашифрованного веб-трафика. Блокирование другого незашифрованного трафика, содержащего такие URL, как группы новостей и FTP, теоретически возможно, однако какие-либо коммерчески доступные решения неизвестны.

Оценка затрат, масштабируемость и влияние на производительность сети

В случае комбинирования с другими методами реализацию URL-блокирования нельзя отнести к самым дорогостоящим.

Другие аспекты блокирования сайтов с помощью URL

Как указывалось выше, метод, с помощью которого осуществляется типичное блокирование через прозрачный прокси-сервер, обычно требует перенаправления трафика на сетевой прокси-сервер. Блокирование сайта с интенсивным трафиком запросов может замедлить производительность как прокси-сервера, так и того сетевого сегмента, где находится прокси-сервер..

Практический опыт URL-блокирования

Положительный опыт внедрения систем подобного типа отмечается в ряде стран мира, включая Великобританию и Новую Зеландию. Большинство поставщиков услуг Интернета в развитых странах в настоящее время действуют по схеме URL-блокирования, ограничивая доступ к материалам о жестоком обращении с детьми.

Фонд мониторинга Интернета (IWF) в Великобритании является благотворительной саморегулируемой организацией, основанной в 1996 году.4 Среди членов IWF операторы Интернета, операторы мобильной связи, поставщики программного обеспечения веб-фильтрации и провайдеры поисковых услуг. В основе работы IWF лежит деятельность по борьбе с доступом к материалам о жестоком обращении с детьми.

Одной из задач IWF является распространение среди провайдеров Интернета и операторов мобильной связи списка веб-адресов, которые содержат изображения жестокого обращения с детьми. В IWF работает горячая линия для представителей общественности, которые могут сообщить о веб-сайте, содержащем материал о жестоком обращении с детьми.

После поступления сообщения о вызвавшем подозрение URL и его проверке IWF добавляет его в существующий список URL, который

[4] Саморегулирование | Фонд по надзору за Интернетом (IWF) - http://www.iwf.org.uk/members/self-regulation

распространяется среди интернет-провайдеров и включается в их системы блокирования.

Подробная информация об используемой интернет-провайдерами технологии блокирования является конфиденциальной. Приведенное ниже описание представляет только в общем виде модель реализации указанной технологии: технология блокирования реализована в виде прозрачного прокси-сервера и зависит от изменений маршрутизации в сети. Некоторые провайдеры при ответе также отображают веб-страницу с указанием причины блокирования. Однако этот подход не является стандартом.

Схема примерного процесса URL-блокирования IWF выглядит следующим образом:

- Определяется URL, который необходимо заблокировать - http://www.example.com/downloads/zapretinfo.zip;
- URL добавляется в блокирующий прокси-сервер;
- Запрос к нежелательному сайту перенаправляется сетевым оборудованием оператора Интернета на фильтрующий прокси-сервер (Так весь трафик, предназначенный для www.example.com, перенаправляется для установления точного соответствия URL);
- Прокси-сервер производит детальную сверку данных с имеющимися образцами.
- Если найдено прямое совпадение, соединение прерывается (либо направляется на страницу с предупреждением, или просто разъединяется).
- Если запрос не совпадает с заблокированным URL, соединение будет продолжено.

3.1.4 Блокирование с помощью анализа содержимого пакетов

Описание решения

Под анализом пакетов мы понимаем изучение содержимого пакета, а не просто проверку IP-адресов источника и назначения. Проверка сетевых пакетов может быть применена на двух уровнях: «поверхностном» и «углубленном».

Поверхностную проверку пакетов можно описать, как блокирование на основе комбинации IP-адреса, порта и протокола: например, весь трафик, предназначенный для IP-адреса 192.0.32.10, TCP на порт 80 (веб-трафик), блокируется. Используя этот подход, можно сохранить доступ к другим сервисам заблокированного сайта - таким, как электронная почта или FTP.

Поверхностная проверка пакетов технологически реализуется теми же средствами, что и сетевое блокирование по IP-адресам и имеет те же недостатки, что и блокирование по IP-адресам (см. выше).

Блокирование исходящих запросов защищенного трафика на соединение по конкретному IP-адресу можно реализовать с помощью списков управления доступом маршрутизаторов (ACL). ACL – это база правил, которая может помогать блокировать или выделять трафик для данного IP-адреса с учетом использования определенного порта соединения (например, порт 443). Но обработка по ACL создает дополнительную нагрузку на процессоры маршрутизаторов, поскольку требуется сравнение каждого IP-пакета с базой правил ACL. Чтобы избежать падения производительности сети в целом, nребуется тщательное планирование производительности и ресурсов. Некоторые производители маршрутизаторов разработали специальные модификации для относительного повышения производительности ACL. Но даже в этом случае маршрутизаторы имеют существенные ограничения пропускной способности по размеру и количеству списков ACL.

Альтернативным подходом спискам ACL является использование брандмауэров с пакетной фильтрацией и устройств управления трафиком. Брандмауэры, как правило, размещаются по периметру локальной/частной сети, которая связана с Интернет. Также можно размещать брандмауэры в различных местах внутри сети интернет- провайдера и настраивать их на блокирование трафика определенного типа, т.е. по IP-адресу и сетевому порту блокируемого сайта. Это решение технологически является эквивалентным решениям с поверхностной фильтрацией пакетов и блокированию по IP-адресу и несет в себе те же недостатки.

Оборудование анализа пакетов более детально проверяет содержимое пакетов по их характеристикам или значениям. DPI-технология стала широко использоваться, в первую очередь, в системах обнаружения и предотвращения вторжений, защищающих сети и системы от вредоносной деятельности. Устройство DPI может опираться на сигнатуры, обнаружение аномалий или анализ трафика. IP-пакеты также могут фрагментироваться при прохождении через сети с различными характеристиками. В этом случае устройство DPI должно перед анализом выполнить сборку пакета из фрагментов.

Если DPI устройство обнаруживает сетевой пакет, соответствующий заранее определенным заданным свойствам, например, трафику, к заблокированному сайту, устройство DPI может ввести команду сброса, тем самым разрывая соединение, или просто выделить дальнейший трафик, предназначенный заблокированному сайту. Ошибки, неточности или неаккуратность настройки параметров оборудования DPI может приводить к блокированию законного трафика, или прохождению вредоносного трафика, или даже блокированию критических ресурсов сети.

Реализация блокирования незашифрованного трафика - технически простая задача, блокирование же зашифрованного трафика на устройствах DPI является проблематичным. Для случая зашифрованного трафика возможно только блокирование по комбинации IP-адреса/сетевого

протокола/порта, что фактически превращает устройство DPI в устройство поверхностной проверки пактов, а также приводит к чрезмерному блокированию веб-серверов, совместно использующих данный IP-адрес (избыточное блокирование распространяется в этом случае и на сайты, доступ к которым осуществляется по технологии SSL/TLS).

Эффективность блокирования и сложность обхода

Поверхностную и углубленную проверку пакетов можно обойти следующими способами:

- изменением IP-адреса, оставаясь в той же сети;
- переходом к совершенно новой сети (к ранее не наблюдавшемуся IP-адресу);
- сайт может использовать методы сетевой защиты такие как защищенные соединения или виртуальные частные сети (VPN), что делает проверку содержимого IP-пакетов или реального IP-адреса назначения невозможной;
- оператор сайта может добавлять или удалять IP-адреса сайта из пула IP-адресов.

Конечные пользователи для обхода проверки пакетов, могут использовать анонимные прокси-серверы или другие службы-анонимайзеры.

При этом следует отметить, что из всех рассмотренных в данной работе методов только DPI предоставляет возможность анализировать не только различные виды представления адреса ресурсов (IP-адреса, DNS-имена, URL) в сети Интернет, но и, при необходимости, содержание передаваемой по незащищенным каналам информации. Однако, это свойство систем DPI в малой степани полезно для задач организации блокирования доступа к определенным ресурсам, хотя и может применяться при решении других задач.

Технические ответные меры Интернет-провайдера на обход блокирования

Применение правильно сконфигурированных устройств DPI позволяет снизить эффективность попыток обхода блокирования, путем простой смены IP-адреса ресурса, однако, дополнительных возможностей противодействия обходу блокирования путем перехода на защищенные соединения или на виртуальные частные сети устройства DPI не предоставляют.

Оценка затрат, масштабируемость и влияние на производительность сети

Сохранение производительности сети является ключевым фактором при внедрении устройств DPI. Следует учитывать, что производительность устройств DPI существенно отстает от производительности сети. На данный момент не существует устройств способных работать на скоростях магистральных каналов. Для того чтобы уменьшить влияние на пропускную способность сети Интернет, оператору, возможно, придется распределять трафик по менее мощным каналам и разместить большее число устройств DPI. Это может вообще поставить под сомнение целесообразность массового использования DPI на всех каналах доступа.

Устройства DPI сравнимы по стоимости с крупным магистральным сетевым оборудованием, и внедрение DPI на сети провайдера может увеличить суммарные расходы провайдера на активное оборудование вдвое и даже больше.

Так как ряд интернет-провайдеров уже разместили системы проверки пакетов в сети для управления трафиком и для других целей, принципиальных препятствий для использования этого метода не существует, однако следует иметь в виду, что его широкомасштабное

использование порождает и новые проблемы в форме растущей сложности построения и эксплуатации сети и постоянного существенного (в разы) увеличения объема инвестиций в сетевую инфраструктуру и обеспечение ее производительности.

Скорее всего, с учетом того, внедрение DPI требует крупномасштабных капитальных вложений, системы DPI в ближайшей перспективе смогут использовать только крупные операторы в случае их многоцелевого использования для защиты и управления сервисами.

Последствия блокирования для пользователей, провайдеров Интернета

При использовании устройств DPI необходимо уделить соответствующее внимание защите данных, обеспечению конфиденциальности и соблюдению правил перехвата данных. Характер технологии дает провайдерам доступ к личным данным и другой конфиденциальной информации. Очевидно, что при применении DPI должны быть приняты меры по защите законных интересов пользователей, включая бизнес.

3.1.5 Комбинированное блокирование

С точки зрения снижения уровня обхода блокирования в некоторых случаях более эффективным может оказаться сочетание различных методов блокирования сайта. Но ряд методов обхода, как, например, VPN и службы-анонимайзеры, сохраняют эффективность в случае использования любых методов блокирования и их комбинаций.

Блокирование сайта по IP-адресу несбалансированно и, практически во всех случаях приводит к избыточному блокированию. Это может подорвать

доверие к любой схеме блокирования сайтов. Избыточное блокирование при IP-фильтрации является неизбежным в случае доступа к виртуальным веб-сайтам. Блокирование по IP-адресу нельзя отнести к основным методам блокирования.

От применения DNS-блокирования на неавторитативных серверах следует отказаться так как оно несовместимо с новыми технологиями защиты DNS (DNSSEC, DANE).

Мы полагаем, что в качестве основного метода следует рассматривать блокирование на основе комбинированного URL-блокирования. В этом случае после перенаправления запросов по IP адресам блокируемых ресурсов на прокси-серверы, последние производят фильтрацию по конкретным URL.

Наконец, для повышения эффективности URL-блокирования можно применять и DPI. Следует учитывать при этом высокую стоимость данного решения и фактическое отсутствие дополнительных преимуществ при его применении с точки зрения блокирования.

Однако, как указывалось выше, как и в случае использования прочих методов, блокирование с использованием любого комбинированного подхода может быть обойдено с использованием служб-анонимайзеров, таких как The Onion Router (TOR), VPN или анонимных прокси-серверов.

3.2. Инфраструктурное блокирование

Описание решения

Интернет-приложения очень часто зависят или полагаются на поддержку общесетевых, глобальных инфраструктурных сервисов - таких, как DNS, удостоверяющие центры, базы данных WHOIS и реестры маршрутизации в Интернет. Эти сервисы управляют или определяют

структуру и доступность интернет- приложений, предоставляя необходимые данные для программ.

Данные инфраструктурные сервисы состоят из технических баз данных, содержащих определенную информацию о структуре и актуальной конфигурации сети.

База данных RIR содержит информацию о том, кому были выделены IP-адреса и как связаны между собой автономные системы. Следует отметить, что для предоставления конкретных услуг Интернета разные операторы и приложения используют эти данные по-разному.

Последствия внесения изменений в эти базы/реестры гораздо сложнее предсказать, чем последствия фильтрации конкретного веб- сервера.

Как физические объекты серверы, которые используются для предоставления инфраструктурных сервисов, существуют в пределах юрисдикций конкретных правительств, и их операторы обязаны подчиняться соответствующим законам. Законы могут требовать осуществления блокирования и накладывать соответствующие обязательства на операторов инфраструктурных услуг в рамках соответствующей юрисдикции, либо через прямые действия правительства, либо путем требований блокирования через суд.

Последствия блокирования для пользователей, провайдеров Интернета

Как неоднократно указывалось выше, глобальная природа Интернета часто делает блокирование даже одного IP-адреса чрезмерным в том смысле, что оно может затронуть и другие ресурсы, не связанные с блокируемым, и нанести побочный ущерб, ограничив не противоречащее закону использование ресурсов.

Блокирование инфраструктурных услуг ведет к существенно более глобальным последствиям, которые могут привести к снижению устойчивости, ухудшению доступности и удобства использования глобальной сети Интернет. Инфраструктурное блокирование может подорвать доверие к Интернету в целом и стимулировать развитие параллельных или «подпольных» инфраструктур, ведущих к «балканизации» Интернета.

Соответствие архитектуре Интернета

Блокирование инфраструктурных данных идет в разрез с принципом локальности. Глобальный характер интернет-услуг и ресурсов усиливает блокирующие действия, в том смысле, что увеличивает риск сверхблокирования - невозможность законного использования ресурсов.

Пример инфраструктурного DNS блокирования

Рассмотрим DNS-блокирование: на конкретном адресе или имени домена могут размещаться как законные услуги, так и услуги, которые правительство может потребовать заблокировать. Сервис может находиться на хостинге в юрисдикции, где он сочтен нежелательным, но может считаться законным в другой юрисдикции. В таком случае блокирующее действие в юрисдикции расположения закроет доступ к легитимным услугам в другой юрисдикции.

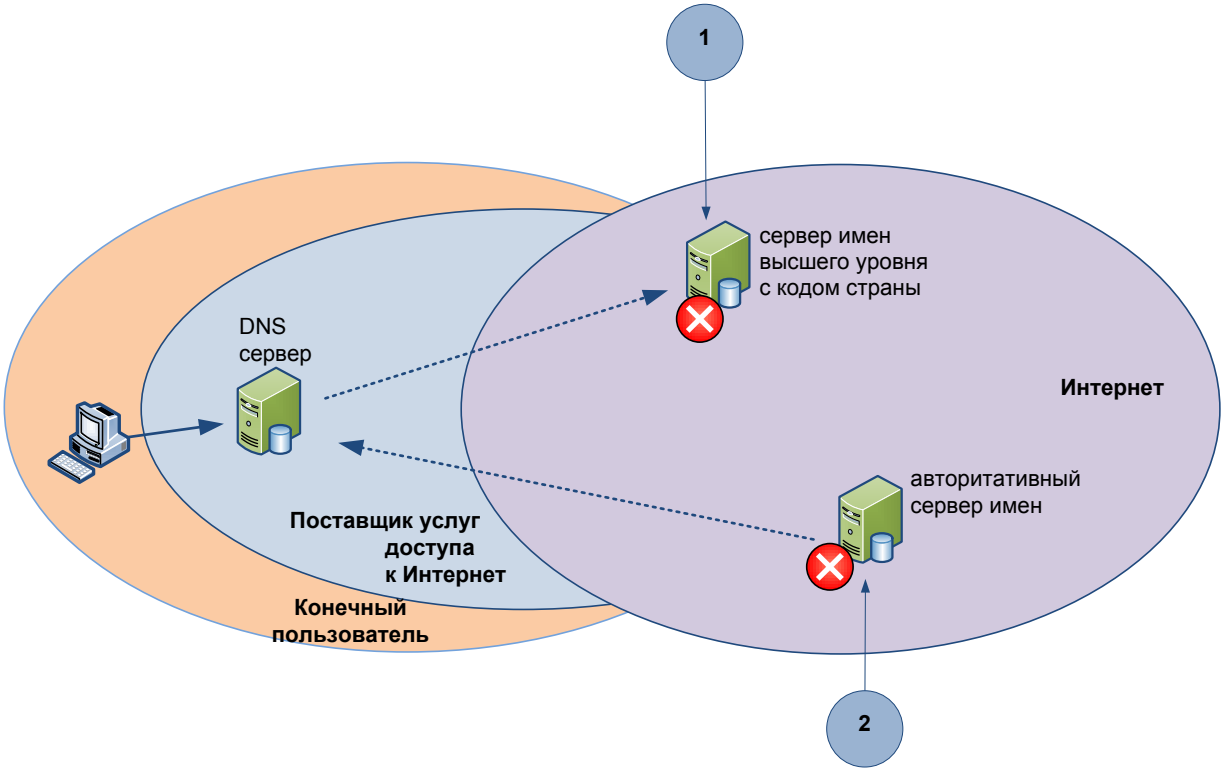


Рис. 3.2.1 Инфраструктурное блокирование

Обозначение	Пояснение
1	Исключение домена реестром или регистратором
2	Блокирование домена оператором авторитативного сервера

Примерами такого типа блокирования являются «изъятия» доменных имен, рассмотренные в следующем примере.

Пример изъятий доменов в США

В США широко используется подход к блокированию доступа к нелегальным сайтам, который не требует предварительного контакта с оператором сайта или предоставления ему возможности оспорить блокирование до момента его реализации. Отдел Иммиграционной и таможенной полиции США (ICE) Департамента по вопросам внутренней безопасности изымает домены сайтов, которые предположительно нарушили

авторское право в США. Согласно закону США о гражданской конфискации, имущество может быть изъято до предварительного заключения, если есть опасение, что оно может быть уничтожено ответчиком до начала слушания.

ICE, руководствуясь постановлением Суда, переключает авторитативные серверы имен этих захваченных доменов и изменяет записи доменных имен, В результате чего посетители соответствующих веб-сайтов перенаправляются на веб-сервер, управляемый ICE, который отображает страницу с предупреждением. «Конфискация» домена осуществляется в сотрудничестве с реестрами, управляющими общими доменами верхнего уровня (gTLD-доменами). Так, например, если сайты имеют суффикс «.com», это осуществляется с участием администратора соответствующего gTLD-домена, которым согласно договору с ICANN является компания VeriSign.

При посещении изъятых адресов веб-сайт выдает следующую страницу с предупреждением федеральных властей США.

Рисунок 3.2.2: Страница федерального сайта для изъятых доменов

«Данное доменное имя было конфисковано ICE – Службой расследований в области национальной безопасности».

Данные меры воздействия могут служить сдерживающим фактором для операторов запрещенных сайтов, поскольку требуют поиска альтернативного домена для работы сайта. Следует отметить, однако, что это не является существенным препятствием и во многих случаях сайты

продолжают работу под новыми именами. Но это не означает, что все операторы сайтов при этом ищут способы обхода.

С другой стороны широко известны способы обхода изъятий, доступные для конечных пользователей. Например, существуют плагины браузера Firefox, которые автоматически перенаправляют конечных пользователей на новые домены сайтов, имена которых были изъяты ICE.

Непродуманная практика использования изъятий также может приводить к нежелательным последствиям: так, в одном случае в результате действий ICE возникла ситуация существенного чрезмерного блокирования - был заблокирован доступ к 84000 сайтов.

При наличии эффективного международного сотрудничества между правоохранительными органами эффективность изъятий может быть выше, но в его отсутствие операторам сайтов по-прежнему довольно легко перейти в альтернативный реестр.

Пример попытки блокирования на уровне базы RIR:

Полиция Нидерландов по запросу правоохранительных органов США потребовала от RIPE NCC ограничить возможности некоторых интернет-провайдеров управлять своими регистрационными данными и, как следствие, сервисами путем введения контроля за изменениями их записей в базе данных реестра IP- адресов[RIPE]. Это несколько отличается от других ситуаций, поскольку не сразу сказывается на возможностях провайдеров в части предоставления услуг.

Провайдеры используют реестры IP-адресов для построения фильтров маршрутизации или пользуются информацией из них для поиска и устранения неисправностей, но использование данных реестров для указанных целей не является обязательным. При этом практически все

крупные провайдеры и большинство средних и мелких используют данные реестры на добровольной основе.

Таким образом, изъятие такого рода пока не может оказать гарантированного непосредственного влияния на подключение к сети, но может повлиять на общее доверие к инфраструктурным сервисам.

Практический пример информации о записи в реестре

Реестр IP-адресов может предоставить информацию о контактных лицах для лиц или организаций, желающих подать жалобу или получить дополнительную информацию о принадлежности адресов или административную информацию относительно управления IP-адресами. Он может быть использован как дополнение/альтернатива баз данных WHOIS DNS, но указанные базы данных не содержат детальной информации о распределении IP-адресов и данные в них зависят от точности предоставленной владельцами сети информации.

Операторы сетей не всегда своевременно обновляют контактную информацию в случае ее изменения, создавая практические проблемы идентификации администраторов сети, которая использует конкретный IP-адрес или пул адресов.

```
% Information related to '213.189.197.0 - 213.189.197.255'

inetnum: 213.189.197.0 - 213.189.197.255
netname: ZENON
descr: Zenon N.S.P.
remarks: INFRA-AW
country: RU
admin-c: ZNO1-RIPE
tech-c: ZNO1-RIPE
status: ASSIGNED PA
mnt-by: ZENON-NOC
source: RIPE # Filtered

% Information related to '213.189.192.0/19AS6903'

route: 213.189.192.0/19
descr: ZENON N.S.P.
descr: 1-ja Jamskogo polia 19
descr: Moscow, Russia
origin: AS6903
mnt-by: AS6903-MNT
source: RIPE # Filtered
```

Рис. 3.2.3. Результат WHOIS-запроса по IP-адресу zniis.ru

Аналогичная проблема точности существует и для DNS реестров. Для эффективной борьбы с правонарушителями необходимо существенное повышение точности и корректности данных в соответствующих инфраструктурных реестрах. Например, при регистрации домена реестр должен обязательно требовать от владельцев доменов предоставление поддающихся проверке контактных данных и гарантировать, что эти данные остаются правильными, когда право собственности на домен переходит в другие руки. Необходима регулярная проверка записей реестра на корректность. Неправильная регистрация контактных данных должна приводить к изъятию домена на том основании, что имело место нарушение условий договора и регламентов. На территории Российской Федерации это может быть реализовано непосредственно лишь в части доменов с суффиксом «.рф» и «.ru». Для улучшения администрирования реестров

доменных имен в целом необходимо развитие международного сотрудничества в этой области.

Эффективность блокирования и сложность обхода

Эффективность инфраструктурного блокирования ограничена принципом автономности. Если интернет-сообщество не согласится с решением о блокировании и начнет противостоять ему, то на уровне отдельных сетей авторитативные данные инфраструктурных сервисов могут быть скорректированы для обхода блокирования с использованием инфраструктурного сервиса. Внедрение DNSSEC и RPKI может на время изменить ситуацию, так как потребуется авторизация изменений. Но это, в свою очередь, может спровоцировать построение альтернативных источников инфраструктурной информации и переход провайдеров на их использование.

С другой стороны, эффективность такого блокирования ограничивает распределенность и мобильность Интернета. Поскольку интернет-услуга доступна из любой точки Интернета, сервис, заблокированный в одной юрисдикции, часто перемещается или переустанавливается в другой. Аналогичным образом, сервисы, которые зависят от заблокированных ресурсов, могут быть быстро переконфигурированы, что позволит им использовать не заблокированные ресурсы.

В случае с инфраструктурным блокированием по DNS также возможны пути обхода блокирования. Если доменное имя заблокировано через изменение авторитативных записей, сетевые операторы могут восстановить сервис, просто увеличив время жизни (TTL) записей, кэшированных до блокирования в рекурсивных резолверах или статически сконфигурировать в резолверах записи с данными до блокирования. Однако статическое конфигурирование не будет работать с данными, подписанными DNSSEC.

Следует также признать, что те, кто стремятся обойти блокирование, всегда смогут выбрать менее надежные, но незаблокированные параллельные услуги.

Подытоживая, следует указать, что инфраструктурное блокирование иногда может быть использовано для немедленного блокирования конкретной услуги путем удаления некоторых ресурсов, от которых эта услуга зависит. Однако глобальная природа ресурсов Интернета порождает вредные побочные эффекты подобных блокирующих действий. Тот факт, что интернет-ресурсы могут быстро перенесены из одного места в другое, переключены между разными доменными именами и IP-адресами, в сочетании с автономностью сетей, образующих Интернет, может быстро сводить на нет последствия инфраструктурного блокирования.

Действия в одной юрисдикции могут иметь более широкие последствия, нарушая принцип локальности и этим снижая доверие в глобальной системе, и могут подтолкнуть операторов к разработке своих собственных автономных решений.

Блокирование услуг путем остановки или вмешательства в работу инфраструктурного сервиса не соответствует принципу иерархичности, мобильности ресурсов Интернета, что будет приводить к нежелательным и на сегодняшний день непредсказуемым последствиям.

3.3. Блокирование в точке подключения

Интернет-пользователи и их устройства постоянно принимают решения вступать им в те или иные интернет-коммуникации. Пользователи сами решают, стоит ли переходить по ссылкам в подозрительных сообщениях электронной почты, браузеры рекомендуют пользователям не посещать сайты, которые кажутся подозрительными; спам-фильтры - оценивать подлинность отправителей и сообщений. Если бы оборудование и программное обеспечение были бы способны не вступать в определенные коммуникации, то блокирование было бы наиболее эффективным, потому что такие коммуникации никогда бы не имели места.

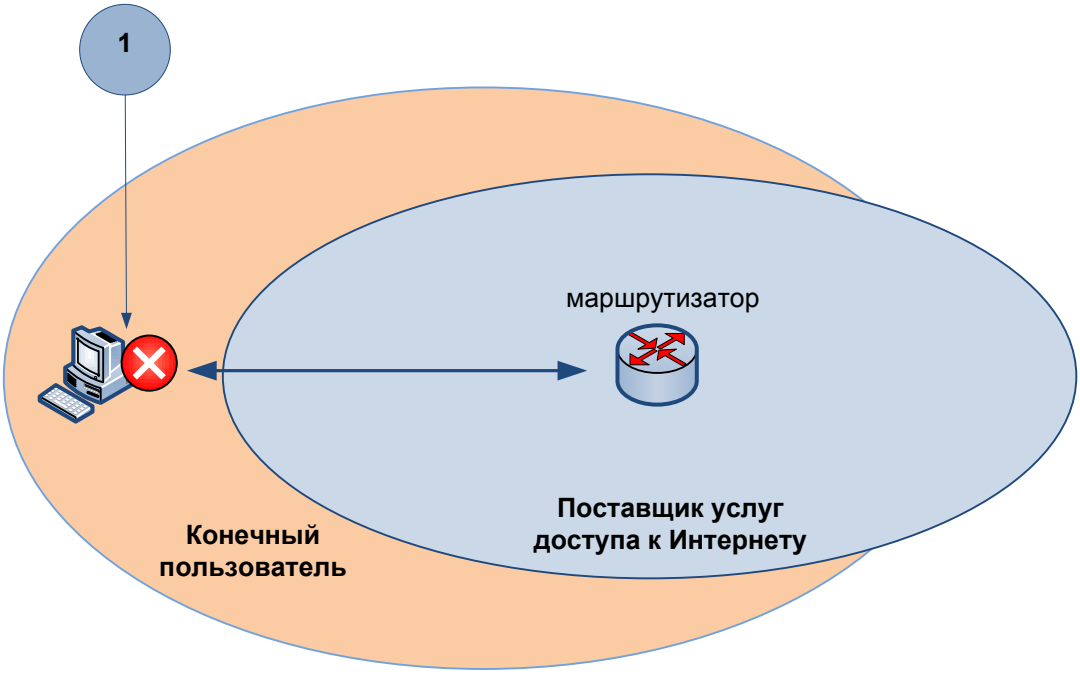


Рис. 3.3.1 Блокирование в точке подключения

Обозначение	Пояснение
1	Пользовательская система блокирования (браузеры, почтовые сервера/MTA)

Сегодня существует ряд систем, рекомендующих пользовательским программам пользоваться или не пользоваться теми или иными услугами. Некоторые современные браузеры, прежде чем загрузить сайт, сверяются с сервисами «безопасного серфинга», чтобы определить, является ли сайт потенциально опасным. Фильтрация спама является одной из самых старейших систем блокирования в Интернете. Современные системы блокирования для принятия решений по конкретному сообщению или отправителю обычно используют те или иные базы «репутаций» или «черных списков». Очень часто системы блокирования (браузеры, почтовые серверы/MTA) используют один и тот же репутационный сервис.

Для пользователей Интернета существуют инструменты, позволяющие реализовать блокирование из дома. Например, может использоваться программное обеспечение, аналогичное антивирусному ПО, которое позволяет пользователям указывать конкретные сайты для блокирования. Производители аппаратных маршрутизаторов могут также предлагать подобные дополнительные функциональные возможности как оператору Интернета, так и конечному потребителю. Эти опции могут включать дополнительные услуги, направленные на блокирование известных вредоносных сайтов, такая функция может дополняться функциями родительского контроля.

Такой подход к блокированию соответствует принципам архитектуры Интернета, он не противоречит принципам сквозной коммуникации, иерархичности, мобильности и локальности/автономности.

Блокирование в точке подключения производится одной из сторон интернет-коммуникации, что позволяет избежать проблем связанных с технологиями сквозной безопасности, которые возникают при сетевом блокировании. Блокирование в точке подключения также не имеет некоторых недостатков инфраструктурного блокирования. В то время как инфраструктурное блокирование влияет только на часть сервиса (например,

разрешение доменного имени), блокирование на стороне пользователя (в зависимости от того как оно реализовано) контролирует все приложения на всех уровнях и соединениях. Это дает системам, расположенным на стороне пользователя, более подробную информацию, на основе которой можно принимать решение о блокировании.

В частности, блокирование на стороне пользователя позволяет успешно бороться с мобильностью злоумышленников. Если блокированная услуга переносит ресурсы или начинает использовать другие, инфраструктурный или сетевой подход не в состоянии повлиять на новые ресурсы (или по крайней мере, не сразу). Сетевое блокирование, в случае, если для связи используется защищенный протокол, может даже не обнаружить, что используется новый ресурс. Блокирование на стороне пользователя, напротив, позволяет определить, что адреса ресурсов, использованных заблокированной услугой, изменились (поскольку полностью видны все транзакции), и перенастроит параметры блокирования после получения обновленных данных от репутационной системы.

И, наконец, в системе блокирования, расположенной в точке подключения, действия по блокированию выполняются автономно. Таким образом, эффекты блокирования локальны по своему воздействию, что позволяет минимизировать последствия для других пользователей или других легитимных сервисов.

Основная проблема, связанная с блокированием в точке подключения, заключается в том, что для его реализации необходимо взаимодействие с конечными пользователями. Когда такое взаимодействие возможно, проблема разрешима, так как от пользователя потребуется только перенастроить или обновить программное обеспечение. Но в целом, крайне сложно наладить сотрудничество с большим количеством пользователей.

При решении проблемы с сотрудничеством можно утверждать, что блокирование в точке подключения может быть намного более эффективным, чем все остальные подходы, потому что оно согласуется с архитектурными принципами Интернета.

4. Анализ практики блокирования и оценка перспектив сети Интернет

4.1. Опыт и практика борьбы с незаконными сервисами

Вопрос о том, как бороться с использованием сетевых услуг для незаконной деятельности, является сложным. Эти технологии также используются в законных целях, так как они являются очень эффективными способами распространения и хранения данных, контента и приложений.

В мировой практике уже сложился определенный набор правовых, административных и добровольно принимаемых подходов для борьбы с незаконными сервисами. Подробный анализ этих мер выходит за рамки настоящего исследования, но уместно обратить внимание на ряд подходов, применяемых в настоящее время.

• Уведомление и закрытие сайта:

Схема уведомления и закрытия может быть существенным дополнением к мерам технического блокирования, предлагая поставщику услуг возможность удаления контента до применения официального блокирования. Это особенно важно, когда метод блокирования несет риск избыточного блокирования. То, что удаление контента осуществляется по требованию регулирующего органа, как мы полагаем, защищает сервис провайдера от ответственности перед владельцем контента.

• Удаление ссылки из поисковой выдачи:

Некоторые поисковые системы, удаляют конкретные сайты из выдачи после представления доказательств о нарушениях. Удаление из поисковой

выдачи может быть эффективной мерой, поскольку затрудняет пользователям поиск незаконных сайтов.

Удаление из выдачи поисковика может повысить эффективность схемы блокирования. Оператор сайта, который был заблокирован, может переместить сайт на альтернативный IP-адрес, URL или домен, но если он не может обеспечить внесение нового расположения в поисковую выдачу, это может затруднить его нахождение для пользователей.

• Лишение доходов

Незаконные сайты могут получать значительные доходы. Некоторые сайты взимают абонентскую плату, осуществляют баннерную рекламу для законных брендов и часто могут быть привлекательными для потребителей. В некоторых случаях (контрафакт) потребителю может быть трудно узнать, является ли сайт действительно незаконным. Одним из методов воздействия может быть требование удаления сервисов платежных платформ с таких сайтов и удаление рекламы с этих сайтов. Существенным может являться исключение такого рода сайтов из систем любой контекстной рекламы и, в первую очередь, из платной контекстной рекламы в выдаче поисковиков. Помимо того, что сервисы будут выглядеть менее законными, удаление сервисов платежной платформы и рекламы может сделать такие сайты экономически неэффективными.

• Изъятия доменов:

В США процедуры изъятия реализуются проще, чем в России, учитывая, что под юрисдикций США находятся крупнейшие реестры доменов. Такая мера, если она будет реализована в России, будет иметь только ограниченный эффект, учитывая, что она будет влиять только на

домены верхнего уровня с кодом страны «.ru» и «.рф». Эффективность данного подхода по изъятию может существенно повыситься при улучшении и развитии международного сотрудничества между правоохранительными органами и, тем самым, минимизации возможностей для операторов нелегальных сайтов по миграции из одного домена верхнего уровня в другой.

Все перечисленные выше меры потенциально могут играть важную роль в поддержке схемы блокирования сайтов, как дополнение к техническим методам, компенсируя недостатки, присущие методам блокирования.

4.2. Анализ последствий применяемых технологий

Блокирование по DNS без нарушения ряда архитектурных принципов и технологий безопасности Интернет может осуществляться только на уровне реестров и авторитативных серверов[SAC056].

4.3 Новые внедряемые технологии и их влияние на блокирование сайтов

Долгосрочная жизнеспособность некоторых современных методов для блокирования доступа к сайтам в Интернете остается открытым вопросом. В этом разделе мы кратко рассмотрим известные появившиеся интернет-технологии, которые, по нашему мнению, могут оказать существенное влияние на то, как может работать схема блокирования сайтов. Учитывая быстрые темпы научно-технического прогресса в этой области и рассмотренные ниже технологии, любое законодательство, направленное на блокирование сайтов, должно опираться на широкий круг перспективных тенденций, а не оставаться привязанным к технологиям сегодняшнего дня.

DNSSEC

Россия, наряду со многими другими странами, начала применение компонентов безопасности DNS (DNSSEC). Цифровые сигнатуры проверяют подлинность источника запросов DNS-имени посредством «цепочки доверия». DNSSEC является ключевым техническим решением по предотвращению «отравления» кэша DNS, техники, которую используют злоумышленники для перенаправления пользователей веб-сайта на другой сайт по выбору хакера. Это может приводить к тому, что пользователь непреднамеренно предоставит конфиденциальные данные хакеру или загрузит вредоносное ПО с сайта.

DNS-блокирование, которое опирается на изменение DNS-записей из неавторитативного источника, является методом блокирования, который конфликтует с DNSSEC. Клиент, использующий DNSSEC, ожидает ответа с цифровой подписью при запросе разрешения имени.

Блокирование на неавторитативном сервере DNS не может предоставить клиенту ни измененного ответа DNS с корректной цифровой подписью, ни корректно подписанного негативного ответ. При этом операционная система или браузер указывает на сомнительную подлинность ответа на запрос заблокированного имени, что может привести к подрыву доверия к DNS в целом, к DNSSEC в частности и потенциально привести не только к путанице, но и к появлению нового класса хакерских атак, мимикрирующих под деятельность блокирующих систем.

DNS RPZ

Служба доменных имен Беркли (BIND) – это широко используемое свободное программное обеспечение для DNS-серверов. Программное обеспечение находится в свободном доступе и включено во многие операционные системы UNIX и Linux. BIND поддерживается и создана

Консорциумом Интернет-систем (ISC). Версия BIND 9.8 полностью включает в себя механизм Response Policy Zones (RPZ)5.

DNS RPZ сервис дает возможность серверам DNS получать обновления из централизованных источников, касающиеся находящихся в черном списке доменов. Концептуально схожая с черными списками спама, система DNS RPZ была первоначально разработана для решения проблемы фишинга и вредоносных веб-сайтов. DNS RPZ вполне может быть применена для блокирования деятельности сайтов, занимающихся другой нелегальной деятельностью. Пока еще не существует известных примеров эффективного применения этой технологии или прямой поддержки от альтернативных поставщиков программного обеспечения для серверов имен, но сама технология может рассматриваться для применения.

IPv6

Адреса IPv4 в настоящее время считаются исчерпанными, и сетевыми провайдерами, поставщиками и предприятиями постепенно начинает использоваться следующее поколение IP-адресов. IPv6-протокол предлагает почти неисчерпаемый запас уникальных IP-адресов. Потребители и операторы сайтов постепенно неизбежно начнут использовать адресацию IPv6.

Существующая тенденция туннелирования IPv6-трафика в рамках IPv4-трафика, уже сейчас также значительно снижает эффективность блокирования сайтов.

IPv6-устройства в будущем смогут быстрее менять IP-адрес и сетевое расположение, чем это позволяет IPv4.

[5] DNS Response Policy Zones (DNS RPZ) - http://ftp.isc.org/isc/dnsrpz/isc-tn-2010-1.txt

Имеются ли какие-либо преимущества IPv6 в отношении блокирования сайтов на настоящий момент непонятно.

Облачные технологии

Услуги на основе облачных технологий, такие как удаленное хранение данных, уже влияют на методы блокирования. Нелегальные сайты часто используют удаленные хранилища данных или виртуальный хостинг в облаках. Сервис может динамически в реальном времени изменять IP-адрес, географическое положение и юрисдикцию, изменять DNS-имя и реорганизовывать свою структуру.

Облачные технологии могут применяться и для блокирования по URL-через прозрачный прокси-сервер. При наличии пропускной способности Интернет провайдер может перенаправить трафик для определенного сайта через прокси-сервер на основе облачной технологии. По мере увеличения требований к производительности система нарастит вычислительные ресурсы, необходимые для выполнения задачи.

Новые технологии передачи HTTP трафика – SPDY

Разрабатываемая в настоящее время модификация протокола HTTP под названием SPDY уже доступна для использования на ряде крупнейших сервисов (таких как Google и Twitter, например) и поддерживается, как минимум, браузерами FireFox и Chrome.

Существенным отличием протокола SPDY от существующего протокола HTTP является то, что если HTTP открывает отдельное TCP-соединение для получения каждого элемента страницы, в протоколе SPDY все элементы передаются по одному соединению. Это примерно аналогично режиму работы HTTP “Keep-Alive” (за исключением ряда особенностей

мультиплексирования данных), но, если HTTP-протокол может работать как по незащищенным, так и по защищенным TCP-соединениям, то протокол SPDY спроектирован только для использования внутри защищенного (https://) соединения.

Таким образом, задача блокирования SPDY-соединений оказывается полностью эквивалентна задаче блокирования доступа к ресурсу по защищенному (https://) соединению, то есть, организующий блокирование столкнется с теми же проблемами. Распространение протокола SPDY приведет к повышению доли защищенных соединений в сети Интернет и к неэффективности применения устройств DPI для блокирования, опирающегося на анализ содержимого пакетов.

DANE

Расширение протокола DNS для аутентификации серверов (DANE) – предоставляет возможность для владельцев серверов распространять через систему DNS информацию об используемых сервером сертификатах цифровой подписи. Это может быть использовано для снижения вероятности создания фальшивого ресурса и перенаправления пользователей на него без их ведома. Очевидно, что использование DANE имеет смысл только в сочетании с DNSSEC, так как без DNSSEC записи DANE могут быть подделаны злоумышленником столь же успешно, как и записи типа A, которые сообщают IP адрес необходимого ресурса.

С точки зрения блокирования доступа к конкретным ресурсам, при использовании DANE не появляется новых особенностей, по сравнению с теми, которые возникают при блокировании ресурсов, использующих DNSSEC, а именно:

- средства блокирования, не использующие механизмы DNS, могут быть использованы обычным способом;
- при наличии доступа к авторитативному DNS-серверу для данного домена возможно блокирование доступа к ресурсу средствами DNS, как путем удаления соответствующих записей (объявляя соответствующее доменное имя «несуществующим»), так и путем перенаправления запросов на специальный ресурс, целью которого может быть как информирование потенциальных потребителей о том, что ресурс заблокирован, так и сбор информации о потенциальных посетителях этого ресурса для последующего анализа;
- при отсутствии доступа к авторитативному DNS-серверу для данного домена возможно блокирование доступа к ресурсу средствами DNS только первым способом, путем перехвата и уничтожения соответствующих запросов/ответов DNS на пути между браузером клиента и авторитативным DNS-сервером. Следует учитывать при этом, что путь к ресурсу и путь к соответствующему DNS-серверу, используемому для разрешения доменного имени данного ресурса, могут быть практически полностью несовпадающими, и имея возможность блокировать доступ к контенту, управляющий блокировкой механизм может не иметь возможности блокировать доступ к DNS-серверу и наоборот, то есть, чем дальше от потребителя находятся механизмы управления блокированием, тем более они ограничены в своих возможностях.

Массовый переход на защищенные соединения

Постоянно расширяющееся использование сети Интернет для целей онлайн-торговли товарами и услугами, банковских операций, обмена информацией между территориально удаленными подразделениями предприятий и организаций, в том числе и удаленного управления оборудованием и информационными системами сделало необходимым

создание и использование механизмов защищенного обмена информацией в сети Интернет.

В настоящее время защищенные (шифрованные) варианты существуют практически для всех используемых в сети Интернет протоколов и они опираются на криптографические схемы и протоколы мирового уровня стойкости.

Наблюдаемая тенденция к повсеместному использованию защищенных протоколов уже привела в частности к тому, что стандартом де-факто в настоящее время является обязательное использование защищенного соединения не только при оказании онлайн-услуг, а практически при любых коммуникациях, связанных с передачей информации, которую отправитель не предназначал для неограниченного распространения, обязательным также считается использование защищенных соединений при аутентификации пользователей на каких-либо ресурсах. Следует отметить, что после установления защищенного соединения для проведения аутентификации, естественным является продолжение информационного обмена по уже установленному защищенному соединению. Таким образом, вся информация, получаемая с ресурса, передается по защищенному соединению.

Повсеместное использование защищенных соединений делает применение DPI (а также любых форм URL-блокирования) для блокирования доступа к каким-либо ресурсам неэффективным. Возможность дешифрования современных криптографически защищенных протоколов «на лету» требует наличия вычислительных мощностей космического масштаба, которыми устройства DPI не будут обладать в течении как минимум еще нескольких десятилетий. Попытки манипуляции с сертификатами соответствующих ресурсов крайне сложны технологически и организационно, они могут эффективно быть блокированы применением DANE (это расширения DNS как раз и создавалось для борьбы с подобными манипуляциями), и, принципиально, имеют частный характер, то есть, могут

применяться по отношению к конкретному ресурсу (или небольшой их группе), но совершенно непригодны в качестве общего решения для обеспечения блокирования списка заранее неизвестных ресурсов.

Таким образом, DPI нельзя рекомендовать как базовое средство для обеспечения эффективного блокирования ресурсов, в связи с тем, что внедрение его является долгим и дорогостоящим процессом, а сфера его применимости будет быстро сжиматься, в частности, начало практики блокирования ресурсов подтолкнет их владельцев (особенно ресурсов, находящихся в «зоне риска») к повсеместному использованию защищенных соединений.

Кроме защищенных соединений типа «клиент-сервер», использующихся при доступе к конкретным ресурсам, в настоящее время широко используются соединения типа «виртуальная частная сеть» (VPN), которые позволяют клиенту включаться посредством установления защищенного (шифрованного) туннельного соединения в некоторую сеть, ресурсы которой могут быть полностью недоступны из публичного Интернета. При этом, внутри этой «частной сети» существует практически полностью структура и инфраструктура сети Интернет (свои DNS-серверы, свои IP-адреса, своя маршрутизация, свои информационные ресурсы и т.п.). В этой ситуации, анализ туннелируемого трафика требует, как уже указывалось выше, оборудования с возможностью дешифрования сетевого трафика «на лету», которое в настоящее время отсутствует на рынке.

Единственной имеющейся на сегодняшний день возможностью противодействовать активности через VPN может быть только недискриминированное блокирование пакетов, передающих туннелируемый траффик. К сожалению, это немедленно приведет к дезорганизации работы предприятий и организаций, использующих эти протоколы для легитимного обмена информацией и будет оказывать существенное негативное воздействие на экономику.

4.4 Заключение о методах блокирования

Подход, используемый в Новой Зеландии[CHILD] на основе перенаправления запросов к блокируемым сайтам по IP адресам на прозрачный прокси-сервер с дальнейшей фильтрацией по URL (IP+URL) - на наш взгляд является наиболее оптимальным на данный момент и может быть рекомендован как основной для операторов в Российской Федерации.

Метод анализа содержимого пакетов также может применяться для блокирования по URL. Но он является дорогостоящим и не менее ограниченным по масштабируемости и эффективности, хотя и можно ожидать, что затраты будут снижаться, так как крупные интернет провайдеры вкладывают средства в устройства DPI и для решения других задач. Тем не менее, прежде чем принимать решение о применении DPI как базового решения следует оценить масштабы требуемых инвестиций и возможные технические последствия для эксплуатации и масштабирования сетей. Также необходимо оценить правовые проблемы, связанные с неприкосновенностью частной жизни, защитой данных и правилами перехвата информации. Отдельной проблемой являются имиджевые, социальные и внешнеполитические/внешнеэкономические риски, связанные с внедрением технологий данного типа.

Представляется, что использование DPI не дает значительных преимуществ по сравнению со схемой IP+URL в задачах блокирования, и, будучи на порядки более дорогостоящим решением, может применяться только в тех случаях, когда целесообразность его применения обусловлена наличием каких-либо других задач.

5. Регулирование доступа к запрещенной информации в Интернете на территории Российской Федерации

В данном разделе представлен обзор текущего законодательства Российской Федерации и правил саморегулирования, имеющих отношение к блокированию информации, а также их реализации с точки зрения технологии.

Практика признания информации запрещенной к распространению в России в настоящее время регламентируется целым корпусом федеральных законов. Первичным нормативным правовым актом, регулирующим отношения в информационной сфере является Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и защите информации» (далее – Закон «Об информации»). Этот акт раскрывает ключевые дефиниции, такие как «информация», «доступ к информации», «электронный документ», «распространение информации», «доменное имя», и т. д., закрепляет общие принципы правового регулирования, а также рамочно определяет порядок блокирования доступа.

Закон «Об информации» не определяет порядка ограничения доступа к информации, который в каждом отдельном случае может быть различным. Отдельные федеральные законы, тем не менее, также не всегда содержат требования к процедуре признания информации запрещенной и, соответственно, ограничения доступа к ней.

До вступления в силу поправок в Федеральный закон от 29 декабря 2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» блокирования доступа к той или иной информации требовали антиэкстремистское законодательство и правила регистрации доменных имен.

Федеральный закон от 25 июля 2002 №114-ФЗ «О противодействии экстремистской деятельности»

В 2012 г. одним из самых распространенных оснований для блокирования ресурсов стал Федеральный закон «О противодействии экстремистской деятельности». Статья 12 указанного закона запрещает использование сетей связи общего пользования для осуществления экстремистской деятельности. Между тем, под экстремистской деятельностью понимается множество различных действий, так или иначе связанных с распространением информации — публичное оправдание терроризма и иная террористическая деятельность; возбуждение социальной, расовой, национальной или религиозной розни; пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; распространение экстремистских материалов; пропаганда нацистской и сходной с ней символики и т. п. Таким образом, у прокуратуры и Роскомнадзора, как органов, ответственных за противодействие экстремизму в Интернете, имеется два основания требовать блокирования доступа к Интернет-ресурсам — (1) распространение материалов, включенных в Федеральный список экстремистских материалов, который составляет Министерство юстиции Российской Федерации, и (2) публикация материалов, которые ведомства сочтут, к примеру, возбуждающими социальную рознь.

Технологии реализации блокирования доступа не определены.

Статья 15.1 Закона «Об информации» и статья 46 Федерального закона от 07 июля 2003 №126-ФЗ «О связи»

Однако наиболее громкой законодательной инициативой в сфере регулирования интернета стал Федеральный закон №139-ФЗ от 28 июля 2012 «О внесении изменений в Федеральный закон «О защите детей от

информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет».

Суть закона заключается в создании Единого реестра доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

Реестр ведет уполномоченная организация или государственный орган (в настоящее время — Роскомнадзор), который на основании заключений, выданных должностными лицами Федеральной службы по контролю за оборотом наркотиков (ФСКН), Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор) или Роскомнадзора принимает решение о включении в реестр отдельных страниц, сайтов или IP-адресов.

В реестр попадают сайты, которые содержат две категории запрещенной информации — (1) признанную запрещенной судебным актом и (2) признанную запрещенной решением органа исполнительной власти, уполномоченного Правительством Российской Федерации (в настоящее время этими органами являются ФСКН, Роспотребнадзор, Роскомнадзор).

К первой категории относится любая информация, признанная судом запрещенной. Например, экстремистские материалы.

Уполномоченные правительством государственные органы принимают решения в отношении информации, относящейся к детской порнографии, информации о способах изготовления и употребления наркотиков и информации о способах совершения самоубийства, а также содержащей призывы к совершению самоубийства.

Следует отметить критику данной законодательной инициативы, напрямую связанную с данной работой, как-то:

— нарушение связности Сети в перспективе;

— имплицитное нарушение статьи 29 Конституции Российской Федерации и статьи 3 №149-ФЗ, связанное с возможной блокировкой законной информации при блокировке по сетевым адресам, на которых может находиться более одного ресурса.

Дополнения к статье 15.1 Закона «Об информации»

В настоящее время Госдума приняла законопроект о дополнении перечня информации, блокирующейся на основании решения уполномоченного органа *информацией о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами*6. Законопроект также подвергся критике интернет-индустрии и общества.

Включение в реестр означает, что все провайдеры обязаны блокировать доступ к этой информации для своих абонентов. Таким образом, у владельца сайта есть выбор — удалить информацию, в отношении которой экспертом по непубличным основаниям принято решение о запрещении или обжаловать блокирование в суде. С учетом темпов работы российских судов процесс может занять не один год, в течение которого сайт будет блокирован.

При этом перечень заблокированных ресурсов является закрытым, но можно проверить на официальном сайте www.zapret-info.gov.ru не находится ли в реестре конкретный адрес, сайт или страница.

Но самой серьёзной проблемой является также способ осуществления блокировки. В законе сказано, что блокирование может осуществляться по доменному имени, по универсальному указателю страницы или по сетевому

[6] http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=109392-6&02

адресу. ***Но технология реализации и методы блокирования не были определены***. Применение же избыточного блокирования по IP-адресу приводит к блокированию десятков или даже сотен не связанных между собой ресурсов. На данный момент количество реально заблокированных сайтов в результате отсутствия точной методологии превышает официальный список в 20-30 раз.

Федеральный закон от 07 февраля 2011 №3-ФЗ «О полиции» и Федеральный закон от 17 января 1992 №2202-1 «О прокуратуре Российской Федерации»

Возможности для вынесения представлений о блокировке или удалении информации в сети «Интернет» также содержатся в Законе «О полиции».

В статье 13 Закона «О полиции» указывается: «Полиции для выполнения возложенных на нее обязанностей предоставляются следующие права: …..вносить в соответствии с федеральным законом руководителям и должностным лицам организаций обязательные для исполнения представления об устранении причин и условий, способствующих реализации угроз безопасности граждан и общественной безопасности, совершению преступлений и административных правонарушений».

В рамках уголовного судопроизводства порядок внесения таких представлений установлен с 2001 г. частью 2 статьи 158 Уголовно-процессуального кодекса Российской Федерации.

Аналогичные указанным в Законе «О полиции» полномочия имеются также у прокуроров согласно закону «О прокуратуре Российской Федерации».

Согласно этим полномочиям сотрудники силовых структур могут требовать от провайдеров хостинга или операторов связи блокировки

определённого контента в интернете, признав его «*причиной или условием*» совершения правонарушения. Однако, технологии реализации блокирования доступа также не определены.

Правила регистрации доменных имён

Способ практически мгновенного блокирования доступа к сайту, если он зарегистрирован в российских национальных доменах *.ru* или *.рф*, российским властям предоставил Координационный центр Национального домена сети Интернет (автономная некоммерческая организация, уполномоченная выполнять функции национальной регистратуры и, соответственно, разрабатывать правила регистрации доменных имен второго уровня).

Предложенное решение относится к инфраструктурному блокированию и не оказывает негативного влияния на технологии Интернет.

В ноябре 2011 года Координационным центром была утверждена новая редакция Правил регистрации доменных имен в доменах .RU и .РФ.[7]

Ранее правила позволяли регистратору прекращать делегирование домена в зоне .РФ без согласия администратора только на основании судебного акта либо мотивированного запроса одного из руководителей органа, осуществляющего оперативно-розыскную деятельность (что также незаконно, но давало хотя бы некоторые гарантии). Правила для домена .RU вообще не предусматривали такого основания как запрос силовых структур.

Новая редакция правил не требует объяснения мотивации. Достаточно просто направить решение регистратору. После общественной реакции, вызванной публикацией в октябре 2011 года новых правил, КЦ пришлось вносить коррективы. Спустя несколько месяцев на сайте КЦ

[7] http://cctld.ru/ru/docs/rules.php

появились «разъяснения» спорного пункта[8], однако сами правила, являющиеся основным документом, регулирующим регистрацию российских доменов, остались без изменений.

RU-CENTER — один из крупнейших российских регистраторов также внес соответствующие изменения в регламент в отношении геодоменов третьего уровня вида xxx.msk.ru и xxx.spb.ru .

В пункте 3.3.6 Регламента регистрации доменов третьего уровня[9], являющийся обязательным приложением к договору на регистрацию доменного имени, указывается следующее:

«3.3.6. Исполнитель вправе незамедлительно прекратить делегирование домена в целях пресечения незаконной деятельности, а также деятельности, наносящей ущерб третьим лицам, в том числе деятельности по распространению и рекламированию порнографических материалов, призывов к насилию, осуществлению экстремистской деятельности, свержению власти и др., а также деятельности, противоречащей общественным интересам, принципам гуманности и морали, оскорбляющей человеческое достоинство либо религиозные чувства, и т.д. При этом Регистратор вправе самостоятельно давать оценку деятельности Пользователя на предмет нарушения законодательства, в том числе в случаях, когда определение таких действий не закреплено нормативными актами. Определение порнографических материалов опубликовано на сайте Регистратора по адресу http://www.nic.ru/dns/service/hosting/moral_standards.html.»

Данные правила позволяют осуществлять изъятия доменов во многих случаях и относятся к методу инфраструктурного блокирования по DNS.

[8] http://cctld.ru/ru/press_center/news/news_detail.php?ID=3500&sphrase_id=61510

[9] http://nic.ru/dns/reglaments/regl_15.html#n3

Инициативы по расширению оснований для блокировки ресурсов в интернете

В настоящее время представители правообладателей (в основном американских) совместно с Министерством культуры Российской Федерации предлагают дополнить Закон «Об информации» новой статьёй 15.2, где будет описываться порядок уведомлений владельцев сайтов, провайдеров хостинга и операторов связи по схеме, аналогичной описанной в статье 15.1 и предполагающей создание реестра авторских прав.

Проект закона «О внесении изменений в отдельные законодательные акты Российской Федерации в целях профилактики и пресечения нарушений интеллектуальных прав в информационно-телекоммуникационных сетях, в том числе в сети Интернет»[10] предполагает следующие изменения законодательства:

Закон «Об информации»

— Статья 1, часть 2: Расширение сферы действия положений Федерального закона «Об информации, информационных технологиях и защите информации» на отношения, возникающие при правовой охране РИД, в случаях, предусмотренных Федеральным законом «Об информации, информационных технологиях и защите информации».

— Статья 15.2: Перечень мер для прекращения нарушения интеллектуальных прав, а также порядок их осуществления провайдерами хостинга и владельцами сайтов в сети «Интернет».

— Обязанность провайдеров хостинга и владельцев сайтов предоставлять персональные данные клиентов для осуществления судебного преследования.

[10] http://mkrf.ru/dokumenty/3974/detail.php?ID=272242

— Обеспечительные меры в отношении информационных посредников и владельцев сайтов — блокирование доступа.

КоАП

- — Расширение предметной области на размещение объектов авторского права без извлечения дохода.
- — Увеличение административной ответственности информационного посредника вплоть до конфискации и приостановления деятельности.

Существенным недостатком в существующей нормативной базе является полное отсутствие руководства по реализации требуемых мер.

Существующая практика приводит к непредсказуемым последствиям как для пользователей сети, так и операторов сети.

Необходим набор мер, реализующих нормы законов и четко описывающий как требования к реализации, так и реалистичную процедуру проверки исполнения, недопускающую вольное трактование контролирующими органами.

Технологии блокирования не должны нарушать целостность и устойчивость сети, ее безопасность и должны защищать интересы законопослушных граждан и бизнеса – включая операторов доступа и сервисов сети Интернет.

6. Сопутствующие аспекты, связанные с блокированием

Необходимо обратить внимание на нижеперечисленные вопросы, решение которых должно иметь место в комплексе с внедрением блокирования, так как они имеют значительное влияние на эффективность процесса блокирования в целом и его последствия независимо от применяемых технических решений по блокированию:

• Идентификация операторов сайтов: Стандартным подходом к выявлению владельцев веб-сайтов является проверка по базе данных WHOIS, основному источнику информации о владельце домена. По отчетам ICANN только 28% записей в базе данных WHOIS являются совершенно точными, и лишь с 46% владельцев доменов можно связаться напрямую или косвенно. Для эффективной профилактической работы необходимо обеспечение точной идентификации. Необходима совместная работа как с национальным Координационным центром, так и с регистраторами и реестрами других ДВУ, а также с ICANN по обеспечению точности баз данных реестров DNS.

В случае невозможности идентификации представляется возможным разрешить блокирование без идентификации, в предположении, что владелец веб-сайта не принял достаточные меры, чтобы его можно было легко идентифицировать, в то время как для его идентификации были предприняты все усилия.

• Своевременное осуществление блокирования: после принятия решения, может оказаться, что для введения блокирования в действие могут потребоваться дни, в зависимости от используемой интернет-провайдерами техники блокирования и режима администрирования сети. Тем не менее, это может быть сделано довольно быстро (теоретически, в течение нескольких минут), если процессы полностью автоматизированы и интернет-операторы имеют соответствующие средства по управлению изменениями.

• Точечность блокирования: ограниченная степень точности блокирования отдельных методов приводит к риску того, что блокирование может непреднамеренно ограничить доступ к законным сервисам, с неблагоприятными последствиями для этих сервисов, а также конечных пользователей. Следует уделять внимание отработке и развитию процедур уведомления владельцев веб-сайтов. Точечное блокирование является более эффективным, если оно осуществляется владельцами сайтов. Предпочтительным являются обращения с требованием к владельцам сайтов удалить нарушающий требования закона контент. Блокирование же веб-сайта следует применять в первую очередь к веб-сайтам, которые не реагируют на подобные обращения. Это также поможет решить проблему масштабируемости блокирования. Следует отметить, что при увеличении числа элементов в списке блокирования от интернет-провайдеров потребуются дополнительные инвестиции в активное оборудование, так как типичное оборудование среднего провайдера в настоящее время даже по самому примитивному IP-блокированию ограничено пределами 2-3 тысяч элементов.

• Ответственность поставщиков услуг: интернет-провайдеры должны быть защищены от любой ответственности, которая может возникнуть в случае блокирования и особенно избыточного блокирования. Рекомендуется выбрать и рекомендовать определенные методы блокирования и однозначно специфицировать методику проверки выполнения блокирования.

Любой предлагаемый регламент или процедура должны учитывать интересы граждан и законных пользователей, так как блокирование веб-сайтов, в конечном счете, может оказать негативное влияние на неприкосновенность частной жизни и свободу слова**.**

Регламенты, процедуры и инструкции по блокированию должны учитывать законные интересы других заинтересованных сторон (т.е. владельцев веб-сайтов, которые могут быть заблокированы в результате этих процессов, конечных пользователей, которые могут потерять доступ к

конкретному контенту, а также интернет-провайдеров, которые могут быть задействованы в обязательствах по блокированию).

Если операторы веб-сайтов или конечные пользователи не будут доверять принятым решениям по блокированию, они будут иметь мощные стимулы к обходу любого блокирования. Чтобы снизить эти риски процесс блокирования должен удовлетворять следующим принципам:

• Доступность: операторы веб-сайтов, интернет-провайдеры и конечные пользователи должны иметь возможность использовать судебный процесс для защиты своих интересов либо в качестве ответчика, либо заинтересованной стороны;

• Пропорциональность решений: должно быть ясно, что решение о блокировании является объективно оправданной мерой.

• Ясность: важно, чтобы были четко определены любые обязательства, возлагаемые на операторов в отношении блокирования доступа к соответствующим веб-сайтам. К этому же относится длительность и масштаб исполнения любого решения, методы, которые должен использовать оператор; то, будут ли компенсироваться расходы, связанные с реализацией требуемых мер.

• Прозрачность: если блокирование было применено, необходимо иметь средства информирования операторов веб-сайтов и конечных пользователей о причинах того, почему веб-сайт перестает быть доступным, а также предоставления четкой информации о том, какие шаги они могут предпринять для обжалования решения.

Для повышения эффективности блокировании веб-сайтов могут применяться дополнительные административные меры. Среди них - изъятия доменов, использование процедур уведомления и закрытия сайта, а также исключение из выдачи поисковых систем, систем контекстной рекламы. Хотя они могут реализовываться независимо друг от друга, но существуют преимущества при их совместном использовании с блокированием веб-сайтов.

Например, схемы уведомления и закрытия сайта могут использоваться для стимулирования операторов веб-сайтов по удалению правонарушающего контента, при угрозе того, что будет применено блокирование. Учитывая риск избыточного блокирования, присущий применению большинства из рассмотренных методов, система предварительного уведомления поможет защитить законные интересы тех операторов, сайты которых могли бы быть случайно заблокированы. В свою очередь она будет создавать дополнительные препятствия для сайтов, предлагающих исключительно незаконный контент.

Общим для всех подходов к блокированию является то, что владелец сайта может относительно легко перенести свой сайт на другой IP-адрес, URL или домен, и новый сайт затем может быть «повторно найден» путем простого поиска. С одной стороны кажется – что это легко может быть решено путем блокирования в поисковых системах. Но в такой ситуации при снятии блокирования пользователи не смогут легко и быстро найти новое местонахождение (из-за удаления из поисковых систем). Блокирование с использованием поисковых систем может также приводить к непредсказуемому непреднамеренному блокированию легального контента.

Можно рассмотреть вопрос о возможном взаимодействии и сотрудничестве с VPN-провайдерами. VPN-провайдеров можно попросить о помощи при блокировании правонарушающих сайтов, доступ к которым имеется у их клиентов. В случае отказа операторы VPN могут рисковать быть заблокированными. Но следует отметить, такой подход следует рассматривать как чрезмерную эскалацию блокирования, что требует очень тщательного анализа с точки зрения эффективности его реализации и последствий его применения.

С учетом текущих тенденций развития технологий доступа к веб-сайтам все рассмотренные методы все равно вряд ли будут способны обеспечить полностью эффективное блокирование сайтов. Также невозможно полностью совместить требования к интернет-провайдерам по

своевременному блокированию и решению проблем обхода, с соблюдением законных интересов операторов сайтов, поставщиков услуг и конечных пользователей.

Обход блокирования является технически относительно простым делом независимо от того, какой из методов блокирования используется. Информация о способах, с помощью которыхк операторы сайтов и конечные пользователи могут обойти блокирование, широко распространена и легкодоступна в Интернете. Сервисы обхода могут предоставляться не только операторами – но и в силу природы Интернета – любыми конечными пользователями в любой юрисдикции планеты.

За последние годы было проведено некоторое количество исследований по анализу поведения пользователей при использовании блокирования. По некоторым оценкам обходом блокирования могут воспользоваться всего лишь 3% конечных пользователей, несмотря на доступность информации и средств обхода для большинства массовых пользователей. В принципе возможно позиционировать схему блокирования сайтов таким образом, чтобы свести к минимуму стимулы для обхода. Например, если операторы и конечные пользователи будут считать процессы принятия решений по блокированию справедливыми, то можно ожидать и уменьшения случаев обхода блокирования.

Если блокирование сайтов с нелегальным контентом станет элементом более широкого комплекса мер, включающего информирование и образовательные программы для широкой аудитории, и будет поддерживаться эффективным развитием и продвижением приемлемых по цене и удобных законных сервисов, то это позволит снизить стимулы для потребителей продолжать использовать нелегальные сервисы. Необходимы дальнейшие исследования в области дополнительных мер, которые могли бы стимулировать изменения в социальной культуре и уровнях толерантности к онлайн-нарушениям.

7. Рекомендации по организационным и техническим решениям

В качестве основной схемы реализации блокирования противоправного контента в Российской Федерации предлагается следующее:

1. Установить, что блокирование должно проводиться провайдерами, оказывающими лицензированные услуги связи.
2. Установить, что блокирование должно проводиться только на сетях доступа и не должно затрагивать магистральные сети, каналы связи между провайдерами, опорные сети операторов национального масштаба, точки обмена трафиком и прочие критические элементы инфраструктуры сети Интернет
3. Установить, что элементом списка блокирования сайтов является URL.
4. Определить понятия “общий” и “частный” для элементов списка блокирования, где “общий”, это URL имеющий *только* доменную часть имени, а «частный» - это URL имеющий кроме доменной части имени еще часть, описывающую путь на конкретном ресурсе
5. Определить технологию распространения списка блокирования (предлагается использовать https:// с авторизацией клиента и сервера по сертификату ЭЦП) и его машиночитаемый формат (предлагается использовать «tab-separated ASCII list” (URL с IDN-именами в них должны заноситься в лист уже перекодированными в punycode)
6. Установить, что провайдеры должны организовать регулярное получение актуального списка блокирования из авторитативного источника и его использование.
7. Рекомендовать использование следующей технологии для реализации блокирования:
   a. Выделение “общей” (доменной) части имени из URL

b. Трансляция с помощью запросов в DNS доменного имени в IP-адрес

c. Создание и распространение по системе маршрутизации сети доступа провайдера специального маршрута для данного IP-адреса, направляющего трафик в специальный анализирующий сегмент

d. Проведение анализа трафика, проходящего через анализирующий сегмент, выявление запросов к URL, содержащихся с списке блокировки, уничтожение данных запросов или перенаправление их на специальный ресурс, уведомляющий о факте блокировки.

e. Маршрутизация трафика, не подпадающего под условия блокирования, с анализирующего сегмента из сети доступа в опорную сеть и далее по сети Интернет на общих основаниях.

8. В случаях, если URL в списке блокировки является «общим» (содержит только доменную часть имени и не содержит уточняющего пути внутри ресурса) и DNS-оператор соответствующей доменной зоны находится в российской юрисдикции, возможно, дополнительно, проводить блокировку на уровне DNS, обязав DNS-оператора производить замену записей в соответствующей доменной зоне записью, указывающей либо на недоступность данного ресурса, либо перенаправляющей запросы на специальный ресурс, уведомляющий о факте блокировки

8. Заключение

Целью настоящего исследования был анализ методов, которые интернет-провайдеры и регулирующие органы могут использовать для ограничения доступа к запрещенным ресурсам в Интернете; потенциальной точности этих методов; оценка степени легкости их обхода; а также наличе в арсенале интернет-операторов мер, препятствующих их обходу..

Доступные для применения в настоящее время технологии блокирования были рассмотрены по отдельности, а также в возможных комбинированных вариантах.

Мы рассмотрели следующие методы блокирования:

• по IP-адресу

• по DNS

• по URL

• углубленный анализ пакетов (DPI)

В соответствующих разделах настоящего исследования были также детально представлены особенности каждого из методов блокирования, их влияние на работоспособность и устойчивость сети, возможные пути обхода блокирования, возможные меры противодействия обходу блокирования.

Анализ существующих методов блокирования позволяет сделать следующий вывод:

Наиболее предпочтительным методом блокирования следует признать комбинированное блокирование с предварительным выделением по IP адресам и дальнейшей фильтрацией по URL (IP+URL). Оно может быть рекомендовано как основной метод для решения данной задачи. Рекомендации по организационным и техническим решениям для реализации предлагаемого метода изложены в разделе 7 настоящего исследования.

Блокирование на основе комбинированного метода **IP+URL** или на основе углубленного анализа пакетов (на самом деле это тот же способ – но с использованием выделенного специализированного оборудования), предлагает достаточную точность, чтобы избежать чрезмерного блокирования, оказывает минимальное воздействие на инфраструктуру сети Интернет, не снижает ее устойчивость в целом и не нарушает работоспособности других сервисов и приложений.

В сегодняшних условиях для большинства интернет-пользователей применения этого метода будет достаточно, и он позволит ограничивать доступ массовых пользователей к блокируемым ресурсам.

В качестве базового метода рекомендуется метод **IP+URL**, а не метод DPI, так как массовое использование DPI несет существенные риски, является спорным с точки зрения соблюдения права на неприкосновенность частной жизни, приводит во многих случаях к ничем некомпенсируемому удорожанию сети, вносит технические ограничения на развитие сети. . Следует отметить также, что это самый технически сложный и дорогостоящий метод и в его отношении существует целый ряд правовых аспектов на международном уровне, - таких как совместимость DPI-блокирования с установленными законодательством, в том числе, международным, нормами о неприкосновенности частной жизни, свободе слова, защите данных и передаче информации по каналам связи, обеспечение. Кроме того, применение DPI может существенно повлиять на производительность сети, поскольку каждый пакет информации проверяется на предмет наличия незаконного контента. В целом, следует признать, что применение DPI ставит под сомнение возможность масштабирования сети в соответствии с растущими потребностями и тенденциями роста Интернета

DNS-блокирование, возможно, представляло бы собой более простой и менее затратный вариант, но при использовании DNSSEC оно требует сотрудничеества с операторами соответствующих авторитативных DNS-серверов, что, в некоторых случаях, обеспечить более сложно, чем

содействие со стороны интернет-провайдеров. Кроме того, DNS-блокирование обладает несколько меньшей точностью указания блокируемого ресурса, чем при использовании метода **IP+URL**. Однако, простота и эффективность этого метода позволяют применять его в случае, когда налажено взаимодействие с DNS-операторами соответствующих доменных зон. Инфраструктурное **блокирование по DNS на уровне авторитативных серверов и реестров можно рассматривать как возможное к применению в качестве дополнительного метода блокирования** в настоящее время и в будущем.

Блокирование IP-адресов не является достаточно точным и надежным методом блокирования сайтов, чтобы рассматривать его для применения либо в качестве первичного метода, либо как элемента комбинированного метода. Использование блокирования IP-адресов приводит к значительному избыточному блокированию и ряду негативных последствий. **Использование блокирования по IP не рекомендуется.**

Следует отдавать себе отчет в наличии технических возможностей для обхода всех методов блокирования, которые относительно просты в применении. Разумеется, методы противодействия обходу существуют, но они имеют ограничения, например, в отношении защищенных соединений и доступа через виртуальные частные сети (VPN).

Тот факт, что для операторов веб-сайтов и конечных пользователей технически возможно обойти блокирование, не означает, что на практике они будут это делать повсеместно. Блокирование веб-сайтов, скорее всего, будет сдерживать случайных и непреднамеренных нарушителей и усложнит распространение незаконной информации среди добросовестных пользователей.

Таким образом, блокирование незаконных ресурсов может способствовать общему уменьшению случаев нарушения в сети Интернет, если оно является частью более широкого набора мер по борьбе с нарушениями.

Обозначения и сокращения

Сокращение	Обозначение
AfriNIC	African Network Information Center (Африканский сетевой информационный центр)
APNIC	Asia Pacific Network Information Centre (Сетевой информационный центр Азиатско-Тихоокеанского региона)
ARIN	American Registry for Internet Numbers (Американский реестр номеров Интернета)
AS	Autonomous System (автономная система)
BGP	Border Gateway Protocol (Протокол граничного шлюза)
CDN	Content Delivery Network (Сеть доставки контента)
ccTLD	Country code top-level domain (Национальный домен верхнего уровня)
DNS	Domain Name System (Система доменных имен)
DNSSEC	Система обеспечения безопасности при передаче информации в системе DNS/ Технология, используемая для аутентификации и проверки запросов доменных имен для уменьшения случаев мошенничества в Интернете (посредством, в частности, перехвата и подделки запросов)
DPI	Deep Packet Inspection (Углубленная проверка пакетов информации)
FAITID	Foundation for Assistance for Internet Technologies and Infrastructure Development (Фонд содействия развитию технологий и инфраструктуры Интернета)
gTLD	Домен общего пользования верхнего уровня
IAB	Internet Architecture Board (Совет по архитектуре Интернета в IETF)

IANA	Internet Assigned Numbers Authority (Орган администрирования адресного пространства Интернета)
ICANN	Internet Corporation for Assigned Names and Numbers (Интернет-корпорация по распределению имен и адресов)
IDN	Internationalized Domain Names (Интернационализованные доменные имена)
IESG	Internet Engineering Steering Group (Руководящая группа IETF)
IETF	Internet Engineering Task Force (Рабочая группа по инжинирингу Интернета)
IRR	Internet Routing Registry (Региональный интернет-реестр)
IRTF	Internet Research TaskForce (Рабочая группа по Интернет-исследованиям)
IXP	Internet eXchange Point (Точка обмена трафиком)
LACNIC	Latin American and Caribbean Internet Addresses Registry (Реестр интернет-адресов стран Латинской Америки и Карибского бассейна)
LIR	Local Internet Registry (Локальная интернет-регистратура)
NRO	Number Resource Organization (Объединение региональных регистратур)
NTIA	National Telecommunication sand Information Administration (Национальная администрация США по вопросам телекоммуникаций и информатизации)
RFC	Requests for Comments (Запросы о комментариях)
RIPE NCC	Réseaux IP Européens Network Coordination Centre (Европейский сетевой координационный центр)
RIR	Regional Internet Registry (Региональная интернет-регистратура)
RPKI	Resource Public Key Infrastructure (Инфраструктура открытых ключей для идентификации сетевых объектов)

TLD	Top-Level Domains (домены верхнего уровня)
ККБС	Консультативный комитет по безопасности и стабильности ICANN (Security and Stability Advisory Committee, SSAC)
ККСКС	Консультативный комитет системы корневых серверов ICANN (Root Server System Advisory Committee, RSSAC)
ОПА	Организация по поддержке адресов ICANN (The Address Supporting Organization, ASO)
ОПНИ	Организация по поддержке страновых имен ICANN (Country-Code Names Supporting Organization, CCNSO)
ОПОИ	Организация по поддержке имен общего пользования ICANN (Generic Names Supporting Organization, GNSO)
ОРМ	Оперативно-розыскные мероприятия
ПКК	Правительственный консультативный комитет ICANN (Governmental Advisory Committee, GAC)
ШПД	Широкополосный доступ

Технический глоссарий

Список управления доступом (ACL)	Сетевая технология, которая позволяет разрешать или запрещать трафик по направлениям или сервисам
Анонимный прокси-сервер	Сервис, который позволяет пользователям делать веб-запросы через сервис-посредник. Прокси-сервер устанавливает соединение от имени пользователя, тем самым скрывая, исходный IP-адрес и обходя сетевые методы блокирования.
Авторитетный сервер имен DNS	Сервер имен DNS, который отвечает за данную зону
Система доменных имен (DNS)	Глобальная иерархическая распределенная база данных. Позволяет осуществить преобразование доменных имен, например, www.example.com -> 192.0.32.10
Гипертекстовый транспортный протокол (HTTP-протокол)	Протокол приложения, используемый обычно между веб-серверами и веб-браузерами
Протокол защищенной пересылки гипертекста (HTTPS-протокол)	Зашифрованный HTTP-протокол с использованием протокола безопасных соединений/защиты транспортного уровня. Данные между веб-браузером и веб-сервером шифруются. Передаваемые данные являются частными. HTTPS-протокол предотвращает прослушивание или изменение данных. Широко используется для онлайн-покупок с помощью кредитной карты. Визуально безопасное соединение HTTPS-протокола обозначается символом в виде замка́ .

Интернет-протокол (IP)	Сетевой протокол на основе пакетов.
Сетевой порт	Назначенный номер соединения, который делает возможным работу множественных сервисов на одном хосте.
Технология Peer-to-Peer (P2P)	Сетевая технология, используемая для распределения распространения контента. Широко используется для неавторизированного распределения авторского контента.
Рекурсивный сервер имен DNS	Сервер, который осуществляет поиск записей доменных имен от имени пользователя. Как правило, кэширует ответы для повышения производительности для последующих запросов.
The Onion Router (ToR)	Анонимная сеть, первоначально разработанная ВМФ США. Используется во многих странах, чтобы обойти государственную цензуру.
Протокол управления передачей данных (TCP-протокол)	Сетевой протокол транспортного уровня с установлением соединений.
Унифицированный указатель ресурса (URL)	Стандартизированный способ записи адреса ресурса в сети Интернет
Протокол дейтаграмм (UDP-протокол)	Сетевой протокол передачи сообщений без образования соединения
Виртуальная частная сеть (VPN)	Технология, которая обеспечивает безопасную передачу данных через Интернет с помощью зашифрованных сетевых соединений. Используется

	для различных целей, включая удаленный доступ для сотрудников.

Список использованной литературы

1. [RFC3724] RFC3724. The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture.
2. [RFC2775] RFC2775. Internet Transparency.
3. [RFC5246] RFC5246. The Transport Layer Security (TLS) Protocol.
4. [RFC4301] RFC4301. Security Architecture for the Internet Protocol.
5. [RFC1122] RFC1122. Requirements for Internet Hosts -- Communication Layers.
6. [RFC3261] RFC3261. SIP: Session Initiation Protocol
7. [Dagon]Dagon, D., Provos, N., Lee, C., and W. Lee, "Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority", 2008, <http://www.citi.umich.edu/u/provos/papers/ndss08_dns.pdf>.
8. [Citizen]Citizen Lab, "Routing Gone Wild", July 2012, <https://citizenlab.org/2012/07/routing-gone-wild/>.
9. [SIGCOMM]"The Collateral Damage of Internet Censorship by DNS Injection", July 2012, <http://conferences.sigcomm.org/sigcomm/2012/paper/ccr-paper266.pdf>.
10. [BT] Meyer, D., "BT blocks The Pirate Bay", June 2012, <http://www.zdnet.com/bt-blocks-the-pirate-bay-4010026434/>.
11. [TPB] "The Pirate Cloud", October 2012, <http://thepiratebay.se/blog/224>.
12. [TOR] "Tor Project: Anonymity Online", 2012, <https://www.torproject.org/>.
13. RFC 1738 – Uniform Resource Locators (URL)
14. [SAC056] "SSAC Advisory on Impacts of Content Blocking via the Domain Name System", October 2012, <http://www.icann.org/en/groups/ssac/documents/sac-056-en.pdf>
15. [US-ICE] U.S. Immigration and Customs Enforcement, "Operation in Our Sites", 2011,

<http://www.ice.gov/doclib/news/library/factsheets/pdf/operation-in-our-sites.pdf>

16. [RIPE], " The RIPE NCC's Case Against the State of the Netherlands Dismissed ", 2013, < https://www.ripe.net/internet-coordination/news/about-ripe-ncc-and-ripe/ripe-nccs-case-against-the-state-of-the-netherlands-dismissed>
17. [HONEY] «HOW FAST-FLUX SERVICE NETWORKS WORK» http://www.honeynet.org/node/132
18. [OFCOM] OFCOM Internal review of request for site blocking report, Consumer, 18/10/2011 http://stakeholders.ofcom.org.uk/freedom-of-information/foi-responses/2011/october2011/1-186872101/
19. [IETFILTERING] Technical Considerations for Internet Service Blocking and Filtering draft-iab-filtering-considerations-02, 2013 https://datatracker.ietf.org/doc/draft-iab-filte/ring-considerations
20. [IGF2012WS180] IGF 2012 Workshop 180 Blocking and Filtering Internet DNS Content, 11/2012, <http://wsms1.intgovforum.org/content/no180-blocking-and-filtering-internet-dns-content> .
21. [CHILD] DIGITAL CHILD EXPLOITATION FILTERING SYSTEM. Public Information Pack http://www.dia.govt.nz/pubforms.nsf/URL/DCESF-PublicInformationPack.pdf/$file/DCESF-PublicInformationPack.pdf