Internet Society — обзор перспектив блокировки интернет-контента

Март 2017 г.

Internet Society

Содержание

Вступительное слово

Государственные органы различных стран мира все чаще используют блокировку интернет-ресурсов для ограничения доступа к нелегальному контенту. Причины, по которым органы власти блокируют доступ к контенту, весьма разнообразны. Здесь и нелегальные онлайн-казино, и кража интеллектуальной собственности, стремление защитить детей и соображения национальной безопасности. Однако, если вынести за скобки проблему детской порнографии, в мировом сообществе нет единства по вопросу о том, что следует считать допустимым контентом с точки зрения общественного правопорядка.

Настоящий документ содержит технический обзор различных способов блокировки интернет-контента, включая эффективность рассматриваемых способов, а также связанные с ними недостатки и проблемы. Его авторы не пытаются оценивать законность блокировки интернет-контента или связанные с ней политические мотивы[1].

Результаты технического анализа привели нас к следующему заключению — блокировка Интернета не является эффективным решением проблем нелегального контента и незаконной деятельности. Она скорее наносит косвенный ущерб пользователям Интернета.

Что касается технической стороны вопроса, мы рекомендуем законодателям осмотрительно подходить к применению средств блокировки Интернета для решения проблем общественного правопорядка. Использование взвешенного подхода и альтернативных методов служит важным шагом к созданию глобального и открытого Интернета, в котором царит атмосфера доверия и обеспечено взаимодействие отдельных сегментов всемирной сети.

1 Читателям, которые интересуются правовой оценкой блокировки контента, мы рекомендуем посетить следующие ресурсы:
- Статья 19: https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf
- Совет Европы: http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet

Введение

Современный Интернет превратился во всемирный общественный феномен. Это произошло во многом благодаря контенту и услугам, которые доступны во всемирной сети и используют особенности ее уникальной архитектуры. Свободное трансграничное распространение контента служит основой благосостояния целых стран. На наших глазах ежедневно реализуются инновации, кардинально преобразующие целые отрасли мировой экономики. Интернет стал одним из основных столпов демократического процесса и площадкой для обсуждения законотворческой деятельности. С помощью Интернета люди даже находят свою любовь… и теряют ее.

В целом, Интернет был и остается двигателем современного мира. Согласно различным оценкам[2], к 2020 г. объем международного интернет-трафика в 95 раз превзойдет объем данных, накопленных в Интернете по состоянию на 2005 г. В 2020 г. количество устройств, подключенных к IP-сетям, втрое превысит численность населения Земли.

Следует признать, что в Интернете содержится контент, который хотят заблокировать авторы политик, законодатели и регулирующие органы разных стран мира. Мы наблюдаем всемирный феномен использования различных способов блокировки интернет-контента для ограничения доступа к контенту, который объявлен нелегальным в законодательстве отдельных стран. Сюда можно отнести блокировку иностранных онлайн-казино в Европе и Северной Америке, а также блокировку на территории Китая сайтов с политическими выступлениями оппозиции. Мотивы, побуждающие законодателей вводить блокировку интернет-контента, весьма разнообразны. Здесь и борьба с нарушением прав интеллектуальной собственности, и предотвращение распространения детской порнографии, и противодействие незаконной деятельности в Интернете, и защита национальной безопасности.

Авторы настоящего документа не ставили перед собой цель оценить мотивы блокировки или степень допустимости либо недопустимости отдельных ее разновидностей с этической, юридической, экономической, политической или социальной точек зрения. Вместо этого мы предлагаем вашему вниманию техническую оценку преимуществ и недостатков наиболее распространенных способов блокировки, используемых для предотвращения доступа к контенту, который объявлен нелегальным. Мы хотим разъяснить читателям возможности каждого способа блокировки, а также связанные с ними побочные эффекты, недостатки, компромиссы и издержки.

В итоге мы приходим к выводу, что использование интернет-блокировки не является эффективным способом решения проблемы нелегального контента. Такой подход не только затратен, но и наносит пользователям Интернета косвенный ущерб, общие сведения о котором приведены на стр. 6.

Что касается технического аспекта проблемы, **мы призываем законодателей осмотрительно подходить** к применению подобных мер и предлагаем внимательно расставлять приоритеты. Необходимо активнее использовать альтернативные подходы, решающие озвученную проблему на месте размещения контента. (Более подробные рекомендации см. в конце настоящего документа, включая руководство по минимизации негативных последствий таких мер.)

Также следует отметить, что в настоящем документе не рассматриваются меры блокировки, связанные с текущим управлением вычислительными сетями или обеспечением безопасности (например, борьба со спамом и вредоносными программами). В некоторых случаях эти задачи эффективно решаются с помощью программных инструментов и средств, описанных в настоящем документе.

Боковая колонка:
«Фильтрация, блокировка или цензура?»

Когда заходит речь о фильтрации интернет-контента, сразу вспоминаются такие слова как «фильтрация», «блокировка», «отключение» и «цензура». Впрочем, конечного пользователя больше волнуют не термины, а практические последствия. Если точнее, недоступность отдельных ресурсов Интернета. Выбирая слова, законодатели и интернет-активисты ориентируются скорее на смысловые оттенки, нежели на техническую корректность терминологии. Слово «цензура» имеет сильную негативную коннотацию, тогда как «фильтрация» выглядит более невинным и безвредным. Он звучит так, словно мы обсуждаем технологию варки пива. В этом документе мы используем простой и незамысловатый термин «блокировка».

2 Cisco® Visual Networking Index: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html

Таблица ниже содержит описание основных недостатков, связанных с блокировкой интернет-контента по соображениям охраны общественного правопорядка:

Проблема	Сведения
Легко обойти	Достаточно мотивированный пользователь сможет противодействовать всем приемам и методам, которые описаны в настоящем документе. Пользователи осваивают различные способы обхода блокировки контента, что снижает её эффективность.
Не решает проблему	Блокировка контента не приводит к удалению контента, который считается нелегальным. В некоторых случаях государственный запрет контента противоречит международным нормам. Однако, если нелегальность контента общепризнана, эту проблему лучше всего решать путем удаления контента там, где он хранится.
Причиняет косвенный ущерб	Когда у легального и нелегального контента совпадает IP-адрес, доменное имя или иные характеристики, блокировка контента затрагивает обе разновидности контента одновременно. Например, блокировка доступа к одной статье «Википедии» путем фильтрации DNS приведет к блокировке миллионов других статей этого же ресурса.
Подвергает пользователей риску	Если местный интернет-провайдер теряет статус надежного и открытого, пользователи Интернета могут обратиться к альтернативным и нестандартным подходам (например, использовать ПО для перенаправления трафика в обход фильтров). Применение временных решений подвергает пользователей дополнительному риску, связанному с безопасностью.
Провоцирует снижение прозрачности	Поддержание прозрачной среды и атмосферы доверия — залог успешной работы Интернета. Блокировка контента наносит ущерб прозрачности, вредит принципу открытости, который служит фундаментом всемирной сети, и провоцирует недоверие к открытым источникам информации.
Ведет к появлению подпольных услуг	Широкое использование блокировки контента приведет к популяризации «подпольных» услуг доступа и альтернативных оверлейных сетей. В результате контент станет труднодоступен для правоохранительных органов. Например, контент переместится в так называемый «глубинный веб», а пользователи начнут использовать виртуальные частные сети (VPN) для туннелирования трафика.
Нарушает тайну частной жизни	Некоторые способы блокировки контента требуют изучения пользовательского трафика, даже если он зашифрован. Нарушение тайны частной жизни пользователей происходит всякий раз, когда третья сторона отслеживает деятельность пользователей Интернета, ведет запись транзакций или вмешивается в работу средств шифрования, используемых для обеспечения безопасности в Интернете.
Сомнительность в части соблюдения прав человека и требований правосудия	Блокировка контента, реализованная без учета требований к необходимости и пропорциональности подобного вмешательства, может причинить большой косвенный ущерб, стать преградой на пути свободного и открытого обмена информацией, а также ограничить права частных лиц.

Мотивы блокировки контента

Настоящий документ **посвящен вопросу блокировки**, обусловленной требованиями законодательства, а также ее влиянию на Интернет и его пользователей. (Подробности о других мотивах блокировки см. на боковой колонке.)

Органы государственной власти применяют блокировку по соображениям охраны правопорядка, ограничивая доступ к информации и сопутствующим услугам, которые являются нелегальными в конкретной юрисдикции, считаются угрозой для общественного порядка или неприемлемы для какой-либо аудитории.

Например, законодатели большинства стран мира едины в желании заблокировать детям доступ к непристойным материалам, а также лишить любых пользователей доступа к материалам, связанным с насилием над детьми. Свое влияние на блокировку контента оказывают и особенности местной правовой среды. Например, блокировка контента может происходить в том случае, если он нарушает законодательство о защите интеллектуальной собственности. считается угрозой национальной безопасности, запрещен по культурным или политическим причинам.

Одна из трудностей, вынуждающих органы власти отдельных стран прибегать к использованию мер блокировки интернет-контента, заключается в том, что различные субъекты права, обеспечивающие доставку контента потребителям, зачастую расположены в разных странах, законодательство которых по-разному смотрит на проблему «нелегального контента». Задача блокировки нелегального контента дополнительно осложняется техническими особенностями Интернета как глобальной среды. Чтобы заблокировать такой контент, недостаточно отключить тот или иной сервер. К примеру, разместившее контент лицо находится в одной стране, серверы с контентом расположены в другой, а доменное имя зарегистрировано в третьей. В результате они находятся вне юрисдикции какого-либо отдельно взятого государства. Это обусловливает важность сотрудничества различных юрисдикций и необходимость тесной координации проводимых мероприятий с заинтересованными лицами, которые не связаны с государством.

Прочие мотивы блокировки контента

В настоящем документе рассматривается блокировка контента согласно требованиям законодательства. Тем не менее, можно назвать еще две распространенные причины блокировки сетевых ресурсов. Первая — **предотвращение угроз сетевой безопасности и реагирование на эти угрозы**. Такая разновидность блокировки встречается довольно часто. Например, большинство предприятий ставят заслоны на пути проникновения вредоносных программ в свои сети. Многие интернет-провайдеры (ISP) блокируют вредоносный трафик, исходящий из их сетей. Источниками этого трафика нередко служат взломанные устройства «Интернета вещей» (например, веб-камеры). Фильтрация электронной почты встречается практически повсеместно. Она включает в себя блокировку нежелательных массовых рассылок, а также вредоносной почты (например, фишинговых сообщений). Настоящий документ не касается этих видов блокировки.

Вторая причина блокировки — **регулирование использования сети**. Блокировка интернет-контента обусловлена требованиями к вычислительной сети, пропускной способности и управлению временем персонала, а не борьбой с отдельными видами контента. Например, работодатели зачастую ограничивают своим сотрудникам доступ в социальные сети на рабочем месте. В зависимости от приобретенных клиентом услуг, интернет-провайдеры также могут блокировать или разрешать доступ, ограничивать пропускную способность или ускорять доступ к определенному контенту. Управление вычислительными сетями редко становится предметом законодательного регулирования, кроме тех случаев, когда дело касается антиконкурентного поведения. Если вам интересна тема сетевой нейтральности, обратитесь к списку рекомендуемой литературы на стр. 26.

Обзор способов блокировки контента

С каждым способом связаны ограничения технического и политического характера, а также последствия, которые необходимо учитывать при рассмотрении отдельных видов блокировки контента. Цель настоящего документа — формирование единого подхода к оценке действенности этих способов и побочных эффектов их применения. Читатели, которые интересуются техническими аспектами блокировки, найдут ссылки на технические документы IETF в разделе Рекомендованная литература на стр. 26.

В настоящем документе рассматриваются следующие виды блокировки контента:

- Блокировка по IP-адресу и протоколу
- Блокировка с помощью технологии DPI
- Блокировка по URL-адресу
- Блокировка посредством платформы (обычно применяется поисковыми системами)
- Блокировка по DNS

Наш выбор пяти разновидностей блокировки обусловлен тем, что они затрагивают составляющие типичного цикла работы конечного пользователя: поиск и получение информации, включая использование поисковой системы, и просмотр информации с помощью браузера или аналогичного инструмента. Этот цикл хорошо известен законодателям, поскольку они сами пользуются Интернетом. Законодательная блокировка контента стремится нарушить работу основных элементов цикла.

На схеме справа показаны этапы типичного процесса поиска информации пользователем Интернета. Здесь также видны различные способы блокировки, используемые для нарушения этого процесса при реализации блокировки с целью поддержания общественного правопорядка. Согласно этой схеме, пользователь Интернета обращается к поисковой системе для получения какой-либо информации (шаг 1). Это стандартная отправная точка. Поисковая система возвращает список результатов (шаг 2). Пользователь выбирает один из них и переходит по ссылке (шаг 3). На эту часть цикла воздействует так называемая «блокировка посредством платформы». Она предусматривает блокировку отдельных результатов, возвращаемых поисковой системой.

Компьютер пользователя задействует службу DNS для поиска сервера, на котором находятся данные (шаги 4 и 5). Эту часть цикла затрагивает вторая разновидность блокировки — так называемая «блокировка по DNS».

Затем браузер пользователя пробует подключиться к серверу (шаг 6). Чтобы заблокировать эту часть цикла, можно использовать три других вида блокировки: блокировку по IP-адресу и протоколу, блокировку по URL-адресу и блокировку с помощью технологии DPI.

Общая схема поиска и блокировки информации в Интернете

1
Пользователь ищет слово «бомба» с помощью поисковой системы.

2
Без фильтрации пользователь видит

3
Пользователь переходит по ссылке в списке результатов (http:/пример.com/бомба)

4
Компьютер пользователя ищет пример.com с помощью DNS, чтобы подключиться к веб-серверу.

пример.com?
DNS
РЕКУРСОР

5
пример.com = 192.0.222

6
Браузер пользователя подключается к веб-серверу пример.com и запрашивает веб-страницу, по ссылке на которую перешел пользователь.

Кому: 192.0.222
Запрос пользовательского ПК к серверу пример.com
Получить: http://пример.com/бомба

7

От: 192.0.222
Запрос от сервера пример.com к пользователю
Получить:

Что видит пользователь в случае блокировки:

При использовании **фильтрации поиска** и других средств блокировки, реализованных с помощью платформы, пользователю недоступны результаты работы конкретной поисковой системы.
Поиск по запросу «бомба» не вернул результатов

При **блокировке по DNS** компьютер пользователя не находит сервер и поэтому не может открыть веб-страницу. Пользователь получает сообщение «Сервер не найден».
Сервер не найден

При **блокировке по IP-адресу и протоколу блокируется** подключение к серверу с IP-адресом 192.0.222. Становится недоступным весь контент на сервере (как запрещенный, так и разрешенный).
Превышено время ожидания подключения

В случае **блокировки по URL-адресу** трафик блокируется при обнаружении URL-адреса в черном списке.
Веб-сайт заблокирован администратором сети

При **блокировке с помощью технологии DPI** обмен трафиком прерывается при обнаружении определенных ключевых слов на веб-странице. Высока вероятность блокировки разрешенного контента.
Подключение было разорвано

Безусловно, Интернет не ограничивается только поисковыми системами и браузерами. Многие из следующих приемов эффективны не только при блокировке веб-страниц. Например, чтобы заблокировать службы VPN, которые шифруют и прячут трафик, можно использовать технологию DPI совместно с блокировкой по IP-адресу и протоколу.

Эти виды блокировки допускают как весьма узкое, так и крайне широкое применение. Например, можно заблокировать отдельный документ или сайт либо же ограничить доступ к «материалам по конкретной проблеме» или к «службам IP-телефонии (VoIP)».

Где происходит блокировка контента?

Многие из приемов блокировки контента, описанных в настоящем документе, могут использоваться на различных уровнях (см. таблицу ниже).

Национальный уровень	Государственная политика может распространять блокировку контента на весь входящий и исходящий трафик отдельно взятой страны. Для этого требуется надежный контроль над всеми межгосударственными каналами связи, реализуемый с помощью национального шлюза или брандмауэра. В некоторых случаях государство также принимает законы, обязывающие всех поставщиков телекоммуникационных услуг и интернет-провайдеров страны поддерживать подобный вид блокировки.
Уровень поставщика телекоммуникационных услуг и местного интернет-провайдера	Отдельные поставщики телекоммуникационных услуг, включая операторов мобильных сетей и традиционных интернет-провайдеров, также могут использовать свои средства блокировки.
Уровень местной сети	Ноутбуки и настольные ПК конечных пользователей обычно подключены не напрямую к оборудованию поставщика телекоммуникационных услуг, а к сетям предприятий, домохозяйств и учебных заведений. В местных сетях также может использоваться блокировка (как правило, определяемая задачами управления сетью и ее политикой безопасности, а не государственной политикой).
Уровень конечной точки	На компьютерах конечных пользователей может быть установлено ПО, принудительно реализующее политику блокировки. Такое ПО часто используется в домашних и корпоративных сетях для управления вычислительной сетью или родительского контроля.

Обратите внимание: если блокировка обусловлена требованиями законодательства, основные меры применяются на первых двух уровнях (т. е. в масштабах государства, в сфере ответственности операторов телекоммуникационных услуг и на уровне местных интернет-провайдеров)

Схема ниже содержит обзор возможных мест и разновидностей блокировки, используемых в каждом конкретном случае.

Разнообразие точек блокировки интернет-контента

Боковая колонка:
Блокировка контента на конечных точках

Настоящий документ посвящен вопросу блокировки интернет-контента по соображениям охраны правопорядка.

Однако важно помнить, что один из наиболее эффективных способов блокировки нежелательного контента — установка специализированного ПО на пользовательском устройстве. Такое устройство обычно называют «конечной точкой», поскольку оно является последним элементом подключения пользовательского устройства к Интернету. На большинстве компьютеров можно найти то или иное ПО для конечных точек, блокирующее вредоносное ПО (вирусы, трояны и фишинговые письма). Установкой этого ПО занимаются либо пользователи, либо специалисты службы ИТ-поддержки.

Есть и другие причины, по которым организации применяют ПО для блокировки контента на конечных точках. Например, библиотеки устанавливают такое ПО на общедоступных компьютерах, чтобы запретить детям просмотр порнографии. С помощью этих программных средств родители также могут ограничить своим чадам доступ к нежелательному контенту.

При блокировке контента на конечной точке могут использоваться многие из описанных в настоящем документе приемов, включая сканирование контента, категоризацию URL-адресов, блокировку по IP-адресу и перехват DNS-запросов. Как правило, блокировка и анализ осуществляются устройством, которое играет роль конечной точки. Однако разработчики такого ПО все чаще переносят сканирование контента и блокировку DNS в облако. В этом случае ПО на конечной точке лишь обслуживает взаимодействие с облаком. Более современные решения этого класса перенаправляют интернет-контент через облачную службу (полностью или частично). Перенос принятия решений в облако дает очевидные преимущества. Во-первых, можно отказаться от регулярного обновления конечных точек. Во-вторых, компьютер или смартфон пользователя перестают расходовать вычислительные ресурсы на оценку контента, которой теперь занимается масштабируемое облако. Впрочем, перенаправление трафика через сторонние решения создает проблемы конфиденциальности, поскольку контент становится доступен третьим лицам. Неудачная реализация этого механизма также влечет за собой проблемы, связанные с безопасностью.

Оценка видов блокировки контента

Пять рассматриваемых видов блокировки различаются по блокируемому контенту и механизму работы.

Ниже мы рассмотрим каждый из способов блокировки контента и оценим его эффективность по четырем критериям[3]

1. **Какие группы пользователей и интернет-служб затрагивает этот способ блокировки?** Каких групп пользователей и служб он не касается?

2. **Подходит ли выбранный способ для предотвращения доступа к отдельным видам контента?** Насколько велик косвенный ущерб от использования этого способа блокировки?

3. **Насколько эффективен этот способ блокировки контента?** Какие категории пользователей и поставщиков контента могут обойти эту блокировку?

4. **Какие побочные эффекты обычно вызывает этот способ блокировки?** Какие технические проблемы он вызывает? Какие проблемы нетехнического характера связаны с применением этого способа блокировки (например, снижение доверия и нарушение основных прав человека)?

3 Эти критерии взяты из документа Internet RFC 7754 под названием Technical Considerations for Internet Service Blocking and Filtering (Технические аспекты блокировки и фильтрации интернет-служб):

Блокировка по IP-адресу и протоколу

Блокировка по IP-адресу требует создания преград внутри сети (например, брандмауэров), которые блокируют весь трафик, передаваемый набору IP-адресов. Блокировка по протоколу опирается на использование низкоуровневых сетевых идентификаторов (таких как номер порта согласно протоколу TCP/IP), идентифицирующих конкретное приложение на сервере или разновидность протокола, используемого приложением. Это наиболее простые подходы к блокировке контента. Они блокируют не сам контент, а весь трафик, передаваемый известным IP-адресам или портам TCP/IP, а также протоколы, связанные с определенным контентом или приложением. Кроме того, блокировку по IP-адресу и протоколу можно реализовать с помощью ПО, установленного на компьютерах пользователей. Обычно это делается с целью защиты вычислительной сети.

Например, если стоит задача заблокировать весь контент, размещенный в вымышленной стране Элгания, можно заблокировать все известные IP-адреса серверов, на которых размещен контент. Аналогичным образом, если нужно заблокировать все службы VPN (используемые для шифрования трафика и скрывающие его источник и получателей), можно настроить блокировку отдельных протоколов, чтобы ограничить работу служб VPN, использующих известные протоколы и номера портов TCP/IP.

При блокировке по IP-адресу и протоколу блокирующее устройство содержит список блокируемых IP-адресов, называемый «черным списком». Предотвращаются любые попытки подключения к серверу, IP-адрес которого есть в черном списке.

При блокировке по IP-адресу и протоколу будет недоступен весь контент сервера, IP-адрес которого есть в черном списке (и «бомбы», и «котики»).

Соответственно, доступным окажется любой сервер, которого НЕТ в черном списке, независимо от контента на сервере.

Один из видов блокировки по IP-адресу — ограничение пропускной способности при передаче трафика. В этом случае трафик блокируется лишь частично. Пользователи воспринимают такую блокировку как замедление работы или нестабильность используемой службы. Подобная блокировка, незаметная для пользователей, отбивает у них желание использовать заблокированную службу, которая теперь кажется ненадежной. Она также может стимулировать пользователей к переходу на альтернативные службы. (Предприятия и интернет-провайдеры используют этот механизм для управления сетями и пропускной способностью каналов связи.)

Блокировка по IP-адресу и протоколу требует размещения специальных устройств между конечным пользователем и контентом. Блокирующая сторона (например, интернет-провайдер пользователя) должна полностью контролировать подключение конечного пользователя к Интернету. Если трафик пользователя идет в обход блокирующего устройства или пользователь скрывает истинный пункт назначения трафика (например, с помощью VPN), эта разновидность блокировки оказывается неэффективной.

Как правило, блокировка по IP-адресу является сравнительно неэффективным средством фильтрации. Его сложно поддерживать в актуальном состоянии и оно часто приводит к непреднамеренной блокировке ресурсов. Издатели контента могут легко обойти блокировку, переместив контент на новые серверы с новыми IP-адресами.

Кроме того, блокировка по IP-адресу невозможна, если поставщики информации пользуются сетями доставки контента (CDN). Эти сети постоянно меняют IP-адреса серверов, где расположены данные.[4] Сети CDN также используют одинаковые IP-адреса для обслуживания разных клиентов и выдачи различных видов контента. Применение подобного вида блокировки к сетям CDN часто приводит к большому количеству непреднамеренных перебоев в обслуживании клиентов.

Блокировка по IP-адресу и протоколу эффективна в отношении конкретных приложений, а не контента. Например, для блокировки VPN-трафика можно заблокировать используемые порты им TCP/IP и протоколы, а также IP-адреса известных общедоступных служб VPN. Этот способ широко используется и отличается высокой эффективностью.

Кроме того, наибольшая эффективность блокировки по IP-адресу достигается в том случае, если контент размещен на отдельном сервере, расположенном в конкретном центре обработки данных, или если нужно заблокировать ограниченное количество известных файлов. Блокировка по IP-адресу **недостаточно** эффективно воздействует на крупных поставщиков услуг хостинга, использующих множество различных центров обработки данных или применяющих сети распространения контента (CDN) для ускорения доступа.

4 Сеть распространения контента — это большая, географически распределенная сеть, серверы которой ускоряют доставку веб-контента пользователям Интернета. Крупные CDN состоят из сотен тысяч серверов, расположенных в различных странах мира. Эти серверы ускоряют доступ к контенту, размещенному клиентами сети. Серверы сетей CDN хранят копии контента, размещенного клиентами (тексты, изображения, аудио и видео). Эти серверы расположены в зонах активного обмена интернет-трафиком, благодаря чему запросы пользователей обрабатываются не централизованными серверами клиентов, а ближайшим пограничным сервером CDN.

Блокировка с помощью технологии DPI

DPI-блокировка предусматривает установку между конечным пользователем и Интернетом устройств фильтрации контента, реагирующих на ключевые слова, паттерны изображений или типы приложений. Эта разновидность блокировки сетевого трафика требует больших вычислительных мощностей и поэтому обходится весьма дорого. На соответствие правилам блокировки приходится проверять весь контент. DPI-блокировку также можно реализовать при помощи ПО, установленного на компьютерах пользователей. Обычно это делается с целью защиты вычислительной сети.

Эффективная DPI-блокировка требует наличия сигнатуры или иной информации о контенте. Для описания контента подходят ключевые слова, особенности трафика (например, размер пакетов и скорость передачи), имена файлов или прочие сведения, связанные с контентом. DPI-блокировка весьма эффективно используется для запрета отдельных приложений и обмена данными (например, для борьбы с пиринговыми файлообменными сетями или голосовым трафиком в IP-сетях [VoIP]), а также для блокировки отдельных разновидностей файлов (например, файлов мультимедиа).

При использовании технологии DPI блокирующее устройство содержит черный список контента. Обнаружение этого контента в трафике происходит путем сопоставления ключевых слов или иными способами, включая сравнительный анализ изображений. Предотвращаются любые попытки загрузки незашифрованного контента, совпадающего с контентом из черного списка.

При использовании технологии DPI возможны как ошибки первого рода (блокировка разрешенного контента), так и ошибки второго рода (пропуск запрещенного контента). Шифрование трафика затрудняет эффективное применение технологии DPI.

На этой схеме слово «бомба» заблокировано, поскольку оно совпадает с контентом. Однако слово «динамит» не подверглось блокировке, даже если оператор устройства DPI желал обратного, поскольку слово «динамит» не входит в черный список контента.

DPI-блокировка широко распространена в крупных предприятиях, использующих ее в системах защиты от утечки данных, в спам-фильтрах, в антивирусах и приложениях для защиты от вредоносных программ, а также для изменения приоритета отдельных типов трафика в ходе управления сетью (например, для приоритетной передачи данных, создаваемых корпоративными видеоконференциями). Однако ее также можно использовать для реализации требований к блокировке контента, предусмотренных государственной политикой. Например, использование сторонних служб VoIP, не связанных с национальным телекоммуникационным оператором, часто подвергается регулированию или ограничению. DPI-блокировка служит эффективным средством принудительной реализации подобных ограничений.

DPI-блокировка требует применения устройств, которые отслеживают и контролируют весь трафик между конечным пользователем и местом хранения контента. В этом случае блокирующая сторона (например, интернет-провайдер пользователя) должна полностью контролировать подключение конечного пользователя к Интернету. Практически повсеместное шифрование трафика ведет к неэффективности систем блокировки, использующих технологию DPI. Чтобы узнать подробнее об этой теме, обратитесь к боковой колонке справа под названием «Трудности, связанные с шифрованием, прокси-серверами и блокировкой».

Технология DPI эффективно блокирует определенные виды контента, которые можно выявить с помощью сигнатур или задать при помощи правил (например, «блокировать весь трафик VoIP»). С другими видами контента DPI-блокировка справляется заметно хуже (например, с ее помощью трудно заблокировать конкретные файлы мультимедиа или документы, содержащие заранее заданные ключевые слова). DPI-блокировка требует анализа всего трафика, получаемого конечным пользователем, поэтому она грубо нарушает тайну его частной жизни.

Общая эффективность DPI-блокировки колеблется в довольно широких пределах. Она зависит как от целей блокировки, так и от используемых средств DPI. Как правило, средства DPI наиболее эффективны при решении задач управления сетью и обеспечения безопасности. Они плохо подходят для реализации законодательных требований к блокировке контента.

Боковая колонка:
Трудности, связанные с шифрованием, прокси-серверами и блокировкой

Некоторые из рассмотренных в настоящем документе способов блокировки, включая технологию DPI и черные списки URL-адресов, имеют очень серьезные ограничения. Применение этих способов требует доступа к трафику. Сетевые устройства-посредники не могут надежно блокировать обмен данными, если пользователи обращаются к веб-серверам с поддержкой шифрования или шифруют трафик иным образом (как правило, с помощью встроенной в приложения технологии шифрования TLS/SSL). Пользователи могут с легкостью обойти другие способы блокировки, применив технологию VPN для шифрования обмена данными, скрытия истинных получателей трафика и его разновидностей. Ученые-исследователи и поставщики решений разработали методы определения видов трафика, однако они скорее напоминают игру в угадайку, чем глубокую аналитическую работу.

Согласно недавнему исследованию, по состоянию на февраль 2016 г. шифрование используется для защиты 49% всего объема интернет-трафика США. (см. http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf) Этот трафик абсолютно невидим для URL-блокировки и средств DPI, анализирующих контент. Единственная доступная информация об этом трафике — доменное имя сервера, где размещены данные. Уход трафика в тень стимулирует применение активной блокировки контента с помощью специальных прокси-серверов. Эти решения перехватывают и дешифруют трафик между устройством пользователя и веб-сервером, тем самым препятствуя комплексному шифрованию по протоколу TLS или SSL.

Использование прокси-серверов вызывает серьезную озабоченность, связанную с вопросами безопасности и конфиденциальности. Вмешательство в TLS/SSL шифрование дает блокирующей стороне доступ ко всем зашифрованным данным, однако может непредумышленно открывать доступ к этим данным для широкого круга лиц. Кроме того, прокси-сервер способен изменять передаваемый контент. Если блокирующая сторона имеет административный доступ к компьютеру пользователя (например, через корпоративную систему управления), такой прокси-сервер оказывается вполне прозрачным для пользователя. Впрочем, наличие прокси-сервера станет очевидным для конечного пользователя при обмене зашифрованным трафиком (TLS/SSL) и при некоторых других действиях. Как правило, в этой ситуации пользователь получает оповещение об использовании недоверенного сертификата. Кроме того, новые отраслевые стандарты и документы IETF (такие как HTTP Strict Transport Security [RFC6797], HTTP Public Key Pinning [RFC 7469] и DANE [RFC 6698]) и новые функции безопасности, реализованные в современных браузерах, заметно осложняют проксирование и дешифрование TLS/SSL трафика без участия пользователя.

Применяемые для блокировки контента прокси-серверы могут снижать пропускную способность при передаче трафика. В результате уменьшается производительность и надежность сетевых служб.

Блокировка по URL-адресу

Блокировка по URL-адресу используется весьма широко. Она может происходить как на компьютере пользователя, так и на сетевом устройстве, расположенном между пользовательским компьютером и Интернетом. Блокировка URL-адресов эффективна в отношении веб-приложений и не предназначена для блокировки других видов приложений (например, VoIP). При использовании URL-блокировки фильтр перехватывает веб-трафик (HTTP) и сравнивает отображаемый в HTTP-запросе URL-адрес с локальной или сетевой базой данных запрещенных адресов. В зависимости от полученного ответа фильтр URL-адресов разрешает или запрещает подключение к запрошенному веб-серверу.

Управление URL-адресами обычно осуществляется с помощью категорий, по которым они распределены для удобства (например, «спортивные сайты»). При необходимости можно заблокировать, ограничить или разрешить категорию целиком[5]. Если блокировка URL-адреса производится согласно требованиям законодательства, управление соответствующими интернет-службами и политиками блокировки обычно осуществляют органы власти. Фильтр URL-адресов может препятствовать прохождению трафика или перенаправлять пользователя на другую веб-страницу, где содержится меморандум о политике или уведомление о блокировке трафика. Принудительная блокировка URL-адресов в сети может осуществляться прокси-серверами, брандмауэрами и маршрутизаторами.

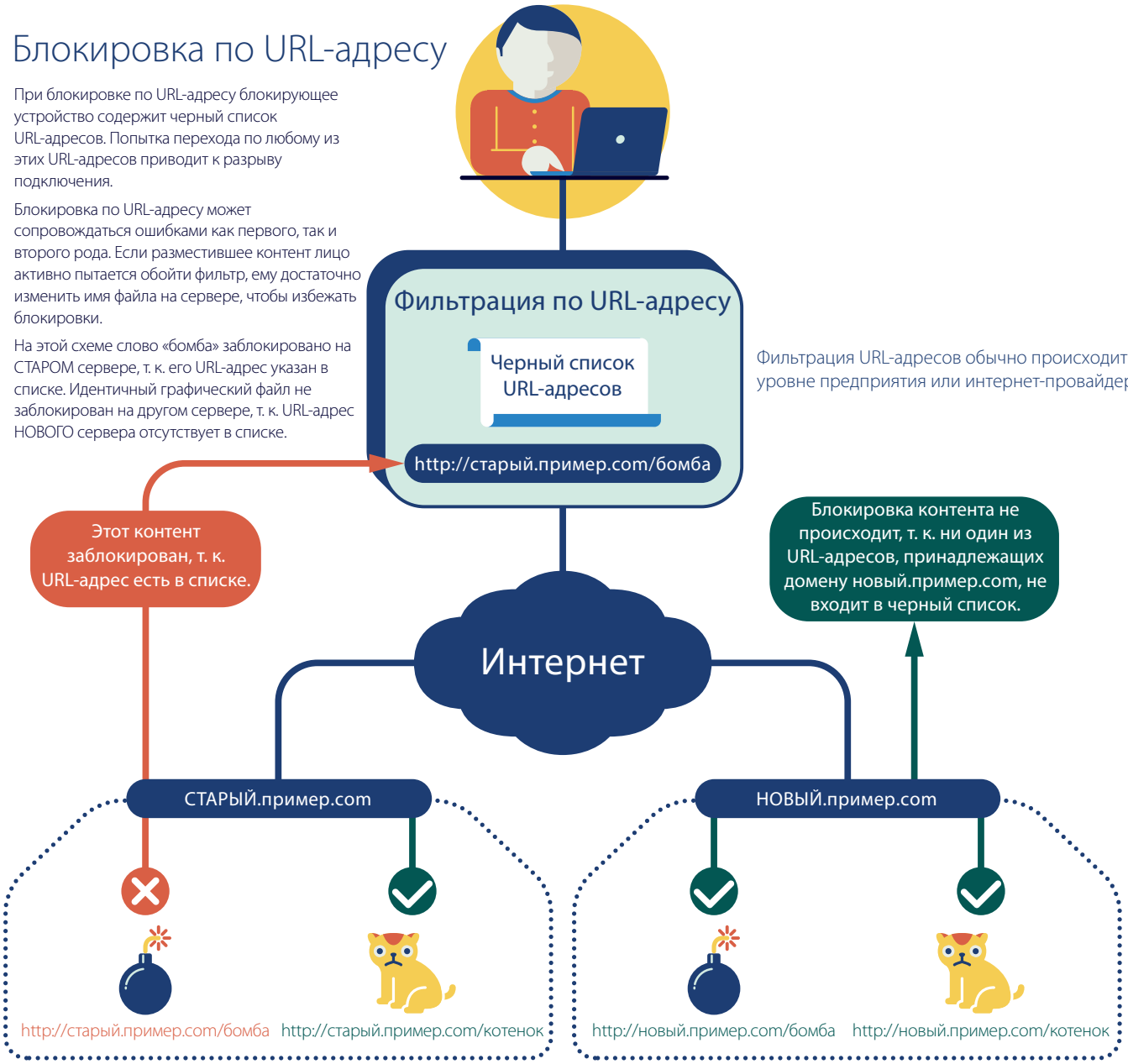
5 Созданием категорий фильтрации по URL-адресам занимаются поставщики услуг безопасности. Эти категории формируются по результатам автоматического сканирования веб-страниц и анализа их содержимого людьми. Большинство поставщиков услуг безопасности предлагают доступ к базам данных фильтрации URL-адресов, используемых для управления корпоративным сетевым трафиком. Эту услугу можно использовать и в иных целях (например, связанных с темой настоящего обзора).

Блокировка по URL-адресу

При блокировке по URL-адресу блокирующее устройство содержит черный список URL-адресов. Попытка перехода по любому из этих URL-адресов приводит к разрыву подключения.

Блокировка по URL-адресу может сопровождаться ошибками как первого, так и второго рода. Если разместившее контент лицо активно пытается обойти фильтр, ему достаточно изменить имя файла на сервере, чтобы избежать блокировки.

На этой схеме слово «бомба» заблокировано на СТАРОМ сервере, т. к. его URL-адрес указан в списке. Идентичный графический файл не заблокирован на другом сервере, т. к. URL-адрес НОВОГО сервера отсутствует в списке.



Фильтрация URL-адресов обычно происходит на уровне предприятия или интернет-провайдера.

Блокировка URL-адресов требует от блокирующей стороны (например, от интернет-провайдера пользователя) умения перехватывать трафик между конечным пользователем и Интернетом, а также управлять этим трафиком. Как правило, блокировка по URL-адресу обходится дорого. Чтобы обеспечить приемлемую эффективность, необходимо использовать достаточно производительное устройство фильтрации, перекрывающее канал связи между пользователем и Интернетом.

Считается, что блокировка по URL-адресу показывает высокую эффективность при выявлении контента, расположенного на различных серверах и доступного посредством разных служб. Очевидно, что URL-адрес не меняется даже при изменении IP-адреса сервера. В некоторых случаях блокировка по URL-адресу не приводит к полному прекращению обмена трафиком. Это происходит при использовании сложных или часто меняющихся URL-адресов. Такая ситуация может сложиться, если издатель контента активно принимает меры по обходу фильтрации URL-адресов. Иногда она возникает как побочный эффект работы современных систем публикации контента (например, применяемых для опубликования больших массивов данных в Интернете).

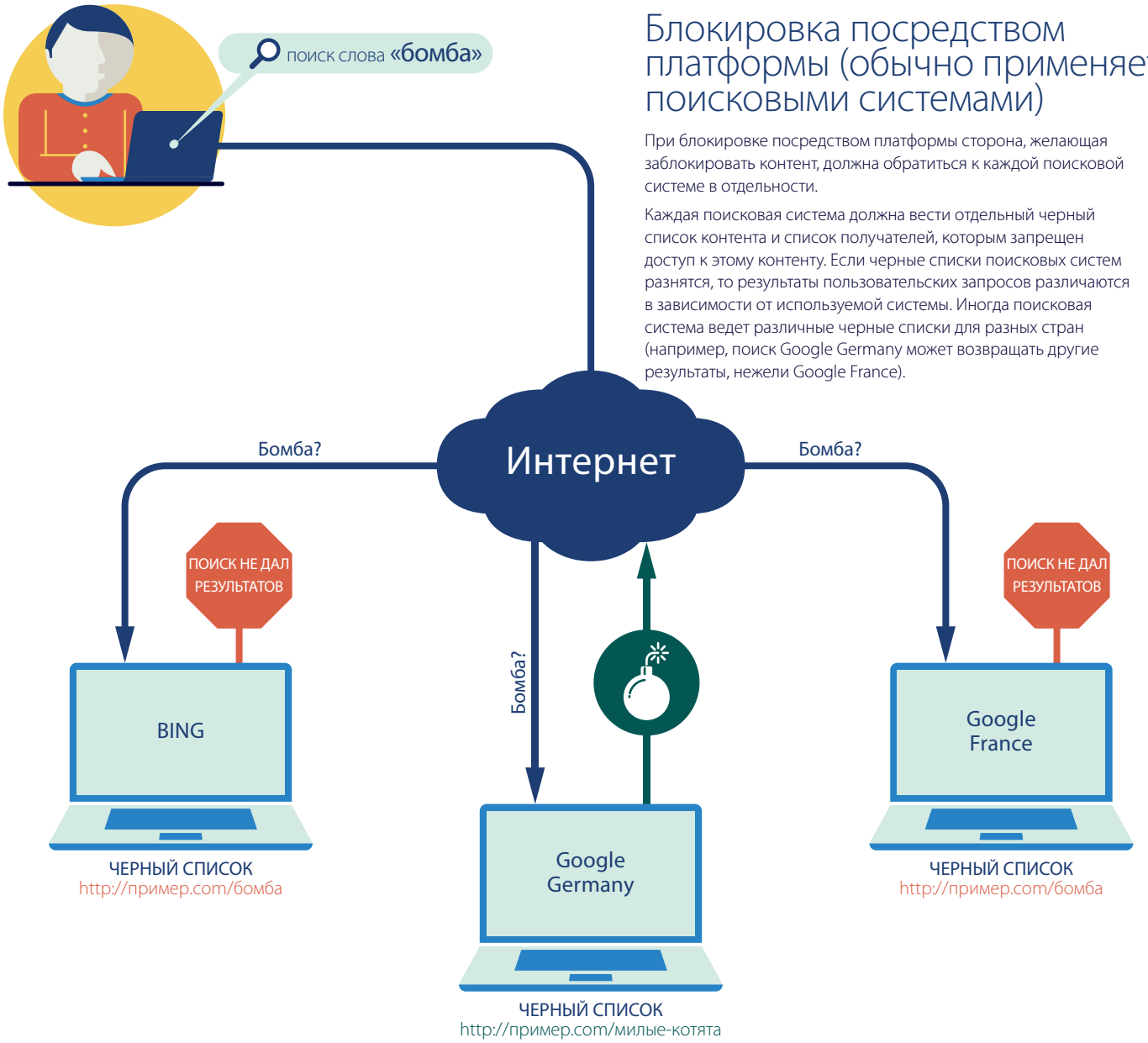
Как правило, блокировка URL-адресов успешно запрещает URL верхнего уровня (например, конкретные веб-страницы), однако ее эффективность сильно падает при работе с более длинными ссылками (например, на отдельные элементы содержимого веб-страниц). Эффективность блокировки по URL зависит от того, каким образом пользователь переходит к контенту. «Длинная ссылка», которую не воспринимает фильтр URL-адресов, откроет пользователю свободный доступ к контенту. Например, сайт Playboy содержит URL-адреса из домена playboy.com и встроенный контент, принадлежащий домену playboy.tv. Если URL-фильтр не содержит домен playboy.tv, видеоконтент этого сайта не будет заблокирован.

Эффективность любых видов URL-блокировки напрямую зависит от качества фильтра. Плохо продуманный или слишком широкий фильтр может блокировать разрешенный трафик либо иным образом снижать качество взаимодействия пользователей с Интернетом (например, увеличивать время загрузки веб-страниц и менять их форматирование в случае блокировки отдельных элементов страницы).

Блокировка URL-адресов и технология DPI требуют применения прокси-сервера, который умеет получать полный URL-адрес, если трафик зашифрован по протоколу HTTPS (TLS/SSL). Чтобы подробнее узнать о защите тайны частной жизни конечных пользователей, см. боковую колонку «Трудности, связанные с шифрованием, прокси-серверами и блокировкой» на стр. 15. При URL-блокировке зашифрованного трафика полный URL-адрес недоступен. Вместо него виден только IP-адрес сервера. В результате непреднамеренная блокировка происходит намного чаще. Прокси-серверы стоят дорого и затрудняют работу в Интернете для конечных пользователей, поэтому запрет URL-адресов плохо подходит для реализации законодательной блокировки.

Блокировка с помощью платформы (обычно используется поисковыми системами)

Органы государственной власти иногда обращаются к крупным поставщикам информационных услуг с требованием заблокировать какую-либо информацию для пользователей из конкретного региона, чтобы не ограничивать доступ к платформе в целом. Наиболее широко известна фильтрация с помощью платформ, используемых основными поисковыми системами и социальными СМИ. Недавно стало известно, что магазины мобильных приложений (например, Apple Store и Google Play) в рамках сотрудничества с властями отдельных стран блокируют загрузку некоторых приложений для местных жителей.



Блокировка посредством платформы (обычно применяется поисковыми системами)

При блокировке посредством платформы сторона, желающая заблокировать контент, должна обратиться к каждой поисковой системе в отдельности.

Каждая поисковая система должна вести отдельный черный список контента и список получателей, которым запрещен доступ к этому контенту. Если черные списки поисковых систем разнятся, то результаты пользовательских запросов различаются в зависимости от используемой системы. Иногда поисковая система ведет различные черные списки для разных стран (например, поиск Google Germany может возвращать другие результаты, нежели Google France).

Блокировка с помощью платформы требует содействия со стороны владельца самой платформы (например, оператора поисковых систем, такого как Google или Microsoft). Данный способ блокировки приводит к расхождениям в результатах поиска, выдаваемых в ответ на один и тот же запрос к поисковой системе, отправленный разными группами пользователей Интернета. Измененный список результатов не содержит ссылки на контент, который по тем или иным причинам считается сомнительным. В некоторых случаях список блокируемого контента определяется местным законодательством и требованиями государственных органов. Кроме того, оператор поисковой системы может самостоятельно заблокировать контент, который считает сомнительным. К примеру, поисковые системы иногда блокируют ссылки на вредоносные программы или на неприемлемый контент, нарушающий их условия обслуживания.

Блокировка средствами поисковой системы требует участия поставщика услуг поиска, поэтому применение этого способа блокировки ограничено двумя весьма узкими сценариями. Первый — создание правил для отдельных стран (блокировка контента согласно правилам, установленным для страны или региона). Второй — применение возрастных ограничений (блокировка материалов, неподходящих для детей).

Осуществляемая поисковой системой блокировка охватывает только ее пользователей и только в том случае, когда они подпадают под действие правил фильтрации. Применение технологии возрастной блокировки контента (например, SafeSearch),[6] предлагаемой крупными поисковыми системами и поставщиками контента, требует от пользователя предварительной регистрации.

Неэффективность блокировки контента средствами поисковой системы обусловлена тем, что она фильтрует не сам контент, а только ссылки на него. Среди нежелательных последствий подобной блокировки — привлечение внимания к заблокированному контенту. Разнообразие поисковых систем и альтернативных методов поиска контента заметно затрудняет принудительную реализацию этого способа блокировки.

Боковая колонка:
Блокировка на других платформах

Блокировка средствами поисковой системы является одной из наиболее популярных разновидностей блокировки. Впрочем, такой подход применяют и многие другие платформы, служащие для взаимодействия больших сообществ пользователей. Среди них можно выделить Facebook (1,5 млрд активных пользователей ежемесячно) и YouTube (более миллиарда уникальных пользователей). Сетевая блокировка и запрет URL-адресов с трудом справляются с блокировкой отдельных элементов контента (например, новостных статей). Органы власти отдельных стран не хотят создавать впечатление, будто собираются заблокировать тот же Facebook целиком. Поэтому они обращаются к владельцам крупных платформ с требованием фильтровать отдельные виды контента, которые считают нелегальными.

Блокировка контента средствами платформы отличается невыясненной эффективностью, масштабами и побочными эффектами. Отсутствуют какие-либо достоверные данные о результатах широкого применения этого способа блокировки на других платформах, кроме поисковых систем. Крупные платформы, такие как Facebook, YouTube и Twitter, всегда блокируют определенные виды контента (например, вредоносные программы и порнографию). Эти платформы поддерживают индивидуальные ленты пользовательского контента, однако не раскрывают подробностей его блокировки для жителей отдельных государств.

Низкая эффективность блокировки средствами поисковой системы ничуть не мешает властям различных стран брать этот способ на вооружение. Органы власти часто требуют от крупных поисковых систем создания особых фильтров, отвечающих местным нормативно-правовым требованиям (например, связанных с нарушением авторских прав или распространением информации о выступлениях, запрещенных законодательством страны). В частности, по данным Google в 2015 году корпорация получила 8 398 предписаний от 74 судебных органов разных стран, связанных с удалением 36 834 результатов поиска[7]. Физические лица также довольно часто просят защитить свои авторские права. Согласно Google, в июне 2016 года по требованию 6 937 владельцев авторских прав было удалено 86 миллионов результатов поиска[8].

Блокировку контента с помощью поисковых систем применяют и физические лица, использующие так называемое «право на забвение». За последние два года, с мая 2014 г. по июнь 2016 г., по запросам жителей разных регионов мира «заблокировано более одного миллиона URL-адресов».

6 SafeSearch — это технология крупных поисковых систем, таких как Google Search, Microsoft Bing и Yahoo!, применяемая для блокировки результатов поиска, содержащих «неуместные или откровенные изображения».

7 https://www.google.com/transparencyreport/removals/government/?hl=en

8 https://www.google.com/transparencyreport/removals/copyright/?hl=en

Блокировка контента по DNS

DNS-блокировка контента позволяет избежать проблем, характерных для других способов блокировки: высоких расходов и снижения производительности по причине фильтрации всего сетевого трафика. DNS-блокировка контента предусматривает изучение DNS-запросов и управление ими.

Этот способ блокировки требует применения особого DNS-рекурсора (см. боковую колонку «Обзор службы DNS»). Он решает сразу две задачи — выполняет поиск в DNS и проверяет наличие запрошенного домена в черном списке. Когда компьютер пользователя обращается к заблокированному имени, рекурсор возвращает неверную информацию (например, IP-адрес сервера с уведомлением о блокировке контента). Рекурсор также может возвратить ответ «Имя не существует». В результате пользователь лишается удобного доступа к контенту, размещенному под некоторыми доменными именами.

DNS-блокировка контента, равно как и любая другая сетевая блокировка, эффективна только в том случае, если блокирующая организация полностью контролирует сетевое подключение конечного пользователя. Если пользователь может выбрать другое сетевое подключение или использовать иной набор DNS-серверов, этот способ оказывается неэффективным. Например, когда Турция заблокировала некоторые DNS-запросы в 2012 г., пользователи перешли на общедоступные DNS-серверы Google, чтобы обойти блокировку. В ответ турецкие власти начали перехватывать весь трафик, передаваемый DNS-службе Google, что привело к заметному косвенному ущербу. DNS-блокировка контента требует применения брандмауэров или иных устройств, способных перехватывать DNS-запросы и перенаправлять их на особые DNS-серверы, осуществляющие блокировку. В противном случае, этот способ блокировки теряет эффективность.

Эффективность DNS-блокировки контента практически равнозначна блокировке по IP-адресу. Она работает несколько эффективнее, но лишь потому, что черный список доменных имен проще актуализировать. Кроме того, этот список оказывается точнее перечня IP-адресов при реализации большинства других способов блокировки контента. Однако данный способ имеет и слабые стороны. Легче изменить доменное имя, чем IP-адрес. В результате такую блокировку легко обходят как конечные пользователи, так и издатели контента.

Другая разновидность DNS-блокировки контента связана с отменой регистрации доменов и удалением имен из базы данных DNS. Этот способ блокировки труднее обойти, и причиняемый им косвенный ущерб не столь велик. Как правило, он зависит от эффективности международного сотрудничества, когда требование или судебное предписание исходит из иной юрисдикции, нежели юрисдикция местонахождения регистратора или реестра доменных имен.

DNS-блокировка контента и блокировка по IP-адресу имеют одинаковые недостатки: отдельно взятый сервер может содержать легальный и нелегальный контент одновременно, а также иметь один адрес (например, facebook.com). В результате блокируется весь размещенный на сервере контент, независимо от его легальности. Кроме того, изменение ответов на DNS-запросы может вызывать иные технические трудности, мешающие работе прочих разрешенных законодательством служб[9].

В основе DNS-блокировки контента также лежит допущение, что пользователь соблюдает обычные правила работы в Интернете и использует стандартную службу DNS для преобразования имен в IP-адреса. Пользователи с правами администраторов своих компьютеров, имеющие определенные технические навыки, могут отказаться от услуг стандартной службы DNS в пользу альтернативных служб. Кроме того, они могут использовать локальный список преобразования имен в адреса.

Боковая колонка: Обзор DNS

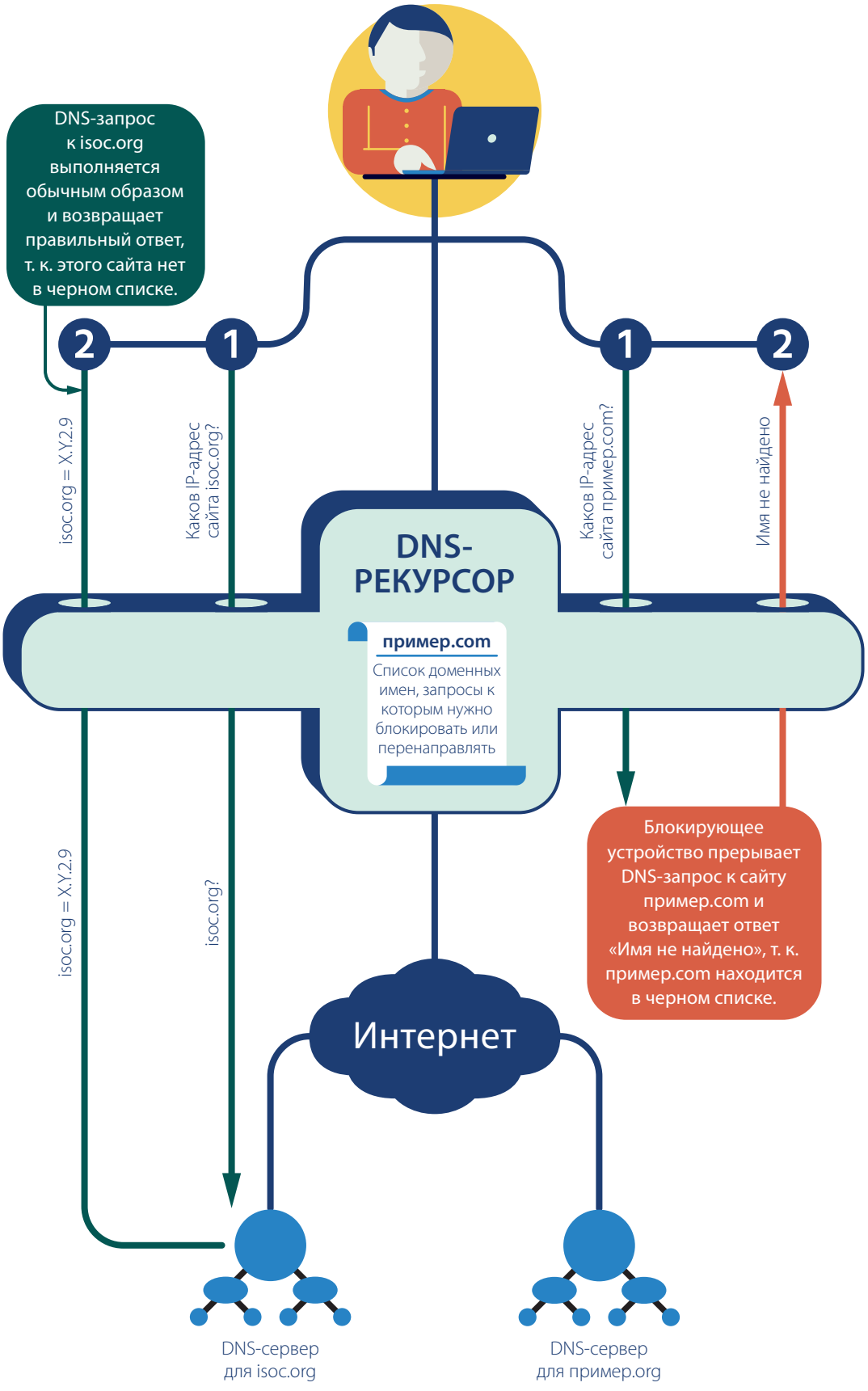
Архитектура DNS довольно проста. Эта система ищет текстовую строку, разделенную точками (доменное имя) в базе данных, распределенной по различным DNS-серверам. Строка может содержать подстроки, обозначающие протоколы (www), названия сайтов (isoc) и домены (org). Поиск доменного имени возвращает ответ (например, IP-адрес веб-сайта) или уведомление о том, что имя не существует.

Наиболее распространенный вид поиска в базе данных DNS — отыскание IP-адреса. Адрес ищется всякий раз, когда пользователь вводит URL в браузер. Приложения (например, браузеры) обычно отрабатывают не все этапы поиска. Вместо этого приложение обращается к посреднику под названием «рекурсор». В свою очередь, посредник ищет запрошенные сведения в распределенной базе данных DNS.

DNS-блокировка контента требует изменения обычного режима работы рекурсора.

9 Если вас интересуют подробности, советуем обратиться к отчету Internet Society под названием Perspectives on DNS Filtering (Перспективы DNS-фильтрации), размещенному по адресу https://www.internetsociety.org/internet-society-perspectives-domain-name-system-dns-filtering-0

Блокировка по DNS



При блокировке по DNS блокирующее устройство содержит черный список DNS-имен.

Как правило, подключение к Интернету требует преобразования DNS-имени в IP-адрес и обратно. Заблокировав запрос и вернув неверный ответ, мы тем самым отбиваем у пользователя желание получить блокируемый контент или подключиться к заблокированным службам другим способом (например, путем ввода IP-адреса в адресную строку).

Общие сведения о блокировке контента

Способы блокировки интернет-контента					
	Блокировка по IP-адресу и протоколу	**Блокировка с помощью технологии DPI**	**Блокировка по URL-адресу**	**Блокировка с помощью платформы (обычно производится поисковыми системами)**	**Блокировка по DNS**
Обзор	К сети подключается устройство, блокирующее трафик в зависимости от IP-адреса и приложения (например, работу VPN-клиента)	К сети подключается устройство, блокирующее трафик в зависимости от ключевого слова и (или) другого контента (например, имени файла)	К сети подключается устройство, перехватывающее веб-запросы и ищущее URL-адреса в черном списке	Сотрудничество с поставщиками приложений (например, поисковыми системами), позволяет адаптировать контент к местным требованиям	Локальная сеть или интернет-провайдер перенаправляют DNS-трафик на измененный DNS-сервер, блокирующий поиск некоторых доменных имен
Степень эффективности	IP-адрес легко сменить, контент легко перенести. **Этот способ блокировки ненадежен**. Он подходит только в том случае, если публикатор информации не принимает активных мер по обходу блокировки.	Эта блокировка весьма эффективна, если блокируемую информацию легко описать. Данный способ категорически не подходит для блокировки неопределенного контента (например, «заблокировать всю порнографию»). Его легко обойти путем **шифрования трафика.**	Этот распространенный способ **весьма эффективен при блокировке доступа к целым категориям** информации. Впрочем, новые и малоизвестные сайты легко проскальзывают сквозь этот фильтр, равно как и шифрующие трафик веб-серверы.	На рынке поисковых систем нет монополии, а предпочтения потребителей постоянно меняются, поэтому **данный способ блокировки малоэффективен и носит скорее декоративный характер**.	Издатели контента и конечные пользователи легко обходят DNS-блокировку. DNS-блокировка эффективна лишь при условии, что с каждым доменным именем связан небольшой объем блокируемого контента, и весь этот контент подлежит блокировке. **Этот способ неэффективен в силу технической сложности, чрезмерности блокировки и легкости обхода.**
Кого затрагивает?	Всех, чей трафик передается через устройство блокировки.	Всех, чей трафик передается через устройство блокировки.	Пользователей, чей трафик передается через устройство, предназначенное для перехвата и анализа трафика.	Пользователей поисковой системы, осуществляющей блокировку	Пользователей измененного DNS-сервера. Эту блокировку можно принудительно включить на уровне местной сети или поставщика услуг.
Точность блокировки	**Затрагивает весь контент на сервере (и легальный, и нелегальный).** Работает даже при шифровании данных.	**Затрагивает только контент, соответствующий правилам блокировки.** Требует применения прокси-серверов, умеющих работать с зашифрованными веб-страницами.	**Затрагивает отдельные веб-страницы и их элементы.** Требует применения прокси-серверов, умеющих работать с зашифрованными веб-страницами.	**Затрагивает отдельные веб-страницы и их элементы.** Обычно относится к отдельным URL-адресам.	**Затрагивает весь контент, отдаваемый с доменного имени (легальный и нелегальный).** Неэффективен при блокировке распределенного контента.
Краткое описание способа	Блокировка контента	Блокировка контента	Блокировка контента	Осложняет работу с контентом для пользователя	Осложняет работу с контентом для пользователя
Масштабы косвенного ущерба	Блокировка крупных серверов вызывает громадное количество ошибок первого рода (страдает и легальный, и нелегальный контент).	В зависимости от качества правил блокировки, количество ошибок первого рода может быть и очень большим, и крайне малым. Составление эффективных правил — сложная задача.	Как правило, фильтрация по URL-адресам требует использования коммерческих служб категоризации трафика. Она подходит для блокировки стандартных категорий сайтов, однако любая необычная блокировка приводит ко множеству ошибок.	Считается, что количество ошибок первого рода невелико, поскольку каждая страница блокируется по отдельному запросу. Из результатов поиска по запросу, связанному с нелегальным контентом, удаляется любая неуместная информация.	Указание доменных имен, принадлежащих крупным серверам, ведет к огромному количеству ошибок первого рода (блокировка легального и нелегального контента). Неэффективен при использовании сетей CDN (или вызывает слишком много ошибок первого рода).
Стандартные способы обхода блокировки	Публикаторы меняют IP-адреса, переносят контент или используют сети доставки контента (CDN). Пользователи VPN скрывают IP-адреса.	Применение многоуровневого шифрования эффективно решает проблему блокировки. В случае неудачных правил фильтрации небольшое изменение текста помогает обойти блокировку.	Применение многоуровневого шифрования эффективно решает проблему блокировки. Блокировка эффективно обходится с помощью нестандартного уровня обмена данными между приложениями.	Пользователи легко могут перейти на другую платформу (например, на другую поисковую систему).	Пользователи могут отказаться от локальных средств поиска в базе данных DNS или перенаправить запросы на стандартный общедоступный сервер (как правило, через VPN).
Побочные эффекты и технические неполадки	Актуализация длинных списков IP-адресов связана с трудностями и ошибками, требует кропотливого ручного труда. Сетевые устройства, реализующие этот тип блокировки, обычно отличаются высокой производительностью. Ее обычно всегда хватает.	Фильтрация контента путем анализа требует больших вычислительных ресурсов, поэтому неприменима во многих средах, в которых они отсутствуют. Применение прокси-серверов заметно снижает безопасность.	Фильтрация URL-адресов требует высокой производительности, снижает пропускную способность и надежность канала связи. Применение прокси-серверов заметно снижает безопасность.	Большинство поисковых систем уведомляют об удалении ссылок из результатов поиска. В результате контент можно отследить.	Развертывание модифицированного DNS-сервера снижает безопасность сети.

Заключение

Законодатели, рассматривающие возможность использования различных мер блокировки, интернет-евангелисты и все остальные пользователи, желающие внести свой вклад в улучшение применяемых подходов к блокировке контента, обязаны знать различные способы блокировки, а также прямые и косвенные последствия их применения.

Все способы блокировки имеют два общих недостатка:

1. **Они не решают проблему**

   Блокировка не удаляет контент из Интернета, не препятствует незаконной деятельности и не помогает преследовать преступников; она всего лишь скрывает контент от глаз широкой публики. Сам по себе контент никуда не исчезает.

2. **Они причиняют косвенный ущерб**

   Каждый способ блокировки и чрезмерен, и недостаточен одновременно — неизбежно блокируется разрешенный контент и пропускается запрещенный. Однако ущерб Интернету этим не ограничивается — блокировка увеличивает риски конечных пользователей, связанные с попытками обойти блокировку, снижает прозрачность Интернета, разрушает атмосферу доверия, загоняет интернет-службы в подполье и вторгается в частную жизнь пользователей. Кроме того, необходимо учитывать все затраты, связанные с блокировкой.

Боковая колонка:
Обход блокировки контента

Рассматривая вопрос блокировки интернет-контента, законодатели обязаны помнить об одной важной вещи — достаточно мотивированный пользователь способен обойти любые технические способы блокировки. Обход блокировки зачастую требует минимальных усилий.

Если трафик к отдельному узлу или доменному имени заблокирован, сеть VPN поможет скрыть трафик. Если трафик подвергается анализу, его всегда можно зашифровать, чтобы обойти блокировку. В случае удаления контента другие пользователи могут загрузить его на другие серверы. При удалении доменного имени пользователи сохраняют доступ к узлу, если знают его IP-адрес. Позже можно создать новое доменное имя взамен утраченного. Если ссылки удалены из результатов поиска в одной из поисковых систем, всегда найдутся другие.

Обходом блокировки занимаются не только конечные пользователи. Публикаторы информации также могут применять разнообразные методы обхода блокировки. Если публикатор активно и упорно распространяет контент, ему не сможет помешать никакая блокировка.

Рекомендации

По мнению специалистов Internet Society, наилучший способ борьбы с нелегальным контентом и незаконной деятельностью в Интернете — противодействие нарушителям на месте совершения преступления. Применение фильтров, блокирующих доступ к онлайн-контенту, следует признать неэффективным и не отвечающим поставленным задачам. Эти фильтры причиняют косвенный ущерб законопослушным пользователям Интернета.

Законодатели, озабоченные проблемой распространения нелегального контента через Интернет, должны обратить внимание на две основные стратегии:

1. **Решать проблему на месте возникновения. Наиболее щадящий для Интернета подход — убирать нелегальный контент оттуда, где он хранится, и бороться с незаконной деятельностью там, где она происходит.** Удаление нелегального контента из мест хранения и принятие принудительных мер против правонарушителей позволяет избежать негативных последствий блокировки контента и является более эффективным подходом к удалению нелегального контента[10]. Сотрудничество юрисдикций и заинтересованных лиц — залог успешного решения проблемы нелегального контента в Интернете, для которой не существует государственных границ и которую нельзя решить, опираясь на законы отдельно взятой страны.

10 Если орган власти и потребитель контента принадлежат к одной юрисдикции, проще удалить нелегальный контент из места хранения. Тем самым вы избежите трудностей и административных издержек, связанных с трансграничными юридическими мерами. Безусловно, глобальный охват Интернета усложняет задачу удаления контента из мест хранения. Поставщики и потребители контента зачастую находятся в разных юрисдикциях и подчиняются разным законам. Тем не менее, мы всегда должны отдавать предпочтение более эффективным решениям проблемы нелегального контента, которые не вредят Интернету.

2. **Правильно расставлять приоритеты и использовать альтернативные подходы. Некоторые обстоятельства допускают иные, более эффективные способы решения этой проблемы.** Приведем несколько примеров.
    - Эффективное сотрудничество поставщиков услуг, правоохранительных служб и органов государственной власти поможет защитить права лиц, ставших жертвами распространения нелегального контента, и принять меры в отношении нарушителей[11].
    - Улучшение саморегулирования требует создания доверительной атмосферы, в которой пользователям доступна информация о том, как отличить законную деятельность от незаконной и легальный контент от нелегального.
    - В некоторых случаях полезно создать для пользователей особые фильтры, которые они смогут установить на собственные устройства (например, средства родительского контроля). Подобные фильтры эффективно решат проблему нелегального контента и окажутся наименее разрушительными для Интернета в целом.
    - Некоторые веб-сайты (например, онлайн-казино), могут добровольно или для соблюдения законодательных норм включить геолокацию для предотвращения доступа из тех стран, где подобные услуги запрещены.

Минимизация негативных последствий

Все способы блокировки контента имеют серьезные недостатки, особенно если рассматривать их в контексте законодательной блокировки контента. Неэффективность этих способов очевидна, а методы обхода блокировки давно известны. Именно поэтому наряду с вышеуказанными причинами мы не рекомендуем использовать блокировку контента.

К сожалению, этот очевидный факт никак не препятствует применению описанных нами способов блокировки. Признавая реальное положение дел, мы предлагаем следующие рекомендации по уменьшению негативного воздействия блокировки:

а. Опробуйте все остальные варианты, кроме блокировки. Прежде чем использовать ее, нужно перебрать все доступные варианты решения проблемы с контентом на месте размещения. Необходимо опробовать все возможные альтернативы блокировке. Не делайте ставку на блокировку контента, руководствуясь исключительно удобством этой меры.

б. Обеспечьте прозрачность. Прозрачной должна быть не только блокировка, но и ее цели, задачи и политики. Органы власти должны сделать все возможное, чтобы затронутые блокировкой пользователи могли высказать озабоченность нарушением своих прав и законных интересов, а также утратой возможностей по причине блокировки.

в. Не забывайте о своей ответственности перед Интернетом. Блокирующая сторона должна помнить — она отвечает за функционирование всей глобальной сети. Ее действия не должны вредить стабильности, безопасности и отказоустойчивости Интернета. Распространенные приемы и методы блокировки ухудшают качество коллективного управления Интернетом и нарушают его функционирование. Этот ущерб бывает как прямым, так и косвенным. Например, в результате блокировки может возникнуть ситуация, когда пользователи мешают друг другу или нарушают личную безопасность друг друга.

г. Думайте глобально, действуйте локально. Локальная блокировка и фильтрация могут оказывать глобальное воздействие. Старайтесь блокировать контент как можно более локально, чтобы уменьшить негативное влияние блокировки на всемирную сеть. Лучше всего блокировать контент на конечной точке пользователя. Такая блокировка наиболее эффективна и причиняет минимум косвенного ущерба.

д. Привлеките к процессу всех заинтересованных лиц. Разработку и внедрение политик следует вести при участии широкого круга участников, включая специалистов по высоким технологиям, экономике и правам потребителей. Только так можно предпринять грамотные шаги, сводящие к минимуму негативные побочные эффекты блокировки.

е. Любые меры блокировки должны быть временными. Блокировку нужно снимать сразу после устранения ее причины. Чтобы обойти блокировку, владельцы нелегального контента часто практикуют его перемещение. Тем не менее, даже в этом случае государство не спешит отказываться от мер блокировки.

ж. Соблюдайте установленные законом процедуры. Любое предписание о блокировке нелегального контента должно опираться на требования законодательства, анализироваться независимыми экспертами и предназначаться для реализации законного решения узкой задачи. Необходимо отдавать предпочтение тем способам борьбы с незаконной деятельностью, которые меньше всего ограничивают права и свободы. Поставщики услуг доступа в Интернет и другие посредники при доступе к всемирной сети не должны де-факто становиться органами охраны правопорядка. Не следует возлагать на них обязанность определения законности или незаконности чьих-либо действий или контента.

11 Например, сотрудничество с предприятиями финансовой отрасли поможет эффективно выявлять и ограничивать незаконные транзакции.

Глоссарий

CDN

Сеть доставки контента или сеть распространения контента (CDN) — это глобальная распределенная сеть прокси-серверов, развернутых в различных центрах обработки данных. Задача CDN — обеспечивать высокую доступность и производительность при передаче контента конечным пользователям. Сети CDN обслуживают доставку значительной части содержимого современного Интернета, включая веб-объекты (текст, графику и скрипты), загружаемые объекты (файлы мультимедия, ПО, документы), приложения (системы электронной торговли, порталы), потоковое вещание (обычное и по запросу), а также социальные сети. (https://en.wikipedia.org/wiki/Content_delivery_network)

Контент

В контексте настоящего документа термин «контент» обозначает всю размещенную в Интернете информацию. Контент может представлять собой полный текст документа или его отрывок, изображение, видеоролик или звукозапись (например, подкаст). Контент может располагаться на веб-страницах, просматриваемых в браузере, или быть доступным с помощью специализированных инструментов (например, в особом приложении).

DNS

Система доменных имен (DNS) — это иерархическая децентрализованная система именования компьютеров, служб и других ресурсов, подключенных к Интернету или к частным сетям. Зарегистрировав доменное имя, физические и юридические лица могут предоставлять с его помощью доступ к различной информации. Система преобразует удобное для запоминания доменное имя в числовой IP-адрес, используемый в более низкоуровневых сетевых протоколах для обращения к службам и устройствам. Существующая с 1985 г. служба доменных имен, представляющая собой всемирный распределенный каталог, жизненно важна для функционирования Интернета. (https://en.wikipedia.org/wiki/Domain_Name_System)

DPI

Технология DPI описывает приемы и методы фильтрации сетевых пакетов путем изучения содержащихся в них данных (иногда и заголовка). Особое устройство анализирует передаваемые пакеты, выявляя несоответствие данных законодательным требованиям, обнаруживая вирусы, спам, признаки хакерского вторжения либо другие элементы. В зависимости от результатов анализа, пакет либо передается дальше, либо поступает в обработку (например, отбрасывается). (https://en.wikipedia.org/wiki/Deep_packet_inspection)

Нелегальный (незаконный)

В контексте настоящего документа термины «нелегальный» и «незаконный» применяются для описания контента, запрещенного на территории отдельно взятой страны, независимо от причины. Причиной запрета может служить нарушение авторских прав или кража интеллектуальной собственности (например, распространение незаконно скопированного фильма). Нелегальным может быть и неприемлемый с нравственной точки зрения контент (например, непристойные изображения или детская порнография). В некоторых случаях контент признается нелегальным, если власти страны хотят ограничить его распространение или считают его оскорбительным (например, запрещают мультфильм, который выставляет президента страны в неприглядном свете). Отметим, что нелегальный в одной юрисдикции контент вполне может быть легальным в другой. Иногда легальность контента зависит не от юрисдикции, а от контекста. Например, детям нельзя показывать непристойные комедии — это незаконно. Если же эту комедию смотрят взрослые, требования закона соблюдены.

IP-адрес	IP-адрес — это идентификатор, назначаемый каждому компьютеру и устройству (например, принтеру, маршрутизатору, мобильному устройству и т. п.), подключенному к Интернету. Он используется для поиска и идентификации узлов при обмене данными между узлами вычислительной сети. (https://en.wikipedia.org/wiki/IP_address)
Ошибка второго рода	Ошибка второго рода происходит в том случае, если не блокируется контент, который нужно блокировать. Например, когда блокирующее устройство разрешает подключение к интернет-магазину запрещенных препаратов, поскольку адрес этого сервера отсутствует в черном списке. Здесь мы имеем дело с ошибкой второго рода.
Ошибка первого рода	Ошибка первого рода происходит при блокировке разрешенного контента. Например, порнографический фильтр может запретить доступ к рецептам горячих пышек, если ключевые слова подобраны неудачно. Это считается ошибкой первого рода.
TLS/SSL	Transport Layer Security (TLS) и его предшественник Secure Sockets Layer (SSL) — это криптографические протоколы, обеспечивающие защиту при обмене данными в вычислительных сетях. Оба протокола чаще всего называют просто SSL. Особенно широко распространены несколько версий этих протоколов, используемые при просмотре веб-сайтов и обмене электронной почтой, для отправки факсов и мгновенных сообщений через Интернет, а также для поддержки голосовой связи в IP-сетях (VoIP). Протокол TLS применяется для защиты обмена данными между серверами и браузерами. TLS обеспечивает конфиденциальность и целостность данных, которыми обмениваются приложения. (https://en.wikipedia.org/wiki/Transport_Layer_Security)
URL	Uniform Resource Locator (URL), обычно называемый веб-адресом — это ссылка на веб-ресурс, описывающая его расположение в сети и механизм получения. Как правило, URL-адреса используются для создания ссылок на веб-страницы (https), однако могут применяться и для обмена файлами (ftp), для отправки и получения электронной почты (mailto), при доступе к базам данных (JDBC) и для решения других задач. В большинстве браузеров URL-адрес веб-страницы отображается в адресной строке, расположенной над страницей. Типичный URL-адрес имеет следующий вид: https://www.пример.com/index.html. В него входит обозначение протокола (https), доменное имя узла (www.пример.com) и имя файла (index.html). (https://en.wikipedia.org/wiki/Uniform_Resource_Locator)
VPN	Виртуальная частная сеть (VPN) служит для создания частных сетей внутри общедоступных (например, в Интернете). С ее помощью пользователи могут обмениваться данными в общих или публичных сетях, словно их вычислительные устройства напрямую подключены к частной сети. VPN открывает для приложений все преимущества частных сетей — обширные функциональные возможности, надежная безопасность и развитые средства управления. (https://en.wikipedia.org/wiki/Virtual_private_network)

Рекомендуемая литература

Если вам нужна дополнительная информация по этой теме, советуем ознакомиться со следующими публикациями.

Техническая документация целевой инженерной группы Интернета (IETF)

Статья A Survey of Worldwide Censorship Techniques (Обзор приемов и методов цензуры в разных странах мира) — черновой документ IETF, draft-hall-censorship-tech-04
https://tools.ietf.org/html/draft-hall-censorship-tech-04

Technical Considerations for Internet Service Blocking and Filtering (Технические аспекты блокировки и фильтрации интернет-служб) — RFC 7754
https://tools.ietf.org/html/rfc7754

Политики, опросы и справочные документы

Статья Filtering, blocking and take-down of illegal content on the Internet (Фильтрация, блокировка и удаление нелегального контента из интернет-ресурсов), Совет Европы, 2015 г.
http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet

Freedom of Expression Unfiltered: How blocking and filtering affect free speech (Фильтрация и свобода самовыражения: влияние блокировки и фильтрации на свободу слова), правозащитная организация Article 19, 2016 г.
https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf

Аналитический обзор Freedom on the Net 2016 (Свобода в Интернете по состоянию на 2016 г.), правозащитная организация Freedom House, ноябрь 2016 г.
https://freedomhouse.org/report/freedom-net/freedom-net-2016

Статья Internet Society Perspectives on Domain Name System (DNS) Filtering (Взгляд Internet Society на перспективы функционирования службы DNS), Internet Society, 2012 г.
https://www.internetsociety.org/sites/default/files/Perspectives%20on%20Domain%20Name%20System%20Filtering-en.pdf

Статья Network Neutrality (Сетевая нейтральность), Internet Society, 2015 г.
http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-NetworkNeutrality-20151030.pdf

Perspectives on Policy Responses to Online Copyright Infringement (Перспективы законотворческого реагирования на нарушение авторских прав в Интернете), Internet Society, 2011 г.
https://www.internetsociety.org/sites/default/files/bp-copyrightpolicy-20110220-en-1.pdf

Благодарности авторов

Международная организация Internet Society выражает Джоэлю Снайдеру из компании Opus One сердечную благодарность за подготовку настоящего документа.

Настоящий отчет составлен под руководством Николаса Сейдлера и Андрея Робачевского из Internet Society.

В отчет также вошли обзоры и комментарии других сотрудников Internet Society, участвовавших в его создании: Констанс Боммлаер, Салли Вентворт, Олаф Колкман, Карл Ганберг, Кристина Руннегар, Константинос Комаитис, Лиа Кисслинг, Джойс Доньез, Кевин Крамер, Бастиан Кваст, Кевин Чеге, Дэн Йорк, Ракель Гатто.

Выражаем особую благодарность рабочей группе Internet Society по связям с общественностью, усилиями которой был сверстан, оформлен и прорекламирован этот документ. Состав рабочей группы: Джеймс Вуд, Бет Гомбал, Лиа Кисслинг и Алессандра Десантиллана.

И наконец, мы благодарим всех, кто внес значительный вклад в доработку этого документа: участников клуба Internet Society Chapter, рядовых членов нашей организации и ее руководителей, а также прошлых и настоящих членов опекунского совета Internet Society за их неоценимый вклад.

internetsociety.org

Galerie Jean-Malbuisson 15,
CH–1204 Женева, Швейцария
Тел.: +41 22 807 1444

1775 Wiehle Avenue, Suite 201
Рестон, Вирджиния 20190, США
Тел.: +1 703 439 2120