Шинелин Н.В. Развитие регулирования мобильного доступа к сети Интернет [Электронный ресурс] // Информационно-экономические аспекты стандартизации и технического регулирования: Научный интернет-журнал. 2013. – № 6(16). Режим доступа http://iea.gostinfo.ru/files/2013_06/2013_06_08.pdf

УДК 338.47

# РАЗВИТИЕ РЕГУЛИРОВАНИЯ МОБИЛЬНОГО ДОСТУПА К СЕТИ ИНТЕРНЕТ

***Шинелин Н.В.**, аспирант ГАОУ ВПО «Московский городской университет управления Правительства Москвы»*

*В статье рассмотрено развитие регулирования мобильного доступа к сети Интернет. Уточнены методы реализации требований современного российского законодательства с помощью технологии DPI. Рассмотрены вопросы регулирования применения технологии DPI и охраны права клиентов на приватность.*

**Ключевые слова:** Интернет, регулирование, приватность, DPI.

UDC 338.47

# REGULATORY DEVELOPMENT OF MOBILE INTERNET ACCESS

***Shinelin N.V.**, post-graduate student at GAOU VPO «The Moscow City University of Management of Moscow Government»*

*The article discusses the development of regulation of mobile access to the Internet. Refined methods of implementing the requirements of the modern Russian legislation with the help of technology DPI. The problems of regulating the use DPI technology and protection of the right to privacy of customers.*

**Keywords:** Internet, regulation, privacy, DPI.

С начала 2014 года в Федеральный закон «Об информации, информационных технологиях и защите информации» № 149-ФЗ планируется внести изменения, направленные на повышение оперативности реагирования на возникающие угрозы гражданам в сети Интернет. Так, в статье 15.3 «Порядок ограничения доступа к информации, распространяемой с нарушением закона»

будут описаны условия и непосредственно процедура ограничения доступа, которая в графическом виде представлена на рисунке 1. К числу таковой относится информация,

«- содержащая призывы к массовым беспорядкам;

- содержащая призывы к осуществлению экстремистской деятельности;

- содержащая призывы к участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка».

Основанием для инициации процедуры проверки и в случае необходимости ограничения ресурса является обращение граждан о наличии такого рода информации на данном ресурсе. Помимо пользователей такие обращения могут поступать со стороны «федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций». Обращение направляется в адрес Генерального прокурора Российской Федерации либо его заместителей, далее – в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), которая является уполномоченным государственным органом, осуществляющим контроль в области массовых коммуникаций, реализующим требование о принятии в установленном прядке мер по ограничению доступа к ресурсу либо части ресурса, где находится противозаконная информация такого рода. После получения соответствующего требования Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций оперативно направляет операторам связи требование об ограничении доступа к ресурсу. Одновременно устанавливается провайдер, владелец ресурса где информация размещена (и, соответственно, созданы условия для размещения такого рода информации), и непосредственно, лицо разместившее информацию. В требовании указывается доменное имя, адрес в сети Интернат, где отмеченная информация размещена.

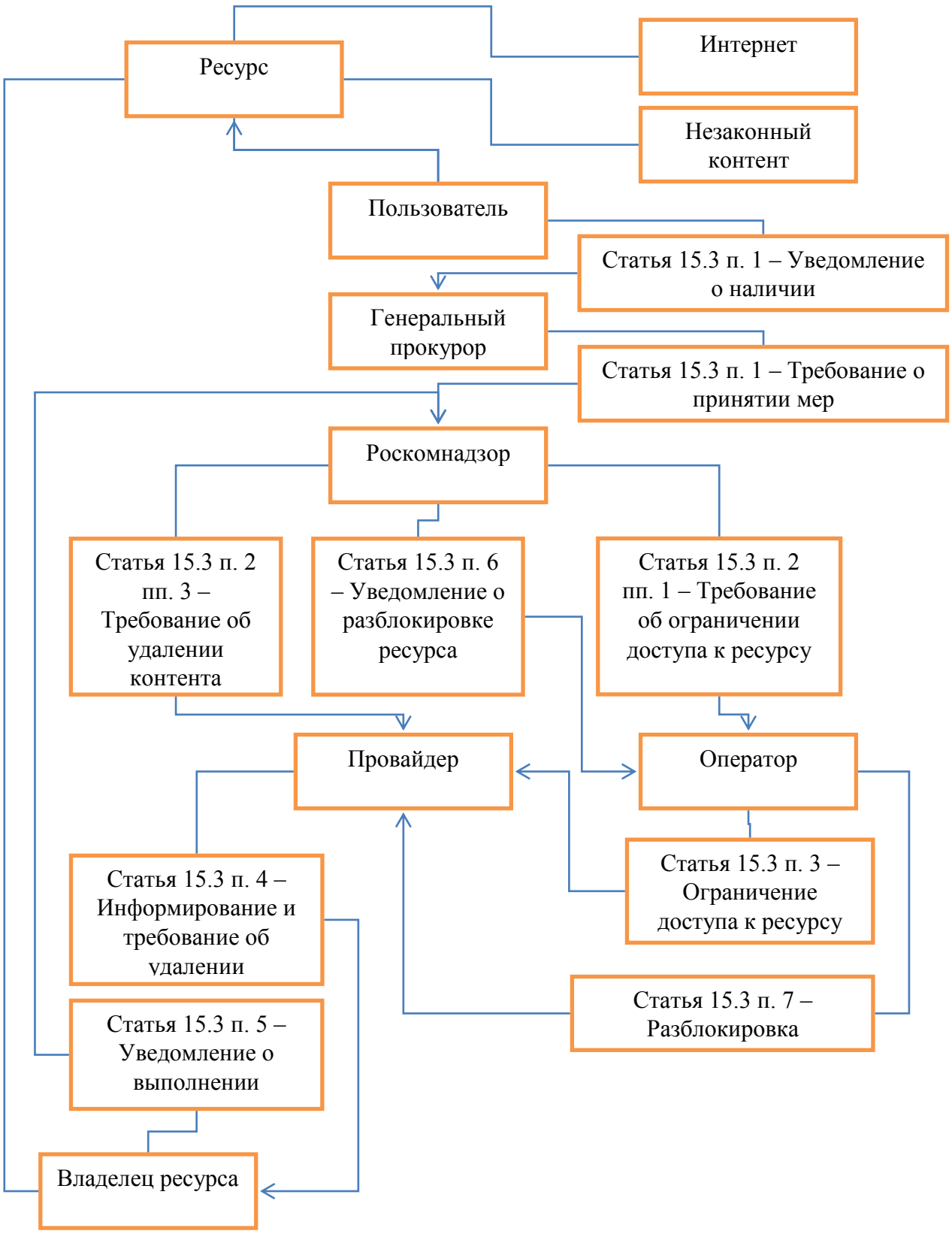


Рис. 1. Порядок ограничения доступа к информации, распространяемой с нарушением закона

http://iea.gostinfo.ru/files/2013_06/2013_06_08.pdf

При получении описанного требования провайдер обязан их незамедлительно выполнить. В течении 24 часов весь ресурс либо его часть, где размещена информация, должны быть удалены владельцем ресурса из сети Интернет.

В случае выполнения владельцем ресурса выданных ему предписаний он направляет соответствующее уведомление в Роскомнадзор. После этого Роскомнадзор, удостоверившись в выполнении предписаний, направляет оператору связи уведомление, разрешающее восстановить доступ к данному Интернет-ресурсу. Соответственно, после получения от Роскомнадзора уведомления оператор восстанавливает доступ к ресурсу либо к его блокированной части.

Корректное выполнение требований органов государственной власти требует от провайдеров закупки весьма дорогостоящего оборудования, реализующего функции Deep Packet Inspection (сокр. DPI) – технологии накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому и по косвенным статистическим признакам, поскольку без применения указанной технологии невозможно отдельно заблокировать конкретную страницу с запрещенным контентом, что приводит к необходимости блокировать весь ресурс по его ip-адресу, если же сайт с противоправным контентом находится на разделяемом хостинге (что является весьма распространенной ситуацией), то блокировка одного запрещенного ресурса требует блокировки и других ресурсов с данным адресом, что наносит серьезный ущерб законным интересам их владельцев и читателей. Кроме того, данный прием может даже использоваться злонамеренно для временной парализации деятельности тех или иных сайтов путем размещения на ресурсе с тем же ip-адресом заведомо противоправного контента.

6 декабря 2012 года представители 159 стран на конференции Международного союза электросвязи ООН в Дубае по инициативе Китая

официально утвердили стандарт Y.2770 по глубокой инспекции пакетов (Deep Packet Inspection, DPI), подробности которого по настоящее время остаются конфиденциальными (вопросы официального опубликования стандартов обсуждаются в [1]).

Приобретение оборудования DPI является крайне затратным: по некоторым оценкам, для магистрального провайдера федерального уровня стоимость составляет порядка 2 млрд. долл.

Основные сотовые операторы России внедрили DPI в 2009 (ОАО «МегаФон», оборудование Huawei), 2010 (ОАО «МТС», оборудование Cisco) и 2011 (ОАО «Билайн», оборудование Procera) годах. Они могут использовать DPI в том числе для подавления peer-to-peer и VoIP-сервисов. Ростелеком планирует внедрить DPI для мобильного Интернета в 2014 году [3].

Однако следует учесть, что оборудование DPI непрерывно развивается для повышения качества работы и точности распознавания передаваемого контента, в том числе в ответ на появление новых методов его маскировки.

Инновации в области DPI технологий позволяют значительно повысить качество защиты клиентов от противоправной информации, однако, с другой стороны, создают угрозу вмешательства в их частную жизнь. Дискуссии вокруг оправданности и допустимых границ применения технологий DPI, с учетом перспектив ее развития, в настоящее время находятся в центре внимания широкой аудитории с научной и практической точки зрения.

Как показывает практика, единственно правильной стратегией применения DPI является интеграция технологических и социальных инноваций в данной области. С точки зрения технологии решения DPI позволяют осуществлять весьма глубокий и разносторонний контроль за деятельностью клиента мобильного оператора в сети Интернет. В некоторых случаях их применение не имеет альтернатив (например, для распознавания и понижения приоритета торрент-трафика, негативно сказывающегося на пропускной

способности сети для остальных ее участников). Однако применительно к защите пользователей от противоправного контента эффективность и минимизация негативных побочных эффектов от применения DPI зависит, во-первых, от лиц, принимающих решения по заданию руководящих правил и, во-вторых, от разделения функций между автоматизированной и ручной блокировкой.

Практика показывает, что перманентно возрастающая часть угроз, связанных с противоправным контентом, находится в рамках глобальных социальных сетей, политика управления контентом которых не соответствует требованиям российского законодательства. В связи с этим возможно лишь реактивное реагирование – блокировка отдельных страниц данных ресурсов по факту выявления противоправного содержимого, что является весьма трудозатратным и недостаточно эффективным. В то же время социальные сети, которые предлагается формировать в рамках отечественных мобильных провайдеров на базе их VOIP-служб и рекомендательных сервисов, встроенных в системы распространения контента, отличаются возможностью проактивного контроля. Во-первых, их пользователи однозначно идентифицируются при приобретении SIM-карт. Во-вторых, в подобные сети можно изначально встроить меритократический механизм оценки безопасности контента, аналогичный известному сервису WOT (web on trust), но учитывающий особенности отечественного законодательства Для этой цели необходимо сотрудничество операторов мобильного Интернета с организациями, подобными Лиге безопасного Интернета с ее проектом «Кибердружина» (см. рис. 2).

Еще одним важным аспектом регулирования инновационных технологий в области мобильной связи является выработка государственных правил разрешенного отклонения от «сетевой нейтральности», не допускающих разрыва единого информационного пространства за счет полного блокирования

сторонних сервисов, и стандартизация правил раскрытия информации операторами в данной области, повышающая транспарентность рынка услуг сотовой связи и снижающая информационную асимметрию клиентов и операторов.


Примечание:

1 – выставление оценок клиентами различным аспектам безопасности ресурсов контаков в социальных сетях;

2 – автоматизированное ранжирование клиентов-экспертов по качеству их оценок;

3 – запросы к профессиональным экспертам по оценке ресурсов, выделенных как подозрительные;

4 – инициативные сообщения профессиональных экспертов о противозаконном контенте;

5 – прямые оценки репутации добровольных экспертов из числа клиентов профессиональными экспертами;

6 – прямые сообщения о критических нарушениях закона;

7 – решения комиссии о выработке правил DPI.

Рис. 2. Меритократическая система задания правил фильтрации Интернет-контента

Данная задача может быть решена как «сверху», принятием государственного решения, так и в порядке взаимодействия императивного и диспозитивного подходов: разработкой и распространением отдельными провайдерами лучших практик в этой области, созданием добровольных отраслевых стандартов и последующим санкционированием их государством [4].

Это особенно важно, учитывая олигополистическое строение рынка сотовой связи (в некоторых местностях, применительно к высокоскоростной передаче данных – монополистическое).

## Список использованной литературы

1. Коровайцев А.А., Ломакин М.И., Докукин А.В. Нормативно-правовое регулирование распространения стандартов на платной основе. Современное состояние // Стандарты и качество, 2013. – № 12. – С. 36-39.
2. Интернет-фильтрация в России: еще и слежка [Электронный ресурс] // Режим доступа: http://www.forbes.ru/tehno/194198-internet-filtratsiya-v-rossii-eshche-i-slezhka
3. Докукин А.В., Ломакин М.И. Интеграция российских инновационных предприятий в мировую экономику на основе развития информационного обеспечения стандартизации // Российское предпринимательство, 2012. – № 2.