**Опыт проведения мониторинга сетей WI FI в местах общего пользования**

**(Слайд 1)**

Здравствуйте уважаемые коллеги!

Мы с Вами коллеги, потому что, у Роскомнадзора и операторов связи общая задача – это обеспечение оказания качественных услуг населению в соответствии с действующим законодательством.

В настоящее время одна из острых проблем это блокировка запрещенных ресурсов операторами связи и пути ее обхода абонентами.

Почему этот вопрос крайне важен для операторов. На сегодняшний день законодательно за данное нарушение ответственность абонента не определена. И если выход на запрещенный сайт состоялся, даже по причине действий абонента, ответственность все равно несет оператор связи и свою правоту вам приходится доказывать в долгих судебных разбирательствах, что, я думаю, мало кому интересно.

**(Слайд 2)**

Одним из важных моментов доступа на запрещенные сайты является доступность информации в сети Интренет, где можно найти множество «Пособий» по обходу блокировок оператора связи.

Также имеются списки открытых прокси-серверов, использование которых позволяет выйти на любой запрещенный сайт.

Отсюда можно сделать вывод, что для грамотных абонентов, не составит труда достичь желаемого результата. Однако, таких пользователей сети «Интернет», как показывает статистика, значительно меньше, чем обычных, попадающих на запрещенные сайты непреднамеренно.

Поэтому и подготовлен сегодняшний доклад, чтобы мы вместе нашли пути решения проблемы и приняли меры, чтобы оградить от незаконной информации в первую очередь таких абонентов, среди которых могут оказаться дети и подростки.

**(Слайд 3)**

Причины не блокирования запрещенных ресурсов могут быть как в зоне ответственности оператора связи, так и в зоне ответственности абонента.

**(Слайд 4)**

Рассмотрим подробнее в каких случаях происходит не блокировка

1. Применяемые программные решения по блокированию запрещенных ресурсов оператора связи.

Учитывая желание сэкономить, большинство операторов связи используют различные программные средства, разработанные самостоятельно или сторонними организациями. Эти программные средства постоянно находятся в стадии доработки и отладки. В связи с чем, максимальное количество ошибок в работе систем фильтрации, случаев неблокирования возникает именно при применении «самоделок».

2. Абонент или оператор связи использует прокси-сервер. Страница попала в КЭШ–прокси до внесения сайта в реестр запрещенных. Список открытых прокси-серверов можно найти с сети «Интернет» в свободном доступе.

3. Абонент использует VPN канал.

4. Преднамеренное или случайное изменение DNS сервера абонента.

Особенностью блокирования по доменным именам является обязательность настройки оборудования абонента на DNS-сервер оператора. В случае если при настройке сети на абонентском оборудовании устанавливается галочка "получить настройки DNS-сервера автоматически", то всё хорошо, но если эти настройки устанавливаются вручную, система блокировки оператора работать не будет. Более того, многие программные продукты рекомендуют абоненту использовать различные публичные DNS-сервера, в частности, Google и Verizon, мотивируя это оптимизацией работы и якобы повышением защищенности. Большинство "непродвинутых" пользователей соглашается с такими предложениями.

5. Использование IP-протокола 6-ойверсии (IPv6).

Способ IPv6 подразумевает, что провайдер предоставляет доступ абоненту к сети Интернет по IPv6, а запрещенный ресурс размещается с поддержкой этого протокола. Например, rutracker.org. Т.к. все базы в так называемой “Информационной системе взаимодействия” поддерживают только 4ую версию протокола IP, то заблокировать доступ к таким ресурсам на уровне провайдера, на данный момент, может позволить себе далеко не каждый провайдер. Блокировка же будет заключаться в установке DPI2 с поддержкой IPv6, который будет заглядывать в каждый пакет, а не только в те, что присутствуют в фильтрах. Однако, стоит заметить, что IPv6 в настоящее время не очень распространен, и лишь небольшой список провайдеров его поддерживают. По данным RIPE это около 12%

6. Использование различных браузеров с разного рода «новшествами». Режимы "Турбо" и "Безопасный WiFi" в Яндекс. Браузере, режим экономии трафика в браузере Google Chrome и т.д.

Отмечу функцию «Безопасный WiFi» Яндекс. Браузера. Мало кто из пользователей откажется от предложения обеспечить безопасное соединение по WiFi. При активации трафик со всех сайтов, где используется обычный HTTP, проходит через сервер Яндекса. Фактически сервер выступает в роли шлюза – Яндекс. Браузер подключается к нему по защищенному HTTPS-протоколу, и обмен информацией между устройством пользователя и сайтом происходит через это надежно зашифрованное подключение. Итог – ресурс доступен.

**(Слайд 5)**

Далее рассмотрим возможные методы борьбы с незаблокированными запрещенными ресурсами, существующие на сегодняшний день.

 Блокирование сайтов непосредственно операторами связи.

Как показывает практика, операторы связи используютразные подходы к методам блокировки:

- Блокировка по IP адресу. Это наиболее простой метод, соответственно у него и самые большие недостатки. При блокировании по IP заблокированными оказывается много иных ресурсов, которые просто находятся на одном IP c запрещенным ресурсом; кроме того, при смене IP адреса доступ к запрещённым ресурсам возобновляется.

- DNS-фильтрация с использованием DNS-сервера оператора (Блокирование по доменным именам). Эффективность данного метода блокирования появляется только в случае правильных настроек абонентского оборудования, а именно, на DNS-сервер оператора связи (при настройке необходимо установить отметку "получить настройки DNS-сервера автоматически". В случае использования различных публичных DNS-серверов, (установка настроек вручную, в частности, Google и Verizon) система блокировки оператора работать не будет. Метод тоже достаточно простой и дешёвый, и гораздо точнее (в части блокируемых ресурсов) и эффективнее предыдущего, но требует принятия оператором организационно-технических мер по контролю применения абонентами настроек на DNS-сервер оператора. Фактически, для блокирования обхода оператору необходимо запретить (технически, либо административно) своим пользователям обращаться к DNS-серверам, находящимся вне сети оператора, либо перехватывать весь DNS-трафик и направлять на собственные DNS-сервера. Но это уже индивидуальные решения. Именно при использовании данного метода блокировки возникает наибольшее количество вопросов с нашей стороны к оператору, т.к. большое количество выявленных случаев неблокирования в ходе мониторинга публичных точек WiFi было связано именно с настройками абонентского оборудования.

- Самым надёжным и верным методом блокировки является блокирование по URL с применением DPI систем. Недостаток этого метода заключается в его высокой стоимости. Большинство операторов позволить их себе не могут.

- Существуют смешанные схемы блокирования, и их большинство. К применению смешанных схем подталкивает необходимость применения разных методов блокирования к разным ресурсам. По большинству ресурсов в Реестр вносится информация и по IP, и по доменному имени, и по URL. Но по НАП – вносится только IP и доменное имя, соответственно, блокировать их нужно либо по IP, но лучше по доменному имени. А по мобильным приложениям – вносится только IP, что предполагает блокирование строго по IP. В последнее время мы выявили, что многие операторы данных тонкостей либо не знают, либо не понимают, либо их системы требуют ручной настройки. Обращаем на это особое внимание.

**(Слайд 6)**

Помимо правильного выбора методов блокирования сайтов, необходимо:

- Использование сертифицированного оборудования и ПО.

- Отключение опции КЭШирование на используемом оборудовании.

- Предпочтительное использование браузера без дополнительных «новшеств», например, таких как режим "Турбо" и "Безопасный WiFi" в Яндекс. Браузере, режим экономии трафика в браузере Google Chrome и т.д.

- Использование DNS-сервера оператора связи.

**(Слайд 7)**

Считаю целесообразным, операторам связи:

- принимать организационные меры по выявлению публичных WiFi точек абонентов. В частности усилить контроль за предоставлением абонентами – юр. лицами списков лиц, использующих оконечное оборудование, проводить анализ полученной информации, выявлять при подключении абонента, для каких целей подключается услуга.

- принимать организационные и технические меры по недопущению перенастройки абонентского оборудования, рекомендовать свою техническую поддержку (выезжать в места организации WiFi точек для настройки оборудования, проведения внутреннего мониторинга);

- разъяснять требования законодательства, предлагать свои услуги по идентификации абонентов, разрабатывать специальные тарифные планы для кафе, ресторанов, парков культуры и отдыха, парикмахерских, государственных учреждений и т.д., в состав услуги где входит организация WiFi точки и идентификация, давать соответствующую рекламу в т.ч. и по ТВ.

- внести необходимые изменения в условиях договора на оказание услуг связи. Например, в раздел «обязанности абонента» конкретизировать условия, необходимые для соблюдения абонентами при организации WiFi точки, запрет на изменение присвоенных оператором сетевых настроек DNS сервера, обязанность уведомления оператора связи о создании публичной WiFi точки и т.п.; в «обязанности оператора» в случае нарушения юридическим лицом или индивидуальным предпринимателем условий договора принимать меры обеспечительного характера

Прошу принять во внимание следующий подход как один из возможных вариантов принятия мер к организаторам точек доступа WiFi.

В случае отсутствия со стороны организатора точки доступа WiFi каких-либо ограничений по доступу детей к запрещённому контенту, наступает ответственность к нему за нарушение требований закона о защите детей. Например, в Саратовской области различные кафе привлечены к административной ответственности за нарушение законодательства о «защите детей от информации, причиняющей вред их здоровью и развитию» в связи с тем, что предоставляют посетителям «без возрастных ограничений возможность подключения к беспроводной сети Интернет, не применяя при этом программно-аппаратные средства защиты детей от информации, причиняющей вред здоровью и развитию», в том числе к экстремистским материалам.

Речь идет о нарушении ч.1 ст.14 Закона о защите детей, согласно которой доступ к информации, распространяемой посредством сети "Интернет", в местах, доступных для детей, предоставляется лицом, организующим доступ к сети "Интернет" в таких местах (за исключением операторов связи, оказывающих эти услуги связи на основании договоров об оказании услуг связи, заключенных в письменной форме), другим лицам при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

Требования утверждены Приказом Минкомсвязи России от 16.06.2014 N 161. Ответственность, предусмотрена ч. 2 ст. 6.17 КоАП РФ.

Неприменение лицом, организующим доступ к распространяемой посредством информационно-телекоммуникационных сетей (в том числе сети "Интернет") информации (за исключением операторов связи, оказывающих эти услуги связи на основании договоров об оказании услуг связи, заключенных в письменной форме) в местах, доступных для детей, административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию, -

влечет наложение административного штрафа на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от пяти тысяч до десяти тысяч рублей; на юридических лиц - от двадцати тысяч до пятидесяти тысяч рублей.

Дела возбуждаем мы, рассматривает суд.

Также операторам связи необходимо, в случае выявления отсутствия идентификации абонентов, принимать меры в соответствии с условиями договора с абонентом.

Кроме того о выявленных случаях необходимо информировать ТУ Роскомнадзора.

 **(Слайд 8)**

Коллеги, в заключении хотелось бы отметить, что поднятую в докладе проблему нужно все-таки решать и решать совместными усилиями в рамках действующего законодательства. Нарушения необходимо пресекать. Если у вас есть предложения организационного или технического характера просьба их высказывать, все принимаются к рассмотрению.

Спасибо за внимание! Доклад окончен.