Российская ассоциация
электронных коммуникаций
РАЭК

Пресненская набережная
дом 12 блок Б
Башня Федерация этаж 46
Москва 123100

info@raec.ru
(495) 950 56 51

www.raec.ru

МЕЖДУНАРОДНЫЙ ОПЫТ ОХРАНЫ ДЕТЕЙ В ИНТЕРНЕТЕ
Аналитический отчет

Ноябрь 2011

Содержание

Введение

В связи с фундаментальными изменениями в области распространения информации, спровоцированными растущей ролью Интернета и социальных сетей в жизни общества; с учетом необходимости модификации международного и национального законодательства в соответствии с этими изменениями; глубоко понимая технологические и функциональные особенности информационно-коммуникационных сетей и трудности, которые возникают в попытках искусственного их регулирования, — Российская Ассоциация электронных коммуникаций представляет аналитический отчет об одном из аспектов международного опыта в области регулирования Интернета.

Данный отчет является результатом анализа международной практики по охране детей от неприемлемого контента в Интернете. Авторами был изучен европейский опыт, опыт Великобритании, США, Японии. В отчете даны краткие описания различных методик регулирования доступа детей к контенту, проанализированы их основные преимущества и недостатки. По итогам исследования сделаны выводы относительно эффективности той или иной методики и даны соответствующие рекомендации.

В отчете использованы данные Еврокомиссии, Международного союза электросвязи, Ofcom, Google, Института семейной онлайн-безопасности (FOSI).

Российская ассоциация
электронных коммуникаций
РАЭК

Пресненская набережная
дом 12 блок Б
Башня Федерация этаж 46
Москва 123100

info@raec.ru
(495) 950 56 51

www.raec.ru

1. Истории успеха: саморегулирование

Одной из наиболее эффективных моделей регулирования Интернета, по мнению международного сообщества, является принцип саморегулирования, на котором основывается деятельность интернет-отрасли в Европе.

В странах Евросоюза с 2009 года действует Декларация принципов саморегулирования в целях безопасности в Интернете,[1] к которой присоединились Microsoft, Facebook, Google, MySpace, Yahoo, Vodafone и ряд других интернет-компаний[2]. Декларация суммирует семь коротких принципов, которые дополняются подробным описанием политик и технологий обеспечения детской безопасности от каждой компании.

В основе принципов лежат три базовых положения:

1. Интернет-компании и интернет-платформы, позволяющие размещать пользовательский контент (социальные медиа), берут на себя обязательства разрабатывать и встраивать **настройки безопасности**, позволяющие родителям ограничить доступ ребенка к нежелательному контенту. При этом речь идет не о навязанной пользователю контентной фильтрации на уровне магистрального провайдера, а именно о пользовательских настройках безопасности, которые являются добровольным выбором пользователя и не ограничивают его права на доступ к информации.
2. Интернет-компании предоставляют пользователям возможность **сообщить о неприемлемом контенте** и реагируют на жалобы пользователей.
3. Настоящий механизм уведомления интернет-платформы пользователем основывается на четких и прозрачных **правилах и политиках размещения пользовательского контента**, его удаления и ограничения доступа к нему, которые разрабатываются и публикуются интернет-компаниями.

Принципы саморегулирования в целях обеспечения безопасности детей в Интернете (из Декларации):

1. Повышать осведомленность участников воспитательного процесса о принципах и настройках безопасности в Интернете: обучать родителей и учителей правилам интернет-грамотности, чтобы они владели достаточной информацией для передачи этих навыков детям;

[1] Текст Декларации:
http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf
[2] Полный список компаний:
http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm

Пресненская набережная
дом 12 блок Б
Башня Федерация этаж 46
Москва 123100

info@raec.ru
(495) 950 56 51

www.raec.ru

2. Стремиться к тому, чтобы интернет-продукты соответствовали потребностям и учитывали возрастную специфику пользователей, потребляющих эти продукты, согласно «Правилам использования» и «Пользовательскому соглашению», разрабатываемым специально для каждого продукта;
3. Предоставлять пользователям технологии безопасности в Интернете;
4. Обеспечивать пользователей простыми механизмами уведомления о незаконном контенте или о контенте, нарушающем «Правила сообщества», разработанные для этого продукта;
5. Реагировать на жалобы и уведомления пользователей;
6. Предлагать пользователям инструменты для обеспечения безопасности персональных данных в Интернете;
7. Оценивать и модернизировать средства и инструменты для выявления нелегального или запрещенного контента.

Настоящие принципы, регулярно пересматриваемые и дополняемые интернет-отраслью, максимально учитывают специфику Интернета и позволяют избегать стандартизирования, препятствующего развитию технологий. Эти принципы саморегулирования позволяют также гибко реагировать на спрос пользователей.

Более того, эти принципы учитывают специфику распространения пользовательского контента в Интернете и принятые в Европе принципы ограничения ответственности интернет-провайдеров и интернет-платформ за контент, размещенный третьими лицами. Учитывая скорость и частоту обновления интернет-ресурсов (к примеру, на крупнейший видеохостинг в мире YouTube загружается 48 часов видео в минуту, что превышает совокупный объем киноконтента, который демонстрируется голливудскими студиями в год), можно утверждать, что интернет-провайдеры не обладают технологическими возможностями осуществлять предварительный мониторинг и премодерацию загружаемого на их платформы контента. Не говоря уже о том, что премодерация контента, загружаемого пользователями, как любая цензура, противоречит конституционным принципам свободы слова.

Еврокомиссия проводит периодическую оценку настоящих принципов саморегулирования, очередной анализ которых в августе 2011 г. подтвердил их эффективность.[3]

В развитие данного подхода, столь позитивно зарекомендовавшего себя в странах Европы, ЕС реализует новую инициативу по созданию саморегулируемой ИТ-коалиции, которая будет заниматься проблемой детской безопасности. Коалиция должна объединить вокруг себя производителей компьютеров, игровых приставок и оборудования, интернет-

[3] http://ec.europa.eu/information_society/activities/social_networking/docs/final_reports_sept_11/ report_phase_b_1.pdf

Пресненская набережная
дом 12 блок Б
Башня Федерация этаж 46
Москва 123100

info@raec.ru
(495) 950 56 51

www.raec.ru

провайдеров и мобильных операторов, интернет-компании, НКО и представителей властей. Инициатива предполагает подписание и принятие единых принципов, направленных на обеспечение и сохранение детской безопасности и предполагающих размещение необходимой информации для пользователей, противодействие нелегальному контенту, работу с представителями структур правопорядка, соблюдение этических принципов и содействие обучению пользователей, снабжение пользователей необходимыми технологическими инструментами по обеспечению безопасности. Инициатива, реализуемая с 2010 г., также подразумевает создание единой системы приема жалоб от пользователей и единый орган управления, который будет состоять из представителей членов коалиции.

Опыт саморегулирования интернет-отрасли в Японии

После ряда неудачных попыток внедрения в Японии контент-фильтров и систем маркировки контента, было принято решение о создании программы по обеспечению детской безопасности в Интернете в рамках инициативы COP (Child Online Protection Initiative) МСЭ и ООН.[4] Программа, стартовавшая в 2009 г., не предполагает введение каких-либо ограничений на Интернет, а сосредоточена на эффективном вовлечении в процесс организации детской интернет-безопасности участников процесса (государства, НКО, родителей, индустрии, международных организаций). Инициаторы программы полагают, что каждая сторона должна принять посильное участие в создании безопасного интернета и обмениваться опытом с другими участниками – только так можно выработать наиболее эффективное решение.

Успешность настоящего подхода саморегулирования базируется на принципе «посильного участия» и «непрерывного диалога», где каждая сторона пытается предложить решения, в которых она является экспертом: государство разрабатывает нормативные акты, эксперты и общество – методологические подходы, провайдеры – технологические решения, а родители и учителя, вооруженные необходимыми знаниями, рассказывают детям о правилах безопасности в Сети.

Можно с уверенностью утверждать, что интернет-компании, работающие на российском рынке, также обладают набором инструментов безопасности, которые могут быть заложены в основу саморегулирования отрасли в России. Среди них - безопасный поиск Google,[5] режим безопасного просмотра видео на YouTube,[6] безопасный поиск Яндекс[7] и др.

[4] http://www.itu.int/osg/csd/cybersecurity/gca/cop/meetings/june-tokyo/bios/index.html
[5] http://www.google.com/support/websearch/bin/answer.py?answer=510
[6] http://www.google.ru/familysafety/tools.html
[7] http://family.yandex.ru/

Пресненская набережная
дом 12 блок Б
Башня Федерация этаж 46
Москва 123100

info@raec.ru
(495) 950 56 51

www.raec.ru

2. Возрастная маркировка интернет-страниц как технологически неэффективная практика: опыт стран ЕС

В 2008 г. в ряде стран Евросоюза обсуждались инициативы возрастной маркировки интернет-контента, однако они были отвергнуты в силу своей неэффективности.

В конце 1990-х годов в США был разработан стандарт маркировки сайтов RSACi (Recreational Software Advisory Council for Internet). Стандарт предполагал возможность маркировки сайта специальными метками, которые считывались браузером и информировали бы родителей о контенте сайта. В начале 2000-х и вплоть до 2008 года инициатива развивалась в Еврозоне как ICRA (Internet Content Rating Association) под патронажем FOSI (Family Online Safety Institute). По мнению инициаторов, маркеры контента позволили бы формировать на их основе необходимы ограничения.

Идея маркировки изначально была воспринята положительно как обществом, так и игроками рынка. К системе присоединились интернет-гиганты начала 1990-х — Microsoft и Netscape, которые контролировали большую часть рынка интернет-браузеров. Таким образом, большинство компьютеров в мире были оснащены необходимыми технологическими инструментами.

Однако с развитием Интернета стало очевидно, что маркировка контента не решает поставленных задач. Система не успевала за развитием Интернета – маркировка сайтов требовала определенных технических навыков, которыми не обладало большинство пользователей, непрозрачность системы вызывала множество споров, рост социальных сетей и личных страниц делал принципиально невозможной маркировку всего контента в интернете, маркировка не учитывала культурных особенностей, ее невозможно было распространить на международном уровне.

В сентябре 2008 г. Еврокомиссия выпустила отчет по анализу системы возрастной маркировки контента, показавший ее неэффективность.[8] В отчете, в частности, отмечается, что контент в Интернете, в отличии от других форм контента (фильмов на CD/DVD, телепередач и видеоигр), распределен в пространстве и во времени, и не имеет единого источника. Это делает невозможным внедрение национальной или международной системы маркировки контента, поскольку сроки внедрения с учетом возможных законодательных и этических проблем делают саму систему классификации неэффективной.

Более того, исследование инициативы BBC (Великобритания) GCLS (Guidance Content Labeling System), предложенной для маркировки видео по запросу, показало, что в

[8] http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/ reportageverification.pdf

Пресненская набережная
дом 12 блок Б
Башня Федерация этаж 46
Москва 123100

info@raec.ru
(495) 950 56 51

www.raec.ru

большинстве случаев родители предпочитают сами делать индивидуальный выбор в отношении собственных детей. При этом часто родители не считают маркировку справедливой и подходящей для их ребенка.

Также соответствующий маркер на сайте уже говорит о заведомом наличии явно выраженного сексуального материала и/или насилия, что привлекает подростков, которые спокойно могут обойти необходимые ограничения.

По результатам Форума «Безопасный Интернет», организованного Еврокомиссией для обсуждения перспектив существующих систем маркировки контента в 2008 г., было принято решение отказаться от возрастной маркировки онлайн-контента на территории Евросоюза. В частности, были учтены следующие аргументы:

- Ни один из подходов к маркировке контента не может стать универсальным одновременно для всех каналов информации, включая Интернет. Системы, получившие наибольшее распространение и признание в Евросоюзе, являются общественными инициативами производителей индустрии (PEGI / ESRB для видеоигр в Европе) и не регулируются законодательно, более того – не распространяются на интернет-контент.
- Ни один из подходов не решает проблему гибкости и адаптации, учитывающей социально-культурные различия стран даже в границах Еврозоны. Расширение понятийного и классификационного аппарата неминуемо ведет к усложнению системы и потере ее эффективности.
- Скорость реакции на возможные жалобы и проблемы со стороны пользователей, сроки пересмотра решений и т.п. ставят под сомнение способность систем маркировки оперативно реагировать на изменения окружающей среды.

В результате в 2008 году поддержка систем маркировки контента в Европе была прекращена. Эксперты признают, что для отдельно взятого контента (не распространяемого в Интернете) маркировка является хорошим индикатором для пользователей (прежде всего, для родителей): например, маркировка фильмов и компьютерных игр (BBFC/PEGI/ESRB) хорошо зарекомендовала себя в США и странах ЕС. Однако в каждом из этих случаев маркировка является добровольной и осуществляется индустрией, а не регуляторами или сторонними экспертами.

Пресненская набережная
дом 12 блок Б
Башня Федерация этаж 46
Москва 123100

info@raec.ru
(495) 950 56 51

www.raec.ru

3. Фильтрация контента: международные подходы

Вопросы фильтрации интернет-контента с целью обеспечения безопасности детей периодически обсуждаются в разных странах мира. К настоящему моменту не существует универсальных эффективных подходов к осуществлению контентной фильтрации, более того, закрепление ее в законе на уровне магистральных провайдеров — и в этом мнении эксперты международного сообщества сходятся — не только не способствует развитию интернет-отрасли и оказывает пагубное воздействие на экономику страны в целом, но и накладывает существенные ограничения на доступ ребенка к информации в нарушение конституционных прав и свобод.

Ключевая проблема фильтрации на уровне провайдера заключается в невозможности составления объективных критериев блокировки контента. При таком подходе, как правило, осуществляется блокировка ресурса целиком (например, всей социальной сети Facebook или видеохостинга YouTube), при том, что на каждом из блокируемых ресурсов может содержаться большое количество полезного и образовательного контента (на видеохостинге YouTube, например, есть отдельный образовательный раздел, куда загружаются лекции крупнейших мировых университетов и ученых, существует множество детских мультипликационных каналов и пр.).

Более того, контентная фильтрация на уровне провайдера не является универсальным решением и не может заменить родительского контроля и активного пользовательского выбора.

В мае 2010 г. авторитетная британская организация Ofcom, учрежденная Министерством связи и осуществляющая регулирование в сфере электронных медиа и Интернета, по поручению Министерства по делам культуры, СМИ и спорта опубликовала специальное исследование различных методов контентной фильтрации и блокировки интернет-ресурсов, результаты которого на детальном техническом уровне доказывают, что большинство даже самых прогрессивных фильтров не обладают 100%-ной эффективностью.[9]

Более того, исследование апеллирует к пониманию того, что за любой контентной фильтрацией стоит несовершенный список ресурсов, подлежащих блокировке, который может быть субъективен и базироваться на относительных критериях оценки.

[9] http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf

Пресненская набережная
дом 12 блок Б
Башня Федерация этаж 46
Москва 123100

info@raec.ru
(495) 950 56 51

www.raec.ru

В отчете указывается, что технически ни один из методов контентной фильтрации на сегодняшний день не может быть в достаточной степени эффективным и универсальным для решения поставленных задач. Ниже представлены основные выводы отчета.

Блокировка по IP-адресу – является одним из наиболее легких в реализации способов ограничения доступа к сайту, однако обладает рядом существенных недостатков:

- количество IP-адресов конечно (существующий стандарт IPv4 поддерживает 4.3 млрд. адресов), следовательно, последовательная блокировка рано или поздно приведет к дефициту;
- владелец сайта может зарегистрировать несколько IP-адресов для одного сайта (домена) и таким образом избежать полной блокировки;
- владелец сайта может сменить IP-адрес или использовать динамический IP.
- ограничение малоэффективно в случае использования VPN-сетей.

DNS-блокировка – позволяет блокировать доступ к сайту по доменному имени (именно его пользователь вводит в адресную строку браузера). В настоящее время активно применяется провайдерами для ограничения доступа к ресурсам, запрещенным в судебном порядке. Основное преимущество заключается в том, что большинство пользователей получают доступ к нелегальному контенту именно через «известные в узких кругах» ресурсы. Соответственно блокировка «раскрученных» сайтов позволяет гарантировано отсечь основную долю потребителей. Еще одним безусловным преимуществом подобного метода является необходимость регистрации доменного имени на конкретное физическое или юридическое лицо, что позволяет установить возможного владельца ресурса. Тем не менее, DNS-блокировка также имеет свои недостатки:

- блокирование доменного имени окажет действие на ресурсы, расположенные в боле низких уровнях (субдомены) и может ограничить доступ к легальным ресурсам, расположенным в той же доменной зоне;
- некорректное осуществление блокирования провайдером может оказать действие на важные интернет-сервисы (платежные системы, онлайн сервисы), что может нанести убытки законопослушным пользователям;

URL-блокировка – осуществляется на основе пополняемого «каталога», который содержит ссылки (например, http://www.example.com/child_porno.zip) на нелегальный контент. Является наиболее адресным способом, поскольку блокирует именно конкретные ссылки. В качестве примера можно привести Internet Watch Foundation, которая ведет мониторинг интернета на предмет контента, содержащего сексуальное насилие по отношению к детям. Основным недостатком подобного способа является необходимость «ручного» пополнения каталога, а также верификация его содержания. Также каталог должен быть единым и постоянно доступным, для сверки запросов пользователей на уровне интернет-провайдера. Негативные последствия и недостатки:

Пресненская набережная
дом 12 блок Б
Башня Федерация этаж 46
Москва 123100

info@raec.ru
(495) 950 56 51

www.raec.ru

- уязвимость единого каталога для несанкционированного доступа и злоупотребления полномочиями;
- снижение скорости доступа в Интернет из-за увеличения траффика за счет постоянной сверки запросов пользователей;
- возможность использования других протоколов для доступа к контенту (например, p2p и стриминговые сервисы);
- возможность смены URL-адреса заблокированной ссылки на любую другую.

Пакетный анализ – наиболее качественный с точки зрения обнаружения нелегальных запросов, данный метод является самым затратным, поскольку требует наличия специального технического оборудования и необходимой квалификации технических специалистов провайдера. Также данный способ негативно сказывается на скорости доступа в интернет за счет постоянного анализа траффика. Основными недостатками пакетного анализ надо признать следующие:

- несопоставимо высокие затраты на внедрение и поддержание системы блокировки;
- недоступность для большинства средних и мелких провайдеров;
- высокие технические требования.

По итогам анализа в отчете делаются следующие выводы:

- Безусловно, блокирование определенных сайтов может положительно сказаться на общем снижении потребления нелегального контента в Интернете, но в случае, если оно является составляющей частью более общих мер по борьбе с нелегальным контентом.
- Ни один из существующих на данный момент технических способов блокировки не может быть на 100% эффективным – у каждого из них есть недостатки, которые сводят на «нет» преимущества, сказываются на общей производительности Сети и несут в себе угрозу свободе слова и правам пользователей.
- Любой из способов блокировки может быть обойден опытным пользователем с использованием минимальных навыков.
- Блокирование доступа к неприемлемому интернет-контенту может быть эффективным только в случае, если процесс будет максимально прозрачным, низким по стоимости и быстрым в реализации. Это может быть достигнуто исключительно на уровне совместной работы всего интернет-сообщества, а не интернет-провайдеров, осуществляющих технический доступ в интернет.

Таким образом, более эффективной и демократичной практикой ограничения доступа детей к неприемлемому интернет-контенту представляется не контентая фильтрация на уровне магистральных провайдеров, а задействование определенных инструмен-

Пресненская набережная
дом 12 блок Б
Башня Федерация этаж 46
Москва 123100

info@raec.ru
(495) 950 56 51

www.raec.ru

тов и настроек безопасности (фильтров) самим пользователем, будь-то инструменты, встраиваемые в интернет-продукты, или фильтры, устанавливаемые на компьютер.

Также международными экспертами признается оптимальным подход к осуществлению фильтрации в школах, при котором выбор ресурсов для блокировки остается на усмотрение самих учебных заведений. Для этого учителя должны обладать необходимыми навыками цифровой грамотности.

Один из сравнительно успешных примеров в этой области — опыт США, где ограничение доступа детей к контенту в школах осуществляется на основе Закона о защите детей в Интернете от 2000 г. (CIPA (Children's Internet Protection Act)).[10]

Закон вступил в действие с 2000 года и призван защитить детей от опасного контента в интернете, такого как непристойность, детская порнография, а также просто вредный для несовершеннолетних.

Закон обязывает школы и общественные библиотеки использовать фильтры интернет-контента, которые отвечают определенным требованиям, прописанным в законе.

Несмотря на многократные попытки усовершенствовать CIPA, закон остается одним из наиболее стабильных в плане внесения изменений, поскольку в наибольшей мере отвечает требованиям Конституции и не ограничивает права граждан в силу следующих основных причин:

- Школы и библиотеки вправе самостоятельно выбирать поставщика систем интернет-фильтрации из списка, отвечающего требованиям закона.
- Учреждения сами вправе устанавливать правила фильтрации, самостоятельно формируя список блокируемых ресурсов и контента. При этом до начала осуществления фильтрации школы проводят общественные консультации по этому вопросу, где обсуждается политика в области детской безопасности в Интернете.
- Закон не предусматривает установку фильтров на стороне провайдера и тем самым не нарушает права граждан.
- CIPA запрещает любой контроль за активностью пользователей в Интернете.
- При этом ответственность за безопасность детей при работе в Интернете в школах (и библиотеках, на которые также распространяется действие CIPA) возлагается на руководство школы (а не интернет-провайдера или производителя фильтра).

[10] http://www.fcc.gov/guides/childrens-internet-protection-act

Пресненская набережная
дом 12 блок Б
Башня Федерация этаж 46
Москва 123100

info@raec.ru
(495) 950 56 51

www.raec.ru

Краткие выводы

Обобщая вышесказанное, необходимо отметить, основываясь на опыте международного сообщества, что ни одна система возрастной маркировки или контентной фильтрации не способна заменить родительского контроля и не подтвердила свою эффективность.

При этом механизмы саморегулирования успешно работают в странах ЕС и Японии.

Таким образом, целесообразно конструировать диалог вокруг развития регулирования Интернета в целях обеспечения детской безопасности, исходя из двух параметров:

1. Развитие принципов саморегулирования на основе инструментов безопасности и механизмов родительского контроля, встраиваемых в интернет-продукты;
2. Развитие программ повышения интернет-грамотности в школах, а также среди родителей и учителей.

Представители интернет-отрасли должны оставаться активным участником настоящей дискуссии.