



БРЫКИН Арсений Валерьевич - доктор экономических наук, зам. генерального директора ОАО «Российская электроника»
Адрес: 127299, г. Москва, ул. Космонавта Волкова, 12
e-mail: avbrykin@ruselectronics.ru

ИНФОРМАЦИОННАЯ СРЕДА И КАЧЕСТВО ЖИЗНИ СОВРЕМЕННОГО ЧЕЛОВЕКА

В условиях XXI века, века активного развития информационных и коммуникационных технологий, все большее влияние на качество жизни современного человека оказывает окружающая его информационная среда. Если раньше базовыми элементами, формирующими сознание человека и его оценку окружающей действительности, являлись печатные средства массовой информации и телевидение, то теперь первенство безоговорочно перехватил интернет.

В современных условиях интернет считается наиболее распространенной информационной сетью (согласно прогнозу Международного союза электросвязи (МСЭ) [1] к концу 2014 года интернетом будут пользоваться 3 миллиарда человек, или 42,3% населения планеты, в 2000 году их было всего 360 млн) (рис. 1).

Многие государства в течение более десяти лет принимают разной степени успешности попытки по снижению возможности негативного использования интернета, пытаются обеспечить безопасность и улучшение качества жизни граждан в информационном пространстве. Главным образом это касается и государственных мер по снижению террористической активности в сети, и мер по ограничению распространения различного негативного контента, в том числе порнографии. Дан-

ные попытки государственного регулирования постоянно конфликтуют со стремлением обеспечить права и свободы граждан, что обусловлено некоторой спецификой Интернет-пространства:

1. Интернет-пространство глобально и динамично в своем развитии. Предугадать характер информации, время, место, автора и его цели практически невозможно.

2. При стремлении обойти нарушения для распространения негативного контента могут быть использованы не подлежащие учету и не требующие регистрации ресурсы. Популярность этих ресурсов может быть раскручена через ссылки на них в социальных сетях.

3. С учетом возможной постоянной миграции контента по сайтам, имеющим разные географические и юридические привязки, вероятность того, что опубликованный противоправный контент, влияющий на качество жизни гражданина или группы людей, будет немедленно обнаружен и удален, крайне мала.

4. Отсутствует единая международная правовая база, регулирующая размещение контента в интернете.

Проведенный автором статьи анализ показал, что лишь подсистемы противодействия терроризму в ряде государств могут быть отнесены к успешному опыту го-

Самые популярные действия в социальных сетях – коммуникации/поддержка контактов

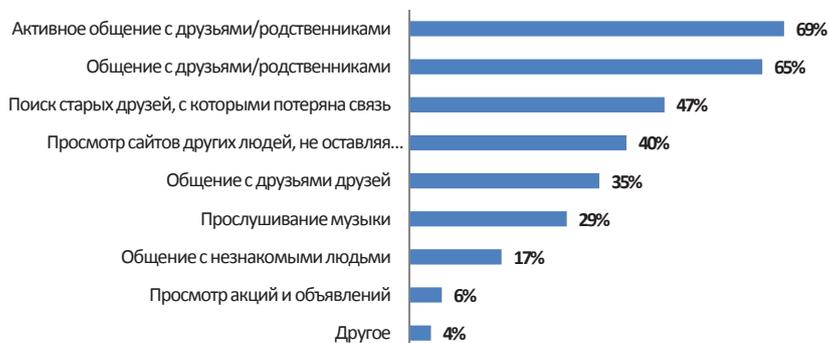


Рис. 1. Перечень действий в социальных сетях

сударственного регулирования и контроля Интернет-пространства. За рубежом организация противодействия терроризму представлена следующими составляющими:

- Правовое обоснование незаконности подобной деятельности.
- Работа правоохранительных органов, специальных служб и ведомств в сфере обеспечения безопасности, в том числе информационной.
- Деятельность специальных контртеррористических групп и национальных антитеррористических центров.
- Разработка методологии противодействия экстремизму.
- Проведение контртеррористических операций.
- Работа служб, занятых ликвидацией последствий терактов.
- Обеспечение тесного контакта со СМИ по вопросам борьбы с антитеррористической деятельностью.
- Развитие соответствующей материально-технической базы (средства связи, новые компьютерные технологии и инфраструктурные элементы) [2].

В последние годы ряд стран мира ведет поиск комплексного решения обеспечения безопасности использования сети Интернет, отчасти проецируя методы, отработанные в сети при борьбе с терроризмом, экстремизмом и порнографией. Далее рассмотрим опыт различных стран в этой сфере.

США. Спецслужбы уполномочены блокировать любой контент, имеющий отношение к экстремизму и терроризму. Провайдеры обязаны выдавать все данные о пользователях по требованию спецслужб. В местах общественного доступа стоят фильтры, ограничивающие доступы к сайтам, содержащим ненадлежащую информацию. Осуществляется постоянный мониторинг киберпространства. Создано специальное подразделение вооруженных сил, отвечающее непосредственно за безопасность в Интернет-пространстве,

- командование боевых действий в кибернетическом пространстве (United States Cyber Command - USCYBERCOM). Существует информационная стратегия по борьбе с терроризмом.

Германия. Действует закон, ограничивающий свободу использования интернета. Функционирует специальная группа министерства внутренних дел, призванная выявлять случаи радикальной исламистской пропаганды, а также анализировать работу некоторых сайтов, представляющих опасность.

Великобритания. Действует закон о неправомерном использовании компьютерных технологий, принятый в 1990 году. Функционирует подразделение министерства обороны по защите от виртуальных угроз (Joint Cyber Reserve Unit), а также подразделение правительственного центра связи - группа безопасности информационных коммуникаций (Communications Electronics Security Group - CESC).

Евросоюз. Конвенция о киберпреступности принята комитетом министров Совета Европы в ноябре 2001 года. Согласно последним данным, конвенцию подписали 46 стран (38 стран ЕС, а также Канада, Япония, ЮАР и США), хотя ратифицировали лишь 24 из них, к не подписавшим ее странам относятся Китай, несколько латиноамериканских стран и Россия.

Израиль. Действуют неправительственные организации, среди них Международный институт по противодействию терроризму (International Institute for Counter-Terrorism), деятельность носит пропагандистский характер.

Индия. Действует несколько спецслужб как на уровне отделов внешних и внутренних разведок, так и на уровне подразделений полиции.

Китайская Народная Республика. С самого начала своего появления интернет в Китае находится под тотальным контролем со стороны властей. Правительство имеет технические возможности

блокировать сайты, на которых появляется информация, идущая вразрез с законами КНР. Введена обязательная регистрация пользователей в Интернет-кафе. Также ведет работу Интернет-полиция, выявляющая незаконный контент в сети. В 2005 году новостные сайты прошли перерегистрацию, согласно которой лично отвечают за публикуемую информацию. С 1 июля 2009 г. в Китае обязательна установка фильтров в компьютеры, в том числе и во ввезенные, для предотвращения доступа к нежелательным сайтам, однако насколько тщательно это контролируется, неизвестно.

Япония. Действует Интернет-портал, посвященный защите граждан от террористической угрозы. Портал имеет информационный характер, позволяя повышать грамотность граждан в вопросах противодействия терроризму.

Республика Казахстан. Действует закон, приравнивающий все Интернет-ресурсы к СМИ, которые стали нести ответственность за размещаемую информацию, а также появилась возможность удаления и блокировки согласно судебным постановлениям.

Республика Беларусь. Действует Закон «О мерах по совершенствованию использования национального сегмента сети Интернет», призванный защитить, прежде всего, рядовых пользователей от деструктивного воздействия экстремистских и аморальных сайтов.

При безусловной важности борьбы с терроризмом стоит заметить, что кроме пропаганды экстремизма и терроризма при использовании сети Интернет в несколько раз возрастает риск вовлечения граждан, особенно детей, в опасные, в том числе асоциальные сферы. Пользуясь интернетом, люди могут:

- столкнуться с нежелательной рекламой;
- получить асоциальную информацию (сексуального, экстремистского или иного характера)

и подвергнуться влиянию нежелательной пропаганды;

- загрузить из интернета нелицензионные материалы (например, музыкальные или видеофайлы);
- стать жертвой запугивания через интернет;
- стать жертвой домогательств насильников или педофилов (например, в онлайн-чатах);
- стать источником информации для киднеппинга и мошенников.

В России пока не существует статистики, дающей представление о том, насколько граждане, в особенности дети, пользующиеся интернетом, подвергаются таким опасностям. Но такая статистика уже есть на Западе.

По зарубежным данным, 9 из 10 детей в возрасте от 8 до 16 лет, которые пользуются интернетом, видят онлайн-порнографию. Около 40% детей, регулярно пользующихся интернетом, однажды подвергались сексуальному домогательству, около 10% подвергались неоднократно. Это касается только онлайн-порнографии. Естественно, существует масса других проблем, актуальных и для России, которая по проникновению в интернет детей и подростков догоняет европейские государства [3] (рис. 2).

По статистическим данным, собранным «лабораторией Касперского» на конец мая 2014 года, можно оценить, на какие категории сайтов с нежелательным контентом дети попадают чаще всего (рис. 3).

При этом в стране формируется так называемый «цифровой» образ жизни, в который подрастающее поколение интегрируется гораздо быстрее тех, кто вызвался его обучать и воспитывать.

Дети в определенном возрасте становятся полноправными участниками мобильных коммуникаций, и прямой запрет использования ими интернета нецелесообразен, да и невозможен.

Дети и новые модели социальных коммуникаций

Реалии:

1. Коммуникационная среда кардинально изменилась.
2. Web-сайты и сервисы для поддержки социальных взаимодействий стали основной коммуникационной средой для нового поколения граждан.
3. Переход от двухсторонних коммуникаций к многосторонним коллективным взаимодействиям.
4. Социальные сети стали неотъемлемой частью жизни 90% детей и подростков.
5. Социальные сети формируют «цифровой» образ жизни людей.

Проблемы:

1. Методы социализации в системе образования не изменились.
2. Угрозы вовлечения детей в опасные сферы через Интернет повысились в разы (контент, педофилы, экстремизм).
3. Методы контроля коллективных взаимодействий детей и подростков в инфопространстве не разработаны.
4. В России нет интегрированного центра коммуникации для детей в виде единой социальной среды.
5. Нет инструментария оценки эффективности программ, ориентированных на детей.
6. Отсутствует адекватная оценка качества жизни в регионах и в стране в целом.

Рис. 2. Проблемы социальных коммуникаций

Рейтинг посещения детьми сайтов с потенциально опасным контентом

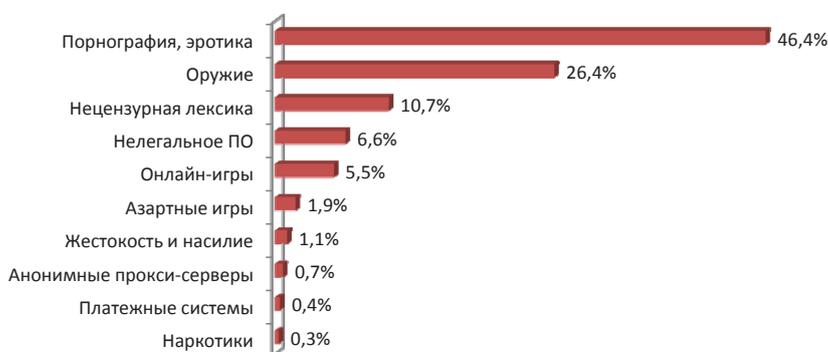


Рис. 3. Рейтинг посещения детьми сайтов с потенциально опасным контентом [4]

С одной стороны, должны создаваться правила пользования детьми интернетом. С другой стороны, с точки зрения автора, **должно существовать контролируемое государством пространство для детей в интернете**, используемое как средство общения, обмена информацией и как инструмент безопасной социализации [5].

За последние несколько лет вопросы, связанные с регулированием Интернет-пространства в России, становятся все более актуальными и сопровождаются острыми дискуссиями применительно к различным сферам жизни общества. Это кроме указанных выше проблем терроризма, экстремизма, негативного контента касается и вопросов законодательного обеспечения госрегулирования СМИ в сети, и вопросов использования ин-

тернета в пропагандистских, политических целях.

Далее приведем краткий анализ российских инициатив в данной сфере.

Президентом России Владимиром Путиным подписан Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации».

Документ предусматривает создание единого реестра Интернет-сайтов (доменных имен, сетевых адресов, указателей страниц сайтов), содержащих информацию, распространение которой в России запрещено, а также механизмов ограничения доступа к ним. Формированием и ведением

такого реестра занимается Роскомнадзор либо привлеченная им для этих целей организация.

Закон предусматривает три категории данных, которые могут быть заблокированы.

Первая: материалы с порнографическими изображениями несовершеннолетних, объявления о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера.

Вторая: информация о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений.

Третья: информация о способах совершения самоубийства, а также призывы к совершению самоубийства.

Основанием для включения сайта в реестр является решение уполномоченных Правительством РФ федеральных органов исполнительной власти или вступившее в законную силу решение суда о признании соответствующей информации запрещенной к распространению.

Непосредственное ограничение доступа к запрещенным ресурсам осуществляют провайдеры хостинга. Это происходит в случаях, если владелец ресурса не удалил противоречащую закону Интернет-страницу добровольно в течение суток с момента получения соответствующего уведомления. Если же и провайдер хостинга не примет должных мер, то доступ к сайту будет ограничен оператором связи.

Нормативно-правовая база, регулирующая инфокоммуникационное пространство в России, вменяет владельцам серверов обязанность уведомлять Роскомнадзор о начале деятельности, хранить данные обо всех действиях пользователей в течение полугода после окончания своей деятельности и предо-

ставлять их правоохранным органам в случаях, предусмотренных законодательством.

В нашей стране активно функционирует крупная общественная организация «Лига Безопасного Интернета», занимающаяся предотвращением распространения опасного контента в интернете (создана при поддержке Минкомсвязи РФ). Вместе с «Лигой Безопасного Интернета» существует целый ряд общественных инициатив, ставящих перед собой задачу развития интернета как саморегулирующейся безопасной среды. Организованное Интернет-сообщество в России активно привлекается и взаимодействует с законодательными органами при разработке соответствующих законопроектов, генерирует и поддерживает общественные инициативы в этой сфере, выступает против «контроля сверху» и введения тотальной цензуры в интернете.

К регуляторным инициативам в этой сфере стоит отнести:

- подготовку законопроекта о блокировке сервисов и ресурсов, дающих анонимный доступ в сеть Интернет;
- регуляцию Интернет-торговли с целью обеспечения безопасности граждан от действий мошенников и их личных данных;
- государственное противодействие пиратству в интернете и защиту авторских прав;
- законопроекты, препятствующие анонимности в интернете как в отношении блогеров (с аудиторией более 3000 человек в сутки), так и в отношении создателей и владельцев сайтов;
- запрещение анонимных переводов средств между физическими лицами.

На данный момент в России применяется несколько способов контроля использования детьми интернета.

Во-первых, это ограничение доступа к нежелательным сайтам через создание так называемых «черных списков» - специальной

обновляемой базы нежелательных для посещения сайтов - и работа фильтров, анализирующих совпадения. В обновлении и распространении этого фильтра активно участвуют члены «Лиги Безопасного Интернета».

Во-вторых, создание «белых списков» - перечня сайтов, содержание которых не является агрессивным. В результате установленные фильтры отказывают в доступе к любой страничке, которая не упоминается в «белом списке». Что касается детей, то технология «белых списков» предполагает давать доступ школьнику только к проверенным «вручную» сайтам, она гарантирует, что ребенок будет посещать только «правильные» сайты, играть в разрешенные компьютерные игры и общаться со сверстниками на модерированных форумах. Программ, использующих технологию «белых списков», довольно много. Некоторые из них (например, Интернет-Цензор) имеют довольно большую популярность среди граждан, стремящихся самостоятельно решить вопрос качества жизни в Интернет-пространстве для себя и своих детей. Ряд систем фильтрации сайтов по этому принципу созданы и продолжают создаваться по инициативе отдельных школ, муниципальных и региональных департаментов образования. Несмотря на поддержку инициативы Минкомсвязи России и профильных комитетов Госдумы, единого федерального «белого списка» до сих пор не существует.

В-третьих, осуществление контроля доступа родителями («родительский контроль»). Например, в Windows и некоторых других программных продуктах есть встроенная функция родительского контроля. Существуют и специальные программы, такие как KinderGate Parental Control. Они позволяют блокировать нежелательные запросы в поисковых системах, контролировать сообщения в социальных сетях, ограничивать

время нахождения в сети Интернет и многое другое. Крупными провайдерами интернета предпринимаются попытки организовать аналогичные сервисы на уровне доступа к каналам связи (сервис МГТС «Родительский контроль»).

Одной из масштабных инициатив стал проект создания некоммерческой доменной зоны ДЕТИ. Предполагается, что в домене будут располагаться сайты, социальные сети и поисковики, предназначенные для детей в возрасте от шести до четырнадцати лет. Администрированием домена будет заниматься Фонд «Разумный Интернет», созданный Координационным центром национального домена сети Интернет. Фонд будет контролировать контент сайтов, расположенных в доменной зоне. Таким образом, ожидается появление

специальной «детской» модификации распространенных Интернет-браузеров, социальных сетей и т.п.

Приоритетная регистрация в новом домене началась 7 апреля 2014 года и проходит в три этапа. На первом этапе до 6 июня принимались заявки от владельцев товарных знаков (знаков обслуживания), внесенных в депозитарий ICANN и зарегистрированных в международной базе данных The Trademark Clearinghouse.

С 16 июня по 14 августа свои имена в домене ДЕТИ смогли зарегистрировать владельцы товарных знаков, охраняемых на территории РФ.

Третий этап, когда свои имена в детском домене смогли получить аккредитованные СМИ и Интернет-проекты, проходил с 19 по 28 августа.

В соответствии с миссией домена ДЕТИ право приоритетной регистрации доменных имен предоставлено также организациям и частным лицам, представляющим в сети Интернет различные детские проекты.

Все желающие могут зарегистрировать доменные имена в домене ДЕТИ через аккредитованных регистраторов - REG.RU, RU-CENTER, WEBNAMES.RU, R01.

Безусловное влияние сети Интернет на качество жизни современного человека постоянно ставит новые задачи с точки зрения его регулирования при соблюдении гражданских прав и свобод. В этом контексте Россия идет поступательными шагами в русле современных тенденций и подходов, внедряемых в других странах мира.

Литература:

1. *Статистика Международного союза электросвязи МСЭ [Электронный ресурс]. - URL: <http://www.itu.int/ITU-D/ict/statistics/explorer/index.html>.*

2. Завьялов С. Зарубежный

опыт в области борьбы с пропагандой терроризма в интернете // Зарубежное военное обозрение. - 2014. - № 4 (805). - С. 34-40.

3. Радио «Свобода». - URL: www.svobodanews.ru.

4. Дети в сети: формула безопасности [Электронный ре-

сурс]. - URL: http://www.securelist.com/ru/analysis/208050844/Deti_v_Seti_formula_bezopasnosti.

5. А. Брыкин. Новые механизмы социализации в системе школьного образования // Экономика России - XXI век. - 2012. - № 25. - С. 63-67.

НАША ИНФОРМАЦИЯ

С 29 сентября по 3 октября 2014 г. в г. Сочи прошла Тринадцатая международная научно-практическая конференция «Электронный век культуры» (ЭВК-2014).

Организаторы: Министерство культуры Российской Федерации, Российская государственная библиотека, Российская ассоциация электронных библиотек и фонд «Электронный век культуры».

В конференции принимали участие представители международных организаций, крупнейших учреждений культуры, коммерческих компаний, исследовательских институтов, вузов, общественных организаций и СМИ.

Ведущими направлениями работы конференции «Электронный век культуры» традиционно являются определение и обсуждение конкретных направлений информатизации учреждений различных отраслей культуры (библиотек, музеев, театров, учебных заведений и т.д.) и практическое решение связанных с этим вопросов и проблем; знакомство с новейши-

ми достижениями в области компьютерной техники и информационных технологий (создание электронных ресурсов вообще и электронных библиотек в частности, поиск и хранение информации).

Российская ассоциация электронных библиотек 30 сентября и 1 октября проводила Интернет-трансляцию мероприятий конференции.

В первый день работы мероприятия состоялись приветственная часть, основное пленарное заседание, на котором рассматривались вопросы создания и развития электронных ресурсов и библиотек, авторского права, автоматизации библиотек, «круглый стол» «Просто НЭБ» и «круглый стол» «Минкультуры России: законодательные инициативы и стратегические документы Года культуры».

1 октября прошел семинар по проблемам создания и поддержки Интернет-магазина в рамках государственного бюджетного учреждения, третья часть пленарного заседания и подведение итогов.

По материалам сайта: <http://www.aselibrary.ru/>.