ЖУРНАЛИСТИКА И РЕКЛАМА

УДК 070.13

ГОСУДАРСТВЕННЫЕ ПРАКТИКИ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ В СЕТИ ИНТЕРНЕТ

А. А. Антонов-Овсеенко

Тверской государственный университет
кафедра журналистики, рекламы и связей с общественностью

Актуальность работы обусловлена тем, что наряду с появлением новых функций мировой сети совершенствуются как методы киберпреступлений, так и государственные практики, направленные на обеспечение безопасности коммуникаций в Интернете, в том числе безопасности работы СМИ и социальных сетей. Анализируемая проблема состоит в противоречии между необходимостью противодействия реальным опасностям и устремлением государств к осуществлению цензуры Интернета. В работе сделан выбор рекомендаций, касающихся государственных практик в области регулирования коммуникаций в мировой сети.
Ключевые слова: *Интернет, безопасность, цензура, информационные ресурсы.*

В XXI в. деятельность преступников в мировой сети нарастает одновременно с угрозами, исходящими от террористических группировок, действующих обычными способами. Само понятие «кибертерроризм» ввел в обиход еще в 1980 г. сотрудник Института безопасности и разведки США Бэрри Коллин, в 1996 г. агент ФБР Марк Поллит предложил определение кибертерроризма: «Преднамеренная, политически мотивированная атака против информации, компьютерных систем, компьютерных программ и баз данных в результате насильственного вторжения со стороны международных групп или секретных агентов» [1, с. 117]. И вплоть до начала XXI в. проблемой кибертерроризма были озабочены прежде всего сотрудники спецслужб промышленно развитых стран. Однако по мере расширения доступа в мировую сеть во всех частях света с угрозами, происходящими от киберпреступников, сталкивается все большее количество граждан: в связи с этим и все большее количество государств вынуждено задумываться о необходимости разработки методов противодействия этим угрозам. Поэтому актуальность настоящей работы заключается (и будет заключаться в будущем для подобных исследований) в том, что вкупе с появлением новых возможностей и функций мировой сети совершенствуются и видоизменяются как способы и методы совершения киберпреступлений, так и государственные практики, призванные обеспечивать безопасность коммуникаций в Интернете, в том числе безопасную работу интернет-СМИ и коммуникаций в социальных сетях. При этом наряду с выработкой методик борьбы с киберпреступлениями возникает и механическое устремление государств к осуществлению максимального контроля над коммуникациями в мировой сети, в том числе над публикациями в интернет-СМИ и в социальных сетях. И поскольку подобное устремление является по существу одним из новых, модернизированных видов цензуры, постольку задачей настоящего исследования стало выявление разницы между попытками осуществления цензуры в

мировой сети и необходимостью защиты общественных, государственных, коммерческих институтов и физических лиц от происходящих из мировой сети реальных угроз и опасностей. В задачу настоящего исследования входит также выбор рекомендаций, касающихся государственных практик в области регулирования коммуникаций в мировой сети. Подобные проблему уже поднимались учеными [2].

Киберпреступники наносят урон не только государственным и коммерческим структурам в разных частях света, но также и институту средств массовой информации, в том числе его новому, быстро развивающемуся сектору онлайн-СМИ, а также коммуникациям в социальных сетях, которые по масштабности охвата участников также следует отнести к одному из новых видов СМИ. Так, в декабре 2015 г. «Твиттер» (*Twitter*) разослал предупреждения части своих пользователей о том, что хакеры могут попытаться получить доступ к их IP-адресам, адресам электронной почты и телефонным номерам, и значительную долю в списке этой рассылки заняли имена журналистов и политических деятелей. «Твиттер» в своем предупреждении также напомнил, что ранее, в 2014 г., уже были взломаны аккаунты сотрудников министерства внутренней безопасности США (*Department of Homeland Security, DHS*), а британская «Файненшл Таймс» (*Financial Times*) приводила пример того, как хакеры «Сирийской электронной армии», получив доступ к Твиттер-аккаунтам уважаемых изданий, публиковали от их имени ложные новости [5].

С каждым годом появляются все новые примеры масштабных киберпреступлений. В мае 2017 г. компьютеры в 74 странах мира, включая Великобританию, США, Китай, Россию, Испанию и Тайвань, атаковал вирус «УоннаКрай» (*WannaCry*): преступники блокировали работу компьютеров государственных учреждений и крупнейших корпораций и требовали за разблокировку от $ 300 до $ 600 в биткоинах (единицах криптовалюты). По сообщениям СМИ, российский разработчик программного обеспечения компьютерной безопасности «Лаборатория Касперского» зафиксировал около 45 тысяч атак этого вируса [12]. Такой масштаб угроз, исходящих из мировой сети, стимулирует государства в разных частях света к выработке методов и способов эффективной борьбы с ними, в том числе методов так называемого «активного противодействия», подразумевающего поиск и ответный взлом программного обеспечения киберпреступников, а при обнаружении места их дислокации – задержание силами правопорядка. Таким образом, нарастание угрозы преступлений в Интернете становится катализатором выработки государственных практик в обеспечении безопасности компьютерных сетей. Однако методики борьбы с этими угрозами и в целом подходы к регулированию коммуникаций в мировой сети складываются по-разному в разных частях света и государствах.

В 2000 г. Я. Н. Засурский отмечал, что «в большинстве стран регулирование содержания Интернета считается невозможным и неразумным. Исходят при этом из трех главных положений. Первое – в условиях глобализации трудно осуществлять контроль над содержанием в общемировом масштабе. Второе – очень велик объем информации. И третье, возможно, самое важное, – в отношении Интернета действуют обычные законодательства. На практике при возникновении конфликтных ситуаций в отношении деятельности, связанной с Интернетом, как правило, используются традиционные законодательства тех стран, закон которых нарушается» [6, с. 32–33]. Если говорить о Европейском континенте, то здесь, фактически исходя из предложенного Я. Н. Засурским понимания ситуации, в Дополнительном протоколе к Конвенции по киберпреступлениям государств-участников ОБСЕ было дано определение уголовно наказуемых «расистских и ксенофобских материалов», которое включает в себя публичные оскорбления или угрозы «совершения серьезного уголовного преступления, как определено ее национальным правом, в отношении лиц по причине их принад-

лежности к группе, отличной по расе, цвету кожи, национальному или этническому происхождению, а также религии, или группы лиц с учетом этих факторов» [6].

Тем не менее исследователь из Китая Цзя Лежун констатировал в 2004 г., что «к вопросу регулирования содержания Интернета разные страны выработали собственные подходы, поэтому признанного всеми принципа в решении этой проблемы пока не существует» [9, с. 30]. Он также обратил внимание на те особенности мировой сети, которые усложняют какое-либо регулирование ею, – такие, как проблема соблюдения баланса между развитием новых технологий и защитой общественных интересов; трудности, связанные с квалификацией преступлений в сети; стремительное развитие новых технологий, за которыми не поспевает разум чиновника; необходимость сотрудничества на международном уровне, обусловленная глобальным характером сети.

Действительно, методы противодействия киберугрозам существенно отличаются друг от друга в разных странах. В частности, китайский подход, по Цзя Лежуну, состоит в выработке специального законодательства: это логически следует из приведенного выше его рассуждения о «трудностях, связанных с квалификацией преступлений в сети», и из сложившейся за десятилетия государственной практики в области контроля за коммуникациями в Интернете. Создание специального законодательства началось здесь с 1994 г. «Китай относится к числу немногочисленных стран, в которых уже на раннем этапе развития телекоммуникаций, и особенно Интернета, были приняты новые законы, касающиеся этой сферы, – пишет Цзя Лежун. – Так, в октябре 2000 г. в Китае <…> было опубликовано “Положение о телекоммуникации КНР”» [9, с. 45], согласно которому для осуществления такой деятельности требуется получение лицензии от государства, все операции разделены на «базовые» и операции «с прибавочной стоимостью». Затем с принятием в 2001 г. Китая во Всемирную торговую организацию (ВТО) появилось «Управляющее правило об иностранных инвестициях в телекоммуникационные предприятия», которым обеспечивается одновременно контроль государства за ходом таких инвестиций и ограничение их объема. Этот документ регулирует режимы лицензирования для коммерческих сайтов и режим работы сайтов информационных, права и обязанности учредителей, кроме того он содержит перечень категорий информации, распространять которую на территории КНР запрещено. К этим категориям отнесены, в частности, «нарушение государственной безопасности, разглашение государственной тайны, подрыв государственной власти, разрушение солидарности государства; нанесение ущерба репутации и интересам государства; …нарушение религиозной политики государства, пропаганда ереси и феодальных суеверий; распространение слухов, нарушение социального порядка, расшатывание социальной стабильности» [9, с. 95]. В результате разработка и практика применения этих документов в Китае привели исследователя к выводу о том, что «по сравнению с развитыми странами в китайском телекоммуникационном секторе некоторые барьеры все еще существуют, поэтому полной свободы телекоммуникационной политики в Китае нет» [Там же, с. 44].

К практике выработки и применения специальных законодательств, регулирующих коммуникации в Интернете, обращаются и другие государства. Одной из первых стран, где были предприняты попытки регулирования мировой сети, стали США: здесь в 1996 г. был принят «Закон о связи», часть положений которого относится непосредственно к сети. В Германии, с одной стороны, в 1997 г. были приняты поправки в Уголовный кодекс, предусматривающие ответственность за преступления в Интернете, но также и специальный закон «Об информационных и коммуникационных услугах» [10, с. 151]. Кроме того, как отмечали в 2011 г. Д. Кофф и Я. Браун, правительства некоторых стран нередко обращаются к своим сторонникам с прось-

бой «направлять жалобы хостинговым компаниям на пользовательский контент. Благодаря таким жалобам активные аккаунты на *Youtube* и *Facebook* были отключены либо удалены в таких странах, как Китай, Египет, Эфиопия, Тунис» [8, с. 181].

В России, фактически по примеру Китая, государство с начала 2000-х гг. предпочитает идти по пути выработки специального законодательства, регулирующего коммуникации в мировой сети. При этом законодательные акты зачастую вступают в противоречие с базовыми положениями российского же закона о СМИ, как, например, подготовленный депутатом А. Луговым закон о внесудебной блокировке сайтов за экстремизм, призывы к массовым беспорядкам и участию в несанкционированных мероприятиях. По требованию Генеральной прокуратуры РФ, действовавшей в соответствии с «законом Лугового», агентство Роскомнадзор 13 марта 2014 г. заблокировало интернет-издания «Грани.ру», «Ежедневный журнал», «Каспаров.ру» и блог оппозиционера А. Навального. Весной 2015 г. заблокированные интернет-СМИ подали жалобу в Европейский суд по правам человека, поскольку, по их мнению, «закон Лугового» «не учитывает правового статуса средства массовой информации, который им предоставлен законом о СМИ» [11], однако в России деятельность этих СМИ так и не была восстановлена.

В противоречие с российским законом о СМИ вступил и так называемый «закон о блогерах» – федеральный закон № 97-ФЗ от 5 мая 2014 г., который обязал всех владельцев электронных ресурсов с аудиторией свыше 3 000 пользователей в сутки регистрироваться в правительственном агентстве «Роскомнадзор» так же, как это делают обычные СМИ.

Таким образом, в мире сложились два подхода к регулированию коммуникаций в сети, которые еще в 2000 г. сформулировал Я.Н. Засурский: «Один – американо-европейский, второй – подход стран Юго-Восточной Азии. Это подход Китайской Народной Республики и Сингапура, где существуют специальные положения и методы ограничения доступа к определенным видам информации. В европейской практике эти методы не одобряются, прежде всего, как непрактичные и неэффективные» [7, с. 32–33]. Такие методы, добавим от себя, демонстрируют и упомянутое выше механическое устремление части государств к осуществлению цензуры Интернета. Именно эти устремления учитывала в 2016 г. американская неправительственная организация «Фридом Хауз» (*Freedom House*) при составлении рейтинга государств с несвободным общением в Интернете, куда были отнесены в том числе Китай, Сирия, Иран, Эфиопия, Узбекистан, Казахстан, Белоруссия и др. России в рейтинге за 2016 г. были присвоены 65 негативных баллов, однако и в целом по ситуации в мире свобода коммуникаций в Интернете во втором десятилетии XXI в. неуклонно снижается, поскольку, по данным «Фридом Хауз» на 2016 г., «67% интернет-пользователей жили в странах, где критика правительства подвергается цензуре, год назад их было 61%» [3].

Необходимость противодействия происходящим из Интернета угрозам, в том числе угрозам общественной нравственности и морали, не вызывает сомнений. Однако, как это было продемонстрировано выше, правительства некоторых государств используют реальные угрозы в целях осуществления политической цензуры и контроля за общением в мировой сети в целом. Насколько целесообразны и, главное, осуществимы на практике эти устремления?

В России тенденция в сторону усиления контроля государства за общением граждан в сети в 2017 г. продолжилась с разработкой поправок в закон «Об информации, информационных технологиях и защите информации» и Кодекс об административных правонарушениях: к окончанию весенней сессии Государственной думы РФ депутаты предложили установить ответственность за отказ удалить противоправный и недостоверный контент из социальных сетей. Физические

лица, согласно законопроекту о поправках, должны будут заплатить от трех до пяти млн. руб., юридические лица – от 30 до 50 млн. руб. Появление этих поправок вызвало обоснованную критику со стороны популярной социальной сети «В контакте». Как заявил СМИ сотрудник пресс-службы сети, «любой пользователь может сообщить о неправомерном, оскорбительном или недостоверном, по его мнению, контенте с помощью кнопки “Пожаловаться”, и одна из самых больших служб модерации примет меры… Дополнительные ограничительные законы совершенно избыточны и по сути своей неисполнимы» [13]. По поводу других ограничений, предусмотренных в законопроекте о запрете обхода блокировок, представители профессионального Интернет-сообщества в России также заявляли, что такие инициативы говорят «прежде всего о том, что российские законодатели на знают, как устроена сетевая инфраструктура, не понимают разницы между приватностью и анонимностью, не видят последствий принятия решений и, самое главное, не сознают цены ошибки» [4]. Кроме того, выяснилось, что обойти блокировки, которые по решению суда налагает на те или иные интернет-ресурсы в России правительственное агентство «Роскомнадзор», с технической точки зрения не составляет труда: общественная организация «Роскомсвобода», заявляющая о том, что ее деятельность направлена на противодействие цензуре в Интернете, вскоре после появления законопроекта о запрете обхода блокировок объявила на своем сайте о начале продаж ВПН-сервисов (*Virtual Private Network*) – соединений, шифрующих данные, которые передаются через Интернет. «Мы постарались отобрать те сервисы, которым доверяют *IT*-правозащитники и пользователи во всем мире. Среди них нет случайных сервисов и тех, кто связан с какими-либо государственными спецслужбами каких-либо стран», – заявил информационному порталу *Republic.ru* представитель «Роскомсвободы» [15].

Присоединяясь к мнениям, высказываемым представителями профессионального сообщества как в России, так и за ее пределами, обратим еще раз внимание на приведенные в начале этой работы замечания и рекомендации, высказанные еще в 2000 г. Я. Н. Засурским. Они состоят в том, что в условиях глобализации трудно осуществлять контроль над содержанием в общемировом масштабе, и появление упомянутых выше ВПН-сервисов подтверждает правоту этого положения. Кроме того, реальному обеспечению безопасности коммуникаций в мировой сети будет способствовать использование существующего национального законодательства вкупе с механизмом саморегулирования. В качестве основного итога настоящей работы отметим, что выбор именно этих предложений для использования во взаимоотношениях государства и Интернета представляется наиболее целесообразным.

Список литературы

1. Акопов А. И. Социокультурные и правовые проблемы интернет-журналистики // Журналистика электронных сетей: сб. ф-та журналистики Воронежского госуниверситета. Вып. 1. Воронеж. 2007. 256 с.
2. Антонов-Овсеенко А. А. О конкуренции информационных ресурсов мировой сети с классическими СМИ и «конце эпохи Гутенберга» // Вестник Тверского государственного университета. Серия: Филология. 2016. № 1. С. 151–155.
3. [Б. а.] Меньше свободы в сети // Ведомости. 15.11.2016.
4. Бегтин И. Правила цензуры // Ведомости. 14.06.2017.
5. Голицына А. Иностранцы взламывают Twitter // Ведомости. 15.12.2015.
6. Дополнительный протокол к Конвенции по киберпреступлениям в отношении криминализации деяний расистского и ксенофобского характера, осуществляемых при помощи компьютерных систем [Электронный ресурс] // Министер-

ство внутренних дел Республики Беларусь. URL: http://mvd.gov.by/main.aspx?guid=4593. (Дата обращения: 28.01.2017.)
7. Засурский Я. Н. Регулирование и саморегулирование сети Интернет: европейские документы и опыт // Информационное общество. 2000. № 4. С. 32–33.
8. Кофф Д., Браун Я. Под давлением цензуры // Hammarberg Thomas, Mijatovic Dunja and oters contributors (9). Human rights and a changing media landscape. Council of Europe Publishing. 2011. P. 181–192.
9. Лежун Ц. Интернет и китайские онлайновые СМИ. М. : Изд-во МГУ. 2004. 128 с.
10. Мелюхин И. С. Информационное общество: истоки, проблемы, тенденции развития. М. : Изд-во МГУ, 1999. 308 с.
11. Мухаметшина Е. Блокировка без границ // Ведомости. 11.03.2015.
12. Серьгина Е., Кантышев П. Вирус-вымогатель атаковал 74 страны // Ведомости. 15.05.2017.
13. Чуракова О., Кантышев П., Брызгалова Е. Достоверность требует штрафов // Ведомости. 13.07.2017.
14. Gordonua.com [Электронный ресурс]. URL: http://gordonua.com/news/money/virus-petya-nanes-ushcherb-kompyuteram-bolee-chem-v-60-stranah-195329.html. (Дата обращения: 08.07.2017.)
15. Republic.ru [Электронный ресурс]. URL: https://republic.ru/posts/85005. (Дата обращения: 17.07.2017.)

GOVERNMENTAL PRACTICES ENSURING SECURITY OF INFORMATION RESOURCES ON THE INTERNET

A.A. Antonov-Ovseenko

Tver State University
Department of Journalism, Advertising and Public Relations

The topicality of the present article is determined by the fact that along with the emergence of new functions of global network, the methods of cybercrime are improving, as well as the governmental practices aiming at enhancing the security of communications on the internet, together with the safety of mass media and communication in social networks. The problem analyzed in the article is the contradiction between the necessity of resistance to real threats, and and state's aspiration for establishing censorship on the Internet. The article proposes a set of recommendations, concerning the governmental practices of control in the field of regulation of the global network communication.
Keywords: *Internet, security, censorship, information resources.*

Об авторе:
АНТОНОВ-ОВСЕЕНКО Антон Антонович – доктор филологических наук, профессор кафедры журналистики, рекламы и связей с общественностью Тверского государственного университета (171100, Тверь, ул. Желябова, 33), e-mail: anton-ov-ovseenko@mail.ru.

About the author:
ANTONOV-OVSEENKO Anton Antonovich – Doctor of Philology, Professor at the Department of Journalism, Advertising and Public Relations, Tver State University (170100, Tver, Zhelyabov str., 33), e-mail: anton.antonov.ovseenko@gmail.com.