DOI: 10.24411/2221-3279-2019-10003

ИНФОРМАЦИОННО-ПРАВОВАЯ ПОЛИТИКА В СОВРЕМЕННОМ ОБЩЕСТВЕ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ

Александр Васильевич Малько

Саратовский филиал Института государства и права Российской академии наук, Саратов, Россия

Оксана Леонидовна Солдаткина

Саратовская государственная юридическая академия, Саратовский филиал Института государства и права Российской академии наук, Саратов, Россия

Информация о статье:

Поступила в редакцию:

19 марта 2018

Принята к печати:

1 ноября 2018

Об авторах:
А.В. Малько, д.ю.н., профессор,
заслуженный деятель науки РФ;
директор, Саратовский филиал Института государства и права РАН

e-mail: i_gp@ssla.ru

О.Л. Солдаткина, к.ю.н., доцент,
кафедра информатики, кафедра административного и муниципального права; старший научный сотрудник, Саратовский филиал Института государства и права РАН

e-mail: buzum@mail.ru

Ключевые слова:
информационно-правовая политика; информационная безопасность; правительство как платформа; Международная стратегия США для киберпространства; Закон КНР о кибербезопасности; Цифровая стратегия Великобритании; Основной закон ФРГ

Аннотация: В статье проводится сравнительный анализ основных направлений информационно-правовой политики различных государств по трем направлениям: информационные права и свободы, электронное управление и информационная безопасность. Такое сравнение в данной области актуально в силу того, что проблемы информационного права зачастую носят глобальный характер, а правовое регулирование информационных отношений обладает международной составляющей. По результатам проведенного в статье сравнения национальных законодательств различных стран по отдельным вопросам информационного права сделаны следующие выводы. Реализация основных прав и свобод граждан в информационной сфере занимает особое место среди национальных интересов большинства государств, но права личности могут быть ограничены. Ограничения в информационной сфере рассмотрены на примере сравнения методов управления контентом глобальной сети, для которых характерно определение государством для себя уровня вмешательства в сетевую жизнь граждан и методов обеспечения вмешательства. В этой области ценен опыт Великобритании и Германии. В целом, направления обеспечения информационной безопасности во всех странах похожи.

Необходимость определения стратегических направлений развития правовой системы, определяющих правовую политику государства, признана в России на самом высоком уровне – речь идет, прежде всего, о федеральном законе от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации». Согласно этому нормативному правовому акту документы стратегического планирования регистрируются в государственном реестре документов стратегического планирования. Указанный

реестр на начало февраля 2018 г. содержит более 56 тыс. документов, среди которых присутствуют Государственная программа Российской Федерации «Информационное общество», Стратегия развития электросетевого комплекса Российской Федерации, Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы, Доктрина информационной безопасности Российской Федерации – документы, определяющие стратегические направления осуществляемой государством политики в информационной сфере.

Между тем все еще наблюдающееся переходное состояние отечественной политико-правовой системы не позволяет говорить о выработке основных постулатов правовой политики в информационной сфере как о свершившемся факте. Современное Российское государство отличает поиск новых юридических конструкций, тем более в такой относительно молодой и бурно развивающейся отрасли, как информационное право. В силу того, что информационное общество размывает государственные границы, проблемы информационного права зачастую носят глобальный характер, поиск их решений ведется практически каждым государством и всем мировым сообществом, а правовое регулирование информационных отношений обладает международной составляющей.

Учитывая сказанное выше, представляется полезным провести компаративный анализ основных направлений информационной правовой политики. В рамках статьи, безусловно, не получится разобрать подробно все вопросы выбранного направления в силу их комплексности и объема, поэтому ограничимся некоторыми отдельными направлениями (выделены на основе разделения объектов воздействия информационной правовой политики):

1) информационные права и свободы;

2) электронное управление;

3) информационная безопасность.

Прежде чем приступить к рассмотрению, сделаем общее замечание: в данной сфере существует большое количество международных нормативных правовых актов, решение о ратификации которых во многом и определяет информационно-правовую политику отдельного государства. К числу таких документов относятся: Окинавская хартия глобального информационного общества, принятая на совещании «стран восьмерки» 22 июля 2000 г.; Конвенция Международного союза электросвязи, подписанная в Женеве 22 декабря 1992 г.; Всеобщая декларация прав человека, утвержденная и провозглашенная Генеральной Ассамблеей ООН 10 декабря 1948 г. и другие.

Начнем нашу компаративную процедуру с вопроса о подходах к информационным свободам в законодательствах различных государств.

Среди национальных интересов большинства государств особое место занимает реализация основных прав и свобод граждан в информационной сфере. Традиционно она основывается на принципах свободы информации и запретительном принципе права (все, что не запрещено законом, разрешено). Этот принцип закреплен в основных международных правовых документах и обычно в конституциях государств (при подкреплении и детализации в ряде других законов).

Основу международного блока нормативных актов в указанной сфере составляет Всеобщая декларация прав человека, согласно которой каждый человек имеет право на свободу мысли (ст. 18), право на свободу убеждений и на свободное выражение их. Это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ (ст. 19).

Позднее эти права и свободы были подкреплены и рядом международных документов, например, в ст. 10 Европейской Конвенции о защите прав человека и основных свобод (вступила в силу 3 сентября 1953 г.), где дополнительно указано, что свободы относятся к всякого рода информации, идеям и способам их распространения, или в Конвенции Содружества Независимых Государств о правах и основных свободах человека, принятой 26 мая 1995 г. и вступившей в силу 11 августа 1998 г. в Республике Бе-

ларусь, Российской Федерации и Республике Таджикистан, где также в ст. 11, 32 и 33 определяет право граждан на свободное выражение своего мнения.

Исходя из международных документов, строится конструкт «информационные права и свободы» в подавляющем большинстве государств.

Так, во Франции в статье 11 Декларации прав человека и гражданина 1789 г. закреплено свободное выражение мыслей и мнений «как одно из драгоценнейших прав человека, каждый гражданин поэтому может свободно высказываться, писать, печататься»[1]. Конституционный совет Франции также неоднократно признавал конституционное значение этого принципа (решения Конституционного совета от 19 и 20 октября 1984 г.), равно как и плюрализм социально-культурных течений мысли (решения от 27 июля 1982 г. и от 18 сентября 1986 г.). Свободу печати и аудиовизуальной информации подтверждают отдельные законы (закон от 29 июля 1881 г. о свободе печати, закон от 20 июля 1982 г., закон от 30 сентября 1986 г.)[2].

В Основном законе Федеративной Республики Германия информационные свободы закреплены в статье 5:

«(1) Каждый имеет право свободно выражать и распространять свое мнение устно, письменно и посредством изображений и беспрепятственно черпать знания из общедоступных источников. Свобода печати и информации посредством радио и кино гарантируется. Цензуры не существует.

(2) Границы этих прав указываются предписаниями общих законов, законодательных положений об охране молодежи правом на честь личности.

(3) Искусство и наука, исследования и преподавание свободны. Свобода преподавания не освобождает от обязанности сохранять верность Конституции»[3].

Определенные информационные свободы предоставляются Конституцией и гражданам Китая. Однако здесь мы видим отсутствие запрета на цензуру:

«Статья 35.

Граждане Китайской Народной Республики имеют свободу слова, печати, собраний, союзов, уличных шествий и демонстраций.

Статья 40.

Свобода и тайна переписки граждан Китайской Народной Республики охраняется законом. Никакие организации или отдельные лица ни под каким предлогом не могут препятствовать свободе и тайне переписки граждан, за исключением случаев, когда в интересах государственной безопасности или в целях расследования уголовного преступления органы общественной безопасности или органы прокуратуры в порядке, установленном законом, осуществляют проверку переписки»[4].

Следует отметить также, что все права и свободы личности могут быть ограничены как правами и свободой других лиц, так и по другим основаниям и в случаях, прямо указанных в законах.

В п. 2 ст. 29 Всеобщей декларации прав человека говорится: «При осуществлении своих прав и свобод каждый человек должен подвергаться только таким ограничениям, какие установлены законом исключительно с целью:

– обеспечения должного признания и уважения прав и свобод других (в ст. 12 Декларации перечисляются права и свободы других лиц: личная и семейная жизнь, неприкосновенность жилища, тайна корреспонденции, честь и репутация);

---

[1] Конституция Франции // Конституции государств (стран) мира: Интернет-библиотека конституций Романа Пашкова (France Constitution). Режим доступа: http://worldconstitutions.ru/?p=138&page=3

[2] Мосин О.В. Права человека в Конституции Франции / ЮрКлуб, 2008. Режим доступа: http://www.yurclub.ru/docs/other/article117.html [Mosin, O.V. Prava cheloveka v Konstitucii Francii (Human Rights in the French Constitution) / YurKlub, 2008. Mode of access: http://www.yurclub.ru/docs/other/article117.html]

[3] Конституция ФРГ // Конституции государств (стран) мира : Интернет-библиотека конституций Романа Пашкова (Germany Constitution). Режим доступа: http://worldconstitutions.ru/?p=155

[4] Конституция КНР // Конституции государств (стран) мира : Интернет-библиотека конституций Романа Пашкова (China Constitution). Режим доступа: http://worldconstitutions.ru/?p=31&page=2

– удовлетворение справедливых требований морали;

– общественного порядка;

– и общего благосостояния в демократическом обществе».

Это касается всех прав, в том числе и информационных. Международные конвенции и основные законы государств поддерживают эти ограничения, детализируя списки. Например, Европейской Конвенцией о защите прав человека и основных свобод (п. 2 ст. 10) наряду с подтверждением ограничений прав только по закону расширяется и перечень оснований для ограничений:

– в интересах государственной безопасности, территориальной целостности или общественного спокойствия;

– в целях предотвращения беспорядков и преступлений;

– для охраны здоровья и нравственности;

– для защиты и репутации или прав других лиц;

– для предотвращения разглашения информации, полученной конфиденциально;

– для обеспечения авторитета и беспристрастности правосудия.

Поскольку одним из основных источников информации и средой реализации свободы слова сегодня выступает виртуальное пространство сети Интернет, представляется интересным сравнение методов управления контентом глобальной сети в отдельных государствах.

Правовое регулирование и управление сетью Интернет сегодня является нерешенным вопросом для подавляющего большинства государств. Как правило, здесь реализуется все тот же принцип свободы слова в сети Интернет и фильтрации отдельного контента, содержание которого попадает в списки «вредной» информации. Но практика показывает, что этот метод – не только не эффективен, но и в принципе ведет к некоторым нежелательным последствиям. Среди нашумевших в СМИ примеров блокировки отдельных ресурсов сети Интернет, приводящих к противоположным результатам, является внесение популярного торрент-трекера *Rutracker.org* в реестр запрещенных сайтов (25 января 2016 г.). Сайт был заблокирован по решению Мосгорсуда, дважды признававшего его нарушителем авторских прав на книги издательства «Эксмо». По данным Rutracker.org, активность файлообмена за время блокировки снизилась всего на 5%. Представитель трекера считает, что уровень пиратства в русскоязычном сегменте сети Интернет благодаря блокировкам мог даже вырасти, так как владельцы видеоресурсов и трекеров перестали сотрудничать с правообладателями и добровольно убирать их контент по запросу, то есть запрет существенно ухудшил положение правообладателей информации.

Ответим далее на вопрос: как решается эта проблема в отдельных государствах, взяв несколько «крайних» примеров.

Всемирная сеть представляет собой сложную систему, включающую в себя несколько уровней коммуникации: техническую и информационную. «В этом контексте на доктринальном и правоприменительном уровне обсуждается необходимость концептуального разграничения собственно интернета, рассматриваемого в качестве технического изобретения, которое главным образом связано со сферой телекоммуникаций, и доступа к интернету – использование технологических возможностей интернета для получения информации, т.е. использование интернета, рассматриваемое как “информационная услуга”»[5]. Соответственно и управление виртуальным пространством так же необходимо разделять на два этих уровня.

В технической области, где вопросы регулирования возникли существенно раньше, исторически сложилась «многосторонняя» модель управления (*MultistakeholderModel*), основанная на саморегулировании и многостороннем партнерстве, включающем все заинтересованные стороны (частный сек-

[5] Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. – М.: Статут, 2013. – С. 13. [Kiberbezopasnost' i upravlenie internetom: Dokumenty i materialy dlja rossijskih reguljatorov i jekspertov (Cybersecurity and Internet Governance: Documents and Materials for Russian Regulators and Experts) / Ed. M.B. Kasenova; Comp. O.V. Demidov, M.B. Kasenova. Moscow: Statut, 2013. P. 13.]

тор, гражданское общество, бизнес, техническое и академическое сообщество, правительства, международные организации и прочее). Безусловно, в этой сфере существуют проблемы: нечеткое определение роли заинтересованных сторон в процессе управления, формальная автономия международной некоммерческой организации *Internet Corporation for Assigned Names and Numbers (ICAAN)*, осуществляющей регулирование Интернета в части доменных имен, IP-адресов и прочих механизмов. Тем не менее, несмотря на имеющие недочеты, модель упорядочения технической составляющей сети Интернет в целом уже сложилась.

С регулированием информационной составляющей – а именно эта сторона вопроса в рамках нашего исследования особенно нас интересует – все гораздо сложнее. В этой области также формируется многосторонняя модель управления глобальной сети, включающей несколько уровней. В литературе выделяются следующие проблемы, которые не могут быть решены национальным законодательством, и должны решаться всем мировым сообществом:

1. Разработка международно-правовых гарантий безопасного использования сети Интернет.

2. Гармонизация национальных законодательств в силу существования различия в порядке и методах регулирования национальным правом использования сетевых технологий в противоправных целях.

3. Разработка правил, принципов и норм защиты критически важной инфраструктуры Интернета на международном уровне с учетом трансграничного функционирования сети Интернет.

4. Проблема идентификации пользователей сети, владельцев Интернет-ресурсов и операторов Интернет-услуг.

5. Дальнейшее совершенствование нормативно-правового регулирования порядка оказания трансграничных услуг Интернет-компаниями, являющимися национальными юридическими лицами конкретных государств, например, таких как *Google, Facebook* и т.п.[6]

Существует и часть проблем, которые традиционно решаются на внутригосударственном уровне. Здесь главное найти общий путь развития. Показательными в этой области будут США, где до недавнего времени проводилась политика саморегуляции сети Интернет; Китай, власти которого с самого начала развития отрасли придерживаются методов жесткого контроля виртуального пространства; Франция, сочетающая крайние средства.

США. Согласно принятой в 1791 г. первой поправки к Конституции США, Конгресс США не должен издавать ни одного закона, относящегося к установлению религии или запрещающего свободное исповедание, ограничивающего свободу слова или печати, право народа мирно собираться и обращаться к правительству с петициями об удовлетворении жалоб[7]. Однако в постоянно меняющемся цифровом мире и с увеличением числа злоупотреблений свободой сети Интернет появляются исключения из правил защиты, предоставляемой первой поправкой.

С 2001 г. в США действует «Акт о защите детей в Интернете», согласно которому ограничен доступ к некоторым интернет-ресурсам, содержащим информацию непристойного характера в общественных местах[8]. В 2010 г. была разработана «Стратегия национальной безопасности США», где в качестве одной из основных угроз указаны широкомасштабные кибератаки и в связи с этим правоохранительные органы США обязаны принимать необходимые меры для защищенности киберпространства в целях защиты прав граждан, экономики, торгов-

[6] См.: Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. – М.: Статут, 2013. – С. 45-46. [Kiberbezopasnost' i upravlenie internetom: Dokumenty i materialy dlja rossijskih reguljatorov i jekspertov (Cybersecurity and Internet Governance: Documents and Materials for Russian Regulators and Experts) / Ed. M.B. Kasenova; Comp. O.V. Demidov, M.B. Kasenova. Moscow: Statut, 2013. Pp. 45-46.]

[7] См.: Поправки к Конституции США. Билль о Правах (1791) Поправка I (1791).

[8] Children's Online Privacy Protection Act (COPPA) of 1998, via Federal Trade Commission.

ли, инфраструктуры жизнеобеспечения[9]. В США действует Закон о мошенничестве и злоупотреблении с использованием компьютеров – основной нормативно-правовой акт, устанавливающий уголовную ответственность за преступления в сфере компьютерной информации[10]. Интересна также и борьба за так называемый «принцип сетевого нейтралитета», предполагающий, что провайдеры не могут по-разному относиться к тем или иным сайтам или видам трафика – к примеру, блокировать его или брать отдельную плату за увеличение скорости доступа к какому-то сайту: будучи предложенным в 2008 г. крупными корпорациями, включая Coogle, этот принцип был закреплен Федеральной комиссией по коммуникациям США (FCC) в феврале 2015 г., вызвав при этом неудовольствие все тех же корпораций в связи с изменившейся обстановкой, и был отменен в 2017 г.[11] В 2015 г. Федеральная комиссия по связи США объявила Интернет «телекоммуникационным», а не «информационным» ресурсом, чтобы его было легче регулировать и создать равные условия для следующего поколения предпринимателей. Но наблюдатели и пресса США, по свидетельству A*ssociated Press*, расценили этот шаг как «открывающий новую эпоху правительственного надзора в отрасли, где его было сравнительно мало»[12].

Однако следует отметить тот факт, что США, вместе с усилением контроля над сетью Интернет своей страны, не забывают о «содействии свободе интернета» в мире[13]. Более того, до недавнего времени ключевым моментом современного режима управления сетью Интернет является лидирующее положение в нем США благодаря эксклюзивным контрольным функциям по отношению к пространству имен и адресов Интернета и контрактным отношениям с ICANN и рядом других специализированных организаций. Конечно сейчас эта ситуация изменилась в связи со скандалом с бывшим сотрудником Агентства национальной безопасности США Эдвардом Сноуденом, который раскрыл конфиденциальные сведения американских спецслужб относительно тайной слежки за странами. Его действия стали катализатором для перемен. Так, президент ICANN Фади Шехаде использовал разоблачения Сноудена как предлог объявить о том, что Корпорации интернета пора освободиться от американского влияния, став международной организации (с 1 октября 2016 года ICANN не находится под надзором правительства США), а Бразилия и Германия официально представили в ООН проект резолюции о недопустимости электронного шпионажа[14].

Франция – одна из стран, с самого начала выступающая за регулирование Интернета на государственном уровне. Еще в 2000 г. Национальная ассамблея Франции проголосовала за принятие законопроекта об обязательной регистрации владельцев всех веб-сайтов страны и об уголовной ответственности провайдеров за предоставление хостинга неидентифицированным пользователям[15].

---

[9] См.: National Security Strategy of the United States. May 2010. Washington, DC. Mode of access: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[10] См.: Официальный сайт ФБР. Режим доступа: http://fbi.gov/lasvegas/press-releases/2011/sixteen-persons-charged-in-international-internet-fraud-scheme

[11] В США отменили принцип «сетевого нейтралитета», введенный при Обаме (In the United States, the Principle of «Net Neutrality» Introduced under Obama Was Abolished) / Meduza, 2017. Режим доступа: https://meduza.io/news/2017/12/14/v-ssha-otmenili-printsip-setevogo-neytraliteta-zakreplennyy-v-2015-godu

[12] Власти США упростили регулирование интернета // Взгляд, 2015 [US Authorities Have Simplified Internet Regulation // *Vzglyad*, 2015]. Режим доступа: https://vz.ru/news/2015/2/26/731722.html

[13] См.: Двойной сетевой стандарт США выявляет их лицемерность // газета «Жэньминьжибао» [US Double Network Standard Reveals Their Hypocrisy // Renminjibao Newspaper]. Режим доступа: http://russian.people.com.cn/95181/7909174

[14] См.: В ООН представлен проект резолюции о недопустимости электронного шпионажа / *Вести.RU* [The UN Submitted a Draft Resolution on the Inadmissibility of Electronic Espionage / Vesti.RU]. Режим доступа: http://www.vesti.ru/videos?vid=551195&cid=780

[15] Анисимова А.С. Анализ правотворческой политики зарубежных стран в сфере регулирования интернет-отношений // Вестник Саратовской государственной юридической академии. – 2014. – № 5. [Anisimova, A.S. Analiz pravotvorcheskoi

Одним из органов, регулирующим отношения в сети Интернет, выступает Министерство народного образования[16]. Им осуществляется внедрение централизованных фильтров, которые ограничивают доступ к информации, запрещенной на территории Франции. Фильтрация осуществляется на основании двух «чёрных списков» Интернет-ресурсов: первый включает порнографические ресурсы; второй список состоит из расистских и антисемитских ресурсов.

С 2009 г. во Франции действует Закон о борьбе с пиратством в сети Интернете. В марте 2011 г. французский парламент одобрил суровый законопроект *Loppsi 2*, регулирующий вопросы внутренней безопасности в стране на период до 2013 г. включительно. Контролирующим органом выступает Высший комитет по распространению произведений искусства и защите авторских прав в Интернете, одним из полномочий которого является «слежка» за гражданами. Все данные собираются и легально отправляются в большие общенациональные базы[17]. Предусматривается тесное сотрудничество провайдеров сети с государственными структурами.

15 февраля 2011 г. Конституционным Советом Франции принят закон «О безопасности Интернета», направленный на обеспечение внутренней безопасности страны[18]. Закон, в частности, предусматривает введение следующих мер регулирования и контроля сети: осуществление обязательной фильтрации сети Интернет для пресечения распространения информации запрещенной на территории государства, а также незамедлительного блокирования ресурсов по представлению МВД Франции без необходимости представления судебного решения; введение уголовной ответственности за кражу и использование персональных данных в сети Интернет; легализацию удаленной установки полицейскими подразделениями на компьютеры лиц, подозреваемых в совершении преступлений, специальных программ, позволяющих регистрировать и передавать в полицию данные о действиях, совершаемых пользователями персональных компьютеров (только по решению суда)[19].

На наш взгляд, правовое регулирование данной сферы во Франции имеет положительные черты, поскольку привлечение к ответственности всех субъектов Интернет-отношений подталкивает пользователей к самоцензуре, что выступает большим шагом на пути к безопасной сети. Вместе с тем, Франция вынуждена пересматривать свое отношение к вопросам соотношения свободы слова и национальной безопасности. Череда терактов, прокатившаяся по Франции в январе 2015 г. (атака на редакцию сатирического еженедельника *Charlie Hebdo*, захват заложников в Париже и Даммартен-ан-Гоэль[20]) после издания серии карикатур на пророка Магомета, заставило французское правительство и ученых-правоведов задуматься над указанными вопросами. Время покажет, какие меры будут приняты и ска-

politiki zarubezhnykh stran v sfere regulirovaniia internet-otnoshenii (Analysis of Lawmaking in Foreign Policy the Regulation of Internet Relationships) // *Vestnik Saratovskoi gosudarstvennoi iuridicheskoi akademii*, 2014, No. 5.]

16 См.: Фильтрация и блокирование интернет-контента: мировой опыт // Риа-Новости [Internet Content Filtering and Blocking: Worldwide Experience // *RIA Novosti*]. Режим доступа: http://ria.ru/spravka/20120711/697151590.html#ixzz2fndemnM7

17 См.: Правый мир «Информационный портал». Франция: Тоталитарный закон Loppsi 2 [Right World "Information Portal". France: Totalitarian Law Loppsi 2]. Режим доступа: http://right-world.net/news/312

18 См., например: Фильтрация и блокирование интернет-контента: мировой опыт // Риа-Новости [Internet Content Filtering and Blocking: Worldwide Experience // *RIA Novosti*]. Режим доступа: http://ria.ru/spravka/20120711/697151590.html#ixzz2fndemnM7

19 Правовая жизнь современного российского общества: уровни, срезы, сегменты / (Анисимова А. С. и др.); под ред. А.В. Малько. – Москва: Юрлитинформ, 2016. – 354 с. [Pravovaya zhizn sovremennogo rossijskogo obshchestva: urovni, srezy, segmenty (Legal Life of Modern Russian Society: Levels, Sections, Segments) / (Anisimova A.S. and oth.) ed. by A.V. Malko. Moskow. Yurlitinform, 2016. 354 p.]

20 См.: Патриарх Кирилл: терроризм и насилие недопустимы, как и кощунство // РИА Новости, 25.01.2015 [Patriarch Kirill: Terrorism and Violence are Unacceptable, as Blasphemy // *RIA Novosti,* 25.01.2015]. Режим доступа: http://ria.ru/religion/20150125/1044178924.html#ixzz3UTBEkiad

жутся ли события начала 2015 г. на французском законодательстве, регулирующем виртуальное пространство, однако представляется, что влияние оно окажет[21].

Китай в настоящее время остается страной с самыми суровыми правилами государственного регулирования сети Интернет, вплоть до узаконенной цензуры и активной пропаганды действующего режима – несмотря на закрепленную в Конституции свободу слова. Органом, регулирующим Интернет-отношения, выступает «Центр контроля за вредной информацией», основной задачей которого является отсев контента, по каким-либо причинам признанного социально опасным китайским правительством. Контроль заключается в фильтрации результатов поиска, запрете на доступ к некоторым ресурсам, модерации записей на форумах, блогах и других общественных площадках. Кроме того установлены специальные фильтры на все поисковые серверы[22], официально запрещен доступ к множеству зарубежных социальных сетей[23]. При этом почти каждый третий житель страны имеет доступ во Всемирную сеть, действует более 2 млн сайтов[24].

В 2011 г. Министерство обороны Китая официально объявило о создании специальной структуры по контролю над сетью Интернет – «Онлайн армии голубых мундиров», приоритетным направлением их работы выступает защита от киберпреступников.

В сентябре 2013 г. было объявлено о разработке нового законопроекта, устанавливающие новые правила регулирования «онлайн-болтовни» и считающиеся частью кампании, направленной против блогеров, журналистов и политической оппозиции[25].

Следует отметить, что наряду с подобными мерами ограничения доступа граждан к информации в сети Интернет, в Китае действует система поощрений. Например, в целях противодействия распространения порнографической продукции правительство выплачивает пользователям вознаграждение в размере от 500 юаней (60 долларов) до 2000 юаней (241 доллар) за сигнал о распространении такой информации.

Оценивая систему правового регулирования Интернет-отношений, действующую в Китае, можно отметить ее положительный результат. Столь отлаженный механизм воздействия на сеть Интернет позволяет нейтрализовать информацию, которая может нанести вред человеку и подорвать государственную безопасность[26].

Таким образом, мы видим, что сегодня модель саморегулирования глобальной сети не находит применения ни в одной стране мира – каждое государство определяет для себя только уровень вмешательства в сетевую жизнь граждан и методы обеспечения вмешательства, к которым можно отнести системы принудительной фильтрации всего контента на уровне провайдеров (Китай); «черные списки» запрещенных сайтов с противоправным контентом (Франция), позволяющие точечно реагировать на меняющуюся среду и блокировать известных нарушителей; блокировка сайтов с нежелательным или противоправным контентом по требованию правоохранительных органов к хостинг-провайдерам и интернет-

[21] Правовая жизнь современного российского общества: уровни, срезы, сегменты / (Анисимова А. С. и др.); под ред. А.В. Малько. – Москва: Юрлитинформ, 2016. – 354 с. [Pravovaya zhizn sovremennogo rossijskogo obshchestva: urovni, srezy, segmenty (Legal Life of Modern Russian Society: Levels, Sections, Segments) / (Anisimova A.S. and oth.) ed. by A.V. Malko. Moskow. Yurlitinform, 2016. 354 p.]

[22] См.: Российская газета. Федеральный выпуск (суббота) № 5642. 2011 [Rossiskaya Gazeta, 2011, No. 5642]

[23] См.: Российская газета. Федеральный выпуск № 4983. 2009 [Rossiskaya Gazeta, 2009, No. 4983]

[24] См.: Российская газета. Федеральный выпуск № 5865. 2012 [Rossiskaya Gazeta, 2012, No. 5865]

[25] См.: Китайцев больно ранят слухи // Газета.RU [Rumors Hurt the Chinese Painfully // *Gazeta.RU*]. Режим доступа: http://www.gazeta.ru/social/2013/09/09/5645017.shtml

[26] Правовая жизнь современного российского общества: уровни, срезы, сегменты / (Анисимова А.С. и др.); под ред. А.В. Малько. – Москва: Юрлитинформ, 2016. – 354 с. [Pravovaya zhizn sovremennogo rossijskogo obshchestva: urovni, srezy, segmenty (Legal Life of Modern Russian Society: Levels, Sections, Segments) / (Anisimova A.S. and oth.) ed. by A.V. Malko. Moskow. Yurlitinform, 2016. 354 p.]

провайдерам. На наш взгляд, пока эффективность регулирования сети Интернет демонстрирует только китайский вариант жесткой фильтрации трафика, неприемлемый однако для стран, где установлен запрет цензуры как один из параметров свободы слова.

Российская Федерация пошла по третьему пути – блокирование сайтов контентом по требованию правоохранительных органов к хостинг-провайдерам и интернет-провайдерам (Федеральный закон № 398-ФЗ от 28 декабря 2013 года «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"»). А с 1 ноября 2017 г. в России вступил в силу «усиливающий закон», обязывающий поисковики исключать из выдачи заблокированные ресурсы, а анонимайзеры и VPN-сервисы – закрывать доступ к запрещенным сайтам[27]. За нарушение этого закона поисковым системам грозит крупный штраф, а анонимайзерам блокировка на территории РФ. Сам закон о блокировке неоднократно подвергался критике со стороны пользователей сети и экспертов. Интернет-омбудсмен при президенте Дмитрий Мариничев, назвавший законопроект «безумием», отметил невозможность отделить VPN, используемый в коммерческих целях, от VPN, используемого для обхода блокировок[28]. Более того, опыт Китая, где как упоминалось выше с 2003 г. действует система фильтрации контента «Золотой щит», показывает, что ограничение работы средств для обхода интернет-блокировок не позволяет полностью закрыть доступ пользователей к VPN-сервисам, выходным узлам Tor и другим средствам проксирования трафика[29]. Это говорит о низкой эффективности предпринимаемых в России мер по фильтрации Интернет-контента и диктует необходимость искать другие пути решения этой задачи.

Процедура сравнения по вопросу об электронном управлении различных государств связана традиционно с процессами формирования и развития национальных электронных правительств. Оценка эффективности этого процесса проводится ООН раз в два года посредством составления рейтинга стран по уровню развития электронного правительства. В опубликованном 29 июля 2016 г. рейтинге, Россия заняла 35 место, опустившись на 8 пунктов по сравнению с 2014 г. 27 место, на которое Россия поднялась еще в 2012 г., является достаточно высоким (особенно по сравнению с 2010 г., когда она занимала 59 место)[30].

Чтобы поправить сложившуюся ситуацию, стоит, во-первых, проанализировать критерии оценки и динамику изменения рейтинга; во-вторых, обратиться к опыту государств, постоянно занимающих высокие места в указанном рейтинге (Великобритания, Германия).

Падение места Российской Федерации в общем рейтинге, как и его рост в 2012 г., обусловлены изменениями следующих индексов: индекс телекоммуникаций, индекс онлайновых услуг, индекс человеческого капитала (вместе – композитный индекс развития электронного правительства, на основе которого строится рейтинг ООН). Рассмотрим динамику на примере индекса онлайновых услуг. В индексе телекоммуникационной инфраструктуры, который рассчитывается на основе 5 показателей,

[27] Президент России подписал закон о запрете анонимайзеров // d-russia.ru. 2017, 31 июля. [The President of Russia Signed the Law Banning Anonymizers] Режим доступа: http://www.the-village.ru/village/city/instruction/275986-blokirovka-anonimayzerov

[28] См.: Закон об анонимайзерах: как их будут блокировать и что с этим делать / The Village, 2017 [Law on Anonymizers: How They Will Be Blocked and What to Do about It / The Village, 2017]. Режим доступа: http://www.the-village.ru/village/city/instruction/275986-blokirovka-anonimayzerov

[29] Президент России подписал закон о запрете анонимайзеров // d-russia.ru. 2017, 31 июля. [The President of Russia Signed the Law Banning Anonymizers] Режим доступа: http://www.the-village.ru/village/city/instruction/275986-blokirovka-anonimayzerov

[30] Опубликован новый рейтинг ООН развития электронного правительства / Институт развития информационного общества: официальный сайт [New UN Ranking of E-Government Development Is Published / Institute of the Information Society]. Режим доступа: http://www.iis.ru/content/view/795/91/

собираемых Международным союзом электросвязи, динамика аналогична.

Индекс онлайновых услуг рассчитывается на основе результатов обследования официальных правительственных порталов и веб-сайтов. Внедрение единого портала государственных и муниципальных услуг в совокупности с раскрытием информации о деятельности органов власти на официальных сайтах, начиная с 2012 г. обеспечило России стремительный рост в рейтинге именно за счет индекса онлайновых услуг. Дальнейшее развитие портала государственных и муниципальных услуг позволило сохранить высокие позиции в рейтинге и в 2014 г. Но в этот же период поменялась методика ООН для обследования официальных сайтов, в которую были введены и расширены критерии, связанные с современными тенденциями развития электронных правительств, – открытые данные и электронное участие граждан в управлении стали рассматриваться как важная часть услуг электронного правительства. Возникла насущная необходимость принципиального изменения отношения к самой сути понятия электронного правительства не просто как к использованию информационных технологий для предоставления государственных и муниципальных услуг. Этой переоценки в России не произошло, а потому ее стали обгонять другие страны.

Анализ рейтинга позволяет установить факт, что в первой десятке рейтинга находятся страны, принявшие и реализующие проекты цифровой трансформации своих систем государственного управления, внедряющие у себя таким образом технологий электронного правительства нового поколения – цифрового правительства[31].

На первое место в рейтинге ООН в 2016 г. вышла Великобритания, ставшая пионером внедрения цифровых государственных услуг. Обратимся к ее опыту.

1 марта 2017 г. Великобритания представила стратегию развития цифровых технологий (*Digital Strategy*) – документ включает семь направлений, по которым страна намерена развивать «ведущую цифровую экономику» в мире[32]. Среди этих направлений присутствует и «Цифровое правительство – поддержание Великобритании в качестве мирового лидера в обслуживании своих граждан в Интернете».

Цифровое правительство Великобритании основывается на концепции «Правительство как платформа», обеспечивающей наиболее активное отдельных компонентов на базе общей платформы. При этом планируется отказаться от крупного единственного поставщика и многолетних IT-контрактов; разработать и опубликовать стандарты и руководства по компонентам, платформам и техническим возможностям; снять барьеры для изучения и использования государственных платформ и их компонентов внешними разработчиками; повысить вовлеченность граждан в использование системы, обеспечивающей их единой учетной записью для доступа к электронным государственным услугам; провести ревизию устаревшего контента и пр. Также декларируется использование новейших технологий (облачное программное обеспечение, блокчейн, bigdata) там, где это правильно, – вместо устаревших, но уже привычных.

Для достижения заявленных в *Digital Strategy* требований, 9 февраля 2017 г. принята новая Стратегия трансформации правительства до 2020 г.[33], направленная на повышение скорости, удобства и качества оказания государственных услуг. Стратегия трансформации правительства призвана изменить общие методы доставки услуг, для чего в ней заявлены три основных компонента:

[31] Под цифровым правительством будем понимать правительство, создаваемое и действующее так, чтобы использовать преимущества цифровых данных при оптимизации, трансформации и создании государственных услуг. Данное определение компании «Гартнер» приводится в аналитическом докладе «Цифровое правительство 2020: Перспективы для России» [Analytical Report "Electronic Government 2020: Prospects for Russia"] / IIS. Режим доступа: http://www.iis.ru/docs/DigitalGovernmentRussia2020RUS.pdf

[32] GOV.UK: официальный портал правительства Великобритании. Режим доступа: https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy#contents.

[33] Ibid

1. Трансформация всех общедоступных сервисов – с целью дальнейшего повышения их удобства для граждан, бизнеса и пользователей госсектора.

2. Полная трансформация департаментов – приведет к гибкому исполнению целевых задач, улучшит кросс-канальное предоставление услуг, повысит эффективность.

3. Внутренняя трансформация правительства, которая не обязательно внешне повлияет на публичные сервисы, но жизненно необходима для лучшего взаимодействия частей госаппарата и для осуществления «цифровых» преобразований[34].

В целом Стратегия трансформации правительства рассчитана на то, что пользователи получат услуги, отвечающие их требованиям; правительство сможет максимально быстро реагировать на запросы граждан; повысится доверие граждан к правительству в части хранения и распоряжения их персональными данными; будут построены безопасные системы, устойчивые к киберугрозам на любом этапе цифровой трансформации.

Следовательно, можно констатировать, что в Великобритании запущен процесс трансформации правительства «из организации, предоставляющей продукты и услуги, опирающиеся на данные, в организацию, в первую очередь, руководствующуюся своими данными и использующую такие данные не только для предоставления существующих продуктов и услуг, но и для создания новых»[35].

Отдельно хотелось бы также отметить, что для того, чтобы помочь гражданам, которые имеют недостаточные цифровые навыки, британское правительство намерено предоставить им бесплатное обучение. В обучении взрослых и детей будут участвовать и организации частного сектора, такие как *Google,* банки *Lloyds Banking Group, Barclays*[36]. Мы обратили внимание на этот пункт *Digital Strategy* Великобритании не случайно. Дело в том, что все усилия по цифровизации экономики и правительственного управления будут напрасны, если население не готово «принять» их, пользоваться новыми сервисами и платформами, а некомпетентные в информационной сфере чиновники будут не в состоянии обеспечивать технический прогресс, более того, будут его тормозить.

В связи с этим, представляет интерес опыт Германии, традиционно занимающей высокие места в рейтинге развития электронного правительства (поднялась в общем рейтинге 2016 г. на 6 пунктов). Началом развития электронного правительства в Германии считают 1998 г. И с самого начала одним из главных пунктов реализации немецкого электронного правительства стало повышение компьютерной грамотности населения, включенное в проект *Media@ Komm*. Еще в 2000 г. канцлер Германии Герхард Шредер в своем обращении к парламенту на тему «Жизнь, обучение и работа в информационном обществе» отметил в качестве важнейшего шага на пути к формированию электронного правительства то, что навыки пользования интернетом должны стать частью общего образования. В результате в ходе реализации проектов по развитию электронного правительства, власти ФРГ получили также и общественную среду, подготовленную к новшествам и трансформации к цифровому виду.

Сегодня главным веб-ресурсом, обеспечивающим гражданам и предприятиям Германии онлайн-доступ к правительственным структурам и сервисам, считается портал *www.bund.de.* 17 июня 2013 г. Федеральный Совет ФРГ (*Bundesrat*) одобрил закон «О поддержке электронного правительства

[34] Правительство Британии становится на путь цифровой трансформации // d-russia.ru. – 2017, 15 февр. [The British Government is on the Path of Digital Transformation // d-russia.ru, 2017, 15 Feb] Режим доступа: http://d-russia.ru/pravitelstvo-britanii-stanovitsya-na-put-tsifrovoj-transformatsii.html

[35] Аналитический доклад «Цифровое правительство 2020: Перспективы для России» [Analytical Report "Electronic Government 2020: Prospects for Russia"] / IIS. Режим доступа: http://www.iis.ru/docs/DigitalGovernmentRussia2020RUS.pdf

[36] Власти Великобритании опубликовали стратегию развития цифровых технологий / d-russia.ru, 2017, 3 марта [The UK Authorities Have Published a Strategy for the Development of Digital Technologies / D-Russia, 2017, March 3]. Режим доступа: http://d-russia.ru/vlasti-velikobritanii-opublikovali-proekt-strategii-razvitiya-tsifrovyh-tehnologij.html

(электронного управления)», сокращенно *E-Government-Gesetz*, а 17 сентября 2014 г. была принята программа «Цифровое управление 2020» (*DigitaleVerwaltung 2020*), ориентированная на полную «оцифровку» работы правительства, эффективную электронную административную работу в федеральном правительстве совместно с муниципалитетами, простые, быстрые процедуры взаимодействия на всех уровнях государственных служб, уменьшение ненужной бюрократии; создание единого свободного пространства для граждан и предприятий.

Как видим, просто дальнейшего наращивания количества оказываемых государственных услуг и развития инфраструктуры в современном мире уже недостаточно. Необходимо в принципе пересматривать концепцию государственного управления, ориентируя правительство прежде всего на работу с данными, превращая его в цифровую организацию, а также реализовывать программы повышения грамотности населения и госслужащих. Понимания этого в Российской Федерации еще не произошло, потому что в Стратегии развития информационного общества в Российской Федерации на 2017-2030 гг., утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203[37], все еще встречаются пункты вроде такого: «Применение в органах государственной власти Российской Федерации новых технологий, обеспечивающих повышение качества государственного управления». То есть законодатель до сих пор воспринимает информационные технологии всего лишь как дополнительный инструмент государственного управления, отказываясь при этом менять саму его структуру.

Последним в нашей компоративной процедуре является несомненно важнейший из вопросов, зачастую стоящий во главе угла при развитии информационного общества, – речь идет об основных направлениях правовой политики в сфере обеспечения информационной безопасности, в том числе (и в первую очередь!) в сети Интернет.

Говоря о безопасности чего-либо, необходимо рассматривать две составляющие этого понятия: безопасность как состояние защищенности объекта (в нашем случае информации) от внешних угроз и безопасность как безвредность самого объекта для окружающих. В Доктрине информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 5 декабря 2016 г. № 646)[38], которая выступает основным стратегическим документом, определяющим государственную политику в этой области, закрепляется подход к определению информационной безопасности государства как к состоянию защищенности личности, общества и государства от внутренних и внешних информационных угроз, а среди средств обеспечения информационной безопасности присутствуют и правовые, направленные на совершенствование механизмов регулирования общественных отношений, возникающих в информационной сфере. Доктрина информационной безопасности также определяет в качестве стратегических направлений обеспечения информационной безопасности следующие:

– соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;

– информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;

[37] О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы / Сайт Президента России, 2017 [On the Strategy for the Information Society Development in the Russian Federation for 2017-2030 / Website of the President of Russia, 2017]. Режим доступа: http://kremlin.ru/acts/bank/41919/page/1

[38] Собр. законодательства Рос. Федерации. 2016. № 50, ст. 7074.

– развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;

– ащита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Однако стратегические документы должны обновляться каждые шесть лет, а потому отслеживание развития схожих направлений в мировом сообществе несомненно остается актуальным. Тем более если учитывать, что процесс поиска удачных правовых конструкций в данной сфере нельзя считать завершенным ни в одном государстве мира. Виртуальное пространство как среда коммуникации имеет ряд особенностей, связанных с ее глобальностью, отсутствием границ, интерактивностью, относительной анонимностью, поэтому некоторые вопросы могут быть решены только на уровне международных организациях и уже не первый год идет речь о гармонизации национальных законодательств в сфере информационной безопасности.

Подобные нашей Доктрине информационной безопасности стратегические документы приняты и в других странах.

Так, в США таким стратегическим документом остается «Международная стратегия США для киберпространства», утвержденная в 2011 г. Б. Обамой. Этот документ базируется на трех принципах: свободе самовыражения, неприкосновенности частных данных, свободном доступе к информации. Вышеназванная стратегия для киберпространства уделяет особое внимание нормам международного права, подчеркивая, что существующие подобные нормы мирного поведения и разрешения конфликтов вполне применимы и в киберпространстве. При этом в ней признается, что следует поработать для того, чтобы понять, как и в каком виде эти нормы следует применять[39].

В Международной стратегии США для киберпространства декларируются три основных направления, которых придерживаются американцы в отношении обеспечения кибербезопасности: улучшение международных дипломатических отношений, отражение и предотвращение нападений посредством улучшения систем защиты, содействие всеобщему процветанию и безопасности посредством инвестиций в их развитие. Также здесь подробно раскрываются семь приоритетных направлений развития безопасной, надежной и доступной сети Интернет:

– продвижение международных стандартов и поддержка открытых рынков в целях экономического роста;

– повышение безопасности, надежности и отказоустойчивости глобальных сетей;

– развитие сотрудничества в правоприменительной сфере и обеспечение соблюдения законов;

– готовность вооруженных сил к противостоянию угрозам в киберпространстве;

– создание эффективных структур управления Интернетом;

– наращивание возможностей повышения безопасности и процветания;

– построение в Интернете системы фундаментальных свобод и прав на частную собственность[40].

В рамках реализации стратегии за прошедшее время в США было запущено несколько программ с учетом усиления описанных угроз, причем рост количества инициатив по обеспечению безопасности здесь стимулирует возрастающее количество угроз. Например, был повышен статус так называемого киберподразделения Пентагона, которому значительно расши-

[39] См.: Чарльз Барри о подходах США и НАТО в области международной информационной безопасности // d-russia.ru. – 2015, 1 мая. [Charles Barry on the Approaches of the United States and NATO in the Field of International Information Security // *d-russia.ru*, 2015, May 1] Режим доступа: https://digital.report/charlz-barri-o-podhodah-ssha-i-nato-v-oblasti-mezhdunarodnoy-informatsionnoy-bezopasnosti/

[40] Ibid.

рили полномочия и вывели из-под контроля Агентства национальной безопасности (АНБ), а в конце 2017 г. Палата представителей большинством голосов приняла проект закона по созданию Агентства по кибербезопасности и безопасности инфраструктуры, главной задачей которого станет защита и повышение безопасности и устойчивости кибербезопасности США, связи в случае чрезвычайных ситуаций и критически важной инфраструктуры[41].

В целом, анализ основного стратегического документа США в сфере информационной безопасности и их дальнейших действий (в составе НАТО) в последнее время говорят об усилившемся внимании к кибернетическому противостоянию.

В отличие от США, китайские стратегические документы в сфере информационной безопасности придерживаются политики «мягкой силы» и невмешательства в дела других государств. Вообще, в Китае существует целый ряд документов, определяющих стратегию государства в области информационной безопасности: Стратегия развития информатизации на 2006-2020 гг. (утверждена в 2006 г.), Государственная стратегия по развитию информатизации (утверждена в 2016 г.), Закон КНР о кибербезопасности (принят в 2016 г.)[42]. Принятие в 2016 г. пакета важных стратегических документов в Китайской Народной Республике свидетельствует о том, что кибербезопасность постепенно стала важнейшим аспектом национальной безопасности государства.

В целом стратегические документы в качестве основных принимают концепции «активной обороны» и «симметричного ответа на возникающие вызовы»; декларируют принципы мира, открытости, безопасности и сотрудничества; продвигают идеи «здорового информационного общества», «развития интернет культуры в Китае», «строительства информационной площадки для социализма с китайской спецификой»; заявляют, что китайское политическое руководство единолично управляет собственным информационным пространством (государственные структуры на разных уровнях власти получают обширные полномочия в области контроля над Интернетом). Курс Китайской Народной Республики в области информационной безопасности можно разделить на внутренний и внешний. К первому направлению относится ограничение доступа к определенным информационным и новостным интернет ресурсам (запрет на внешние социальные сети), запрет на использование иностранного программного обеспечения и средств передачи голосовых и текстовых сообщений, тотальный контроль над социальными сетями и интернет-трафиком в целом. К внешнему направлению политического курса в области кибербезопасности КНР относятся кибератаки и прочие действия специализированных государственных подразделений в информационной сфере для нанесения ущерба или повреждения критически важной инфраструктуры сил противника в случае вероятной информационной войны или конфликта.

Имея огромный опыт в области воздействия на сеть Интернет, позволяющий нейтрализовать информацию, которая может нанести вред человеку и подорвать государственную безопасность, Китай предлагает свой опыт и для мирового сообщества. Так, 6 декабря 2012 г. в ходе конференции Международного союза электросвязи (далее – МСЭ) в Дубае по инициативе Китая был официально утвержден стандарт Y.2770 по глубокой инспекции пакетов (*Deep Packet Inspection, DPI*).

Среди стран Евросоюза распространен подход к информационной безопасности с позиций защиты интересов страны и инновационного развития экономики. Особенно ярко это выражается в законодательстве по

---

[41] В США создадут агентство по кибербезопасности (In the United States a Cyber Security Agency will be Established) / d-russia.ru, 2017, 12 дек. Режим доступа: https://digital.report/v-ssha-sozdadut-agentstvo-po-kiberbezopasnosti/

[42] Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. – 2017. Режим доступа: https://cyberleninka.ru/article/v/politika-knr-po-obespecheniyu-kiberbezopasnosti [Razumov, E.A. Politika KNR po obespecheniju kiberbezopasnosti (China's Cybersecurity Policy) // *Rossija i ATR*, 2017. Mode of access: https://cyberleninka.ru/article/v/politika-knr-po-obespecheniyu-kiberbezopasnosti]

информационной безопасности Финляндии, где кибербезопасность воспринимают как проблему экономического характера, мешающую развитию финского информационного общества[43].

Таким образом, мы видим, что Доктрина информационной безопасности Российской Федерации, являясь логичной реакцией на политику стран Североатлантического Альянса в отношении информационной безопасности, созвучна аналогичным иностранным документам.

Заключение

Проведенное сравнение национальных законодательств различных стран по отдельным вопросам информационного права (информационные права и свободы; электронное управление; информационная безопасность) представляется актуальным и полезным в свете процесса развития информационного общества.

Реализация основных прав и свобод граждан в информационной сфере занимает особое место среди национальных интересов большинства государств. При этом все права личности могут быть ограничены правами и свободами других лиц. Ограничения в информационной сфере рассмотрены нами на примере сравнения методов управления контентом глобальной сети в отдельных государствах – от когда-то полностью свободного Интернета в США до жесткой узаконенной цензуры и фильтрации интернет-трафика в Китае. Основной вывод в данной области – сегодня модель саморегулирования глобальной сети не находит применения ни в одной стране мира: государство определяет для себя только уровень вмешательства в сетевую жизнь граждан и методы обеспечения вмешательства.

Что касается электронного управления в различных государствах, то в этом случае речь идет о переходе от концепции «электронного правительства» к модели «цифровое правительство», связанного с преобразованием всей структуры государственного управления. Здесь ценен опыт Великобритании, где реализуется проект «Правительство как платформа», и Германии, где построение «электронного правительства» в принципе начиналось с повышения информационной культуры граждан и служащих.

Вопросы информационной безопасности сегодня выходят на первое место в большинстве государств и международных организаций, ведь воздействие на социум при помощи информации может быть гораздо эффективнее, чем прямые угрозы. В целом, направления обеспечения информационной безопасности во всех странах похожи, что получило отражение в том числе и в российских документах стратегического характера по этому вопросу.

[43] Мучаев А. Доктрина информационной безопасности: как относятся к киберугрозам в других странах // *Госиндекс*. – 2016, 7 дек. Режим доступа: http://gosindex.ru/doktrina-informatsionnoj-bezopasnosti-kak-otnosyatsya-k-kiberugrozam-v-drugih-stranah/ [Muchaev, A. Doktrina informacionnoj bezopasnosti: kak otnosjatsja k kiberugrozam v drugih stranah (Information Security Doctrine: How Do Cyber Threats Relate to Other Countries?) // *Gosindeks*, 2016, 7 Dec. Mode of access: http://gosindex.ru/doktrina-informatsionnoj-bezopasnosti-kak-otnosyatsya-k-kiberugrozam-v-drugih-stranah/]

Литература:

Аналитический доклад «Цифровое правительство 2020: Перспективы для России» / IIS. Режим доступа: http://www.iis.ru/docs/DigitalGovernmentRussia2020RUS.pdf

Анисимова А.С. Анализ правотворческой политики зарубежных стран в сфере регулирования интернет-отношений // Вестник Саратовской государственной юридической академии. – 2014. – № 5.

Динамика институтов информационной безопасности. Правовые проблемы. Сб. науч. трудов / Отв. ред. Т.А. Полякова, В.Б. Наумов, Э.В. Талапина. – М.: ИГП РАН – Изд-во «Канаон+» РООИ «Реабилитация», 2018. – 264 с.

Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. – М.: Статут, 2013.

Мосин О.В. Права человека в Конституции Франции / ЮрКлуб, 2008. Режим доступа: http://www.yurclub.ru/docs/other/article117.html

Мучаев А. Доктрина информационной безопасности: как относятся к киберугрозам в других странах // *Госиндекс*. – 2016, 7 дек. Режим доступа: http://gosindex.ru/doktrina-informatsionnoj-bezopasnosti-kak-otnosyatsya-k-kiberugrozam-v-drugih-stranah/

Правовая жизнь современного российского общества: уровни, срезы, сегменты / (Анисимова А.С. и др.); под ред. А.В Малько. – Москва: Юрлитинформ, 2016. – 354 с.

Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. – 2017. Режим до-

ступа: https://cyberleninka.ru/article/v/politika-knr-po-obespecheniyu-kiberbezopasnosti

Чарльз Барри о подходах США и НАТО в области международной информационной безопасности // d-russia.ru. – 2015, 1 мая. Режим доступа: https://digital.report/charlz-barri-o-podhodah-ssha-i-nato-v-oblasti-mezhdunarodnoy-informatsionnoy-bezopasnosti/

References:

Analiticheskij doklad «TSifrovoe pravitel'stvo 2020: Perspektivy dlya Rossii» (Analytical Report "Electronic Government 2020: Prospects for Russia") / IIS. Mode of access: http://www.iis.ru/docs/DigitalGovernmentRussia2020RUS.pdf

Anisimova, A.S. Analiz pravotvorcheskoi politiki zarubezhnykh stran v sfere regulirovaniia internet-otnoshenii (Analysis of Lawmaking in Foreign Policy the Regulation of Internet Relationships) // Vestnik Saratovskoi gosudarstvennoi iuridicheskoi akademii, 2014, No. 5.

Dinamika institutov informacionnoj bezopasnosti. Pravovye problemy. Sb. nauch. trudov (Dynamics of Information Security Institutions. Legal Issues) / Ed. T.A. Poljakova, V.B. Naumov, Je.V. Talapina. Moscow: IGP RAN – Izd-vo «Kanaon+» ROOI «Reablitacija», 2018. 264 p.

Kiberbezopasnost' i upravlenie internetom: Dokumenty i materialy dlja rossijskih reguljatorov i jekspertov (Cybersecurity and Internet Governance: Documents and Materials for Russian Regulators and Experts) / Ed. M.B. Kasenova; Comp. O.V. Demidov, M.B. Kasenova. Moscow: Statut, 2013.

Mosin, O.V. Prava cheloveka v Konstitucii Francii (Human Rights in the French Constitution) / YurKlub, 2008. Mode of access: http://www.yurclub.ru/docs/other/article117.html

Muchaev, A. Doktrina informacionnoj bezopasnosti: kak otnosjatsja k kiberugrozam v drugih stranah (Information Security Doctrine: How Do Cyber Threats Relate to Other Countries?) // *Gosindeks*, 2016, 7 Dec. Mode of access: http://gosindex.ru/doktrina-informatsionnoj-bezopasnosti-kak-otnosyatsya-k-kiberugrozam-v-drugih-stranah/

Pravovaya zhizn sovremennogo rossijskogo obshchestva: urovni, srezy, segmenty (Legal Life of Modern Russian Society: Levels, Sections, Segments) / (Anisimova A.S. and oth.) ed. by A.V. Malko. Moskow. Yurlitinform, 2016. 354 p.

Razumov, E.A. Politika KNR po obespecheniju kiberbezopasnosti (China's Cybersecurity Policy) // Rossija i ATR, 2017. Mode of access: https://cyberleninka.ru/article/v/politika-knr-po-obespecheniyu-kiberbezopasnosti

Charles Barry o podkhodakh SSHA i NATO v oblasti mezhdunarodnoj informatsionnoj bezopasnosti (Charles Barry on the Approaches of the United States and NATO in the Field of International Information Security) // d-russia.ru, 2015, May 1. Mode of access: https://digital.report/charlz-barri-o-podhodah-ssha-i-nato-v-oblasti-mezhdunarodnoy-informatsionnoy-bezopasnosti

DOI: 10.24411/2221-3279-2019-10003

LEGAL ASPECTS OF INFORMATION POLICY IN THE MODERN SOCIETY: A COMPARATIVE ANALYSIS

Aleksandr V. Mal'ko

Saratov Branch of the Institute of State and Law of the Russian Academy of Sciences, Saratov, Russia

Oksana L. Soldatkina

Saratov State Law Academy, Saratov Branch of the Institute of State and Law of the Russian Academy of Sciences, Saratov, Russia

Article history:

Received:

19.03.2018

Accepted:

01.11.2018

About the authors:
Aleksandr V. Mal'ko, Dr of Law, Professor,
Distinguisged Researcher of Russia;
Director, Saratov Branch of the Institute
of State and Law of the Russian Academy of Sciences

e-mail: i_gp@ssla.ru

Oksana L. Soldatkina, Candidate of Legal Sciences,
Associate Professor, Informatics Department,
Saratov State Law Academy;
Senior Research Associate,
Saratov Branch of the Institute of State and Law
of the Russian Academy of Sciences

e-mail: buzum@mail.ru

Key words:
Information-legal policy; information security;
Government as Platform;
US International Strategy for Cyberspace;
Basic Law of the Federal Republic of Germany;
Cyber Cybersecurity Law of China;
Digital Strategy of Great Britain

Abstract: The article contains a comparative analysis of the main directions of the information policy of different states in three areas: information rights and freedoms, e-government and information security. Such a comparison is an actual character because the problems of information law are often global, and the legal regulation of information relations has an international component. Based on the results of the comparison of national legislations of different countries conducted in the article on certain issues of the information law, the following conclusions are made. Realization of the basic rights and freedoms of citizens in the information sphere occupies a special place among the national interests of most countries, but the rights of the individual can be limited. Legal restrictions in the information field are considered on the example of comparison of methods of content management of the global network, which are characterized by the state's definition of the level of interference in the network life of citizens and methods of ensuring intervention. Electronic governance in various states is characterized by a transition from the concept of «e-government» to the «digital government» model associated with the transformation of the entire structure of public administration. In this field, the UK experience is valuable, where the "Government as a platform" project is being implemented, and Germany, where the construction of «e-government» basically began with the enhancement of the information culture of citizens and civil servants. Information security today comes out on top in the majority of countries and international organizations. In general, information security trends in all countries are similar, which is reflected in the Russian strategic documents.

Для цитирования: Малько А.В., Солдаткина О.Л. Информационно-правовая политика в современном обществе: сравнительный анализ// *Сравнительная политика*. – 2019. – № 1. – С. 42-58.

DOI: 10.24411/2221-3279-2019-10003

For citation: Mal'ko, Aleksandr V.; Soldatkina, Oksana L. Informacionno-pravovaya politika v sovremennom obshchestve sravnitelnyj analiz (Information Legal Policy in the Modern Society: Comparative Analysis) // *Comparative Politics Russia,* 2019, No. 1, pp. 42-58.

DOI: 10.24411/2221-3279-2019-10003