Санкт-Петербургский государственный университет

Илья Николаевич МАКАРОВ

Выпускная квалификационная работа

НОРМАТИВНЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ СЕТИ ИНТЕРНЕТ КАК ФАКТОР ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ

Направление 41.03.04 «Политология»

Основная образовательная программа бакалавриата «Политология»

Научный руководитель:
кандидат политических наук, доцент
Ольга Диомидовна САФОНОВА

Рецензент:
кандидат политических наук, доцент
Александр Андреевич НИКИФОРОВ

Санкт-Петербург
2018

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Информационно-коммуникационные технологии (ИКТ) являются одним из наиболее важных факторов, влияющих на формирование общества XXI века. Всё возрастающая роль информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации является одной из основных характеристик современного этапа развития человечества[1]. Образ жизни людей, их трудовая деятельность, досуг, и даже их множественные взаимодействия с государством в рамках гражданского общества претерпели на себе воистину революционное воздействие ИКТ.

Незаметно для большинства, ИКТ стали жизненно важным стимулом и фактором развития не только национальных экономик, но и общемировой глобальной экономики. ИКТ не просто помогают развивать коммуникацию между различными политическими и эконмическими акторами, но и открывают передо всем миром огромные возможности. Они позволяют как частным лицам, так и коммерческим организациям творчески и эффективно решать поставленные перед собой задачи. Не осталась незатронутой и сфера межнациональных глобальных коммуникаций: ИКТ оказали серьезное влияние на международные отношения в последние два десятилетия.

Как отмечает отечественный специалист в области информационной безопасности П. Шариков, «активное распространение, внедрение и использование информационных технологий быстро привело к тому, что эти технологии стали применяться не только как средство обмена и обработки информации, но и как способ нанесения ущерба»[2]. В последние несколько лет термины с приставкой «кибер» получили широкое употребление в международно-политическом дискурсе и нашли свое отражение в

---

[1] Окинавская Хартия глобального информационного общества. UNESCO's Global Search Engine EN. URL: http://www.unesco.org/new/fileadmin/MULTIMEDIA/FIELD/Tashkent/pdf/okinawa_charter_ru.doc (Дата обращения 16.11.2017)

[2] Шариков П. А. Информационный комплекс / Безопасность Европы / Ин-т Европы РАН. - М.: Весь мир, 2011. - С. 581-591.

стратегических доктринах не только государств, но и международных организаций.

Основной проблематикой в исследовании «безопасности информации» или «информационной безопасности» является трудность в определении природы, и что важнее, деструктивного потенциала информационных угроз. П. Корниш, бывший эксперт Лондонского Королевского Института Иностранных Дел (англ. Chatam House) приводит следующую классификацию информационных угроз[3]:

1) противозаконный действия «хакеров – одиночек, т.е. взломщиков компьютерных сетей;
2) организованная преступность, действующая в глобальных интернет-сетях;
3) идеологический и вытекающий из него политический экстремизм;
4) информационная агрессия, проводимая государством как по отношению к собственными обществу, так и во внешних взаимоотношениях с другими международно-политическими акторами.

На сегодняшний день только первые две разновидности угроз из данной классификации обрели практическое воплощение в мировой политике. Что касается кибертерроризма и кибервойны между государствами, то они не являются явными и оформленными угрозами, которые, тем не менее, могут быть реализованы в будущем. Поэтому для политических элит зачастую сложно однозначно ответить на вопрос, действительно ли информационные атаки несут серьезную угрозу национальной безопасности[4].

Таким образом, вышеперечисленные элементы «проблемного поля» – отсутствие единого понятийного пространства и международно-правовых конвенций, значимая роль новых акторов международных отношений, непрозрачные механизмы воздействия в Интернет-среде – позволяют рассматривать глобальное информационное пространство как «серую зону»

[3] Cornish, P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks//Directorate-General for External Policies of the Union/Policy Department. – Brussels: European Parliament, 2009. – 34 p.
[4] Geers, K. Strategic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence, 2011. – 169 p.

мировой политики. Как отмечают Д. Балуев и А. Новоселов, «серая зона» выглядит как «черный ящик», на входе в который мы имеем риски низкого уровня, порождаемые новыми акторами. На выходе же появляются серьезные угрозы существованию традиционных акторов – государств»[5].

Исходя из выше сказанного, отметим, что, раскрывая содержание термина информационной безопасности самым поверхностным образом, специалисты неминуемо приходят к вопросу о её (информационной безопасности) правовом статусе. Особое место среди бурно развивающихся вычислительных сетей занимает наиболее глобальная всемирная система сетей – Интернет. Состоящий из многих тысяч корпоративных, научных, правительственных и домашних компьютерных сетей, Интернет также, как и другие сложные информационно-коммуникативные сети, не находится под чьим-либо единоличным управлением, в том числе, какого-либо государства или коммерческой организации. Именно поэтому комплексное регулирование Сети довольно сложно, но вполне осуществимо. Возникающие в разнообразных политико-правовых средах дискуссии о государственном и правовом регулировании «Всемирной Паутины», так или иначе, сводятся к поиску ответа на вопрос: существует ли острая необходимость в нормативном регулировании Интернета, ровно, как и в специфической государственной политике по отношению к Сети. Возможно, ввиду отсутствия прямого и бескомпромиссного ответа на данный вопрос, всё ещё отсутствуют даже международно-правовые механизмы, позволявшие бы отстаивать суверенное право государств на регулирование в национальном сегменте интернета. Отсутствие норм, регулирующих межгосударственные отношения в этой сфере, затрудняют формирование системы международной информационной безопасности, направленной на достижение стабильного и равноправного партнёрства, как на уровнях G2G (межгосударственный), B2B

[5] Балуев, Д. Г. «Серые зоны» мировой политики. Очерки текущей политики/Д. Г. Балуев, А. А. Новоселов; отв. ред. М. А. Троицкий. – М.: Научно-образовательный форум по международным отношениям, 2010. – Выпуск 3. – 40 с.

(коммерческий), так и на уровнях B2G и G2B (взаимодействия государственной власти и бизнес-структур).

Актуальность исследуемой темы определяется в первую очередь невероятной динамикой развития информационно-телекоммуникационной сети Интернет в первом десятилетии XXI века, а также многогранным комплексом насущных проблем, связанных с вопросами администрирования Интернета, защищённости законных прав личности и общества в информационной сфере, сохранности информационных ресурсов государства, а также неуклонным ростом числа абонентов этой сети, влияние которой на образ жизни людей стало революционным. Существующая система взглядов в вопросах обеспечения национальной безопасности в целом является более чем разнообразной: отсутствуют единые теоретические подходы к её определению, что служит очевидным препятствием к формированию комплексной политики государственного регулирования различных составляющих информационной сферы, в том числе, и сети Интернет. На данный аспект указывает ряд отечественных политологов, в том числе, факультета политологии Санкт-Петербургского Университета: Александр Андреевич Никифоров[6], Николай Алексеевич Баранов[7] , а также другие исследователи политической науки, например, Анатолий Васильевич Возженников[8] и Казаковцев Алексей Васильевич[9].

Вхождение Российской Федерации в начале 1990-х гг. в единое мировое информационное пространство наложило на её руководство ряд обязательств в области доступа всех граждан к информационным и коммуникационным сетям. Система информационной безопасности была создана в том числе и для защиты

---

[6] Никифоров А.А. Возможности и ограничения протестной мобилизации через социальные сети // Право и политика. – 2014. – № 12. – С. 1903-1909.

[7] Баранов Н.А. Интегративный контекст национальной безопасности российского общества//Механизмы формирования гражданской идентичности в Российской Федерации: сборник статей и материалов Всероссийской научно-практической конференции «Механизмы формирования гражданской идентичности в Российской Федерации» (6-7 декабря 2013 г., г. Казань)/Под ред. А.Г.Большакова, Е.А.Терешиной. Казань: Казан. ун-т, 2014. – с. 172-182

[8] Возженников А.В. Национальная безопасность России: методология исследования и политика обеспечения: Монография. – М.: Изд-во РАГС, 2002. – 424 с.

[9] Казаковцев, А. В. НАТО и Кибербезопасность//Вестник Волгоградского государственного университета. Серия 4: История. Регионоведение. Международные отношения. – 2012. С. 109-114.

и обеспечения соблюдения конституционных прав и свобод человека и гражданина в данной области общественных отношений.[10].

Системообразующий характер, которая приобрела в наши дни Информационная сфера жизни общества, определяет зависимое состояние политической, экономической, оборонной и других составляющих внутренней и внешней национальной безопасности Российской Федерации, которая на данный момент исторического развития критически нуждается в наличии комплексной правовой основы, а также отлаженной системы, механизмов и принципов её обеспечения. На наш взгляд, беспрерывный качественный рост технического развития и количественный рост абонентов глобальных информационных сетей эта зависимость, будет неуклонно возрастать для всех суверенных образований, в том числе России.

Актуально артикулировать и изучить основы правового обеспечения информационной безопасности Российской Федерации в сфере регулирования сети Интернет, его цели, задачи и принципы, проведя подробный анализ нормативно-правовых актов, как федерального, так и международного уровня, выявив механизмы его правового регулирования.

Объект исследования – общественные отношения, складывающиеся в сфере информационной безопасности Российской Федерации.

Предмет исследования – нормативные правовые акты Российской Федерации, регулирующие и контролирующие деятельность физических, юридических лиц и государственных образований в сфере и по поводу сети Интернет, как неотъемлемый компонент обеспечения безопасности функционирования информационной инфраструктуры России.

Цель – посредством политологического и целостно-логического анализа правовых источников информационной безопасности Российской Федерации в

[10] Шерстюк В.П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной безопасности. – М.: Информационное общество, 1999, вып. 5, с. 3 – 5.

сфере регулирования сети Интернет, выявить его особенности, существующие проблемы в функционировании.

Целевая установка ВКР работы реализуется посредством решения следующих основных задач:

- определить предметное поле информационной безопасности в рамках политической науки;
- выявить основные подходы к определению правового статуса сети Интернет, а также артикулировать понятие «интернет-право», как смежной отрасли права;
- обозначить существующие в России механизмы правового регулирования сети Интернет;
- раскрыть недостатки в реализации конституционных прав и свобод российских граждан в интернет-среде.

Методологическая основа дипломной работы

В данной работе раскрываются основные подходы к рассмотрению национальной безопасности с политологической точки зрения. Была предпринята попытка понять юридическую природу сети Интернет, и на основе обзора законодательства, как российского, так и зарубежного, а также сложившейся практики отношений в сети, раскрыть основы государственного регулирования Интернета как одного из ключевых факторов защиты национальной безопасности страны в информационной сфере. В методологическом плане выпускная квалификационная работа построена на использовании теоретико-фундаментального политического анализа, т.е. «political analysis» (общий анализ политики)[11], формально-юридического, а также сравнительно-правового методов.

Первая глава выпускной квалификационной работы базируется на использовании метода теоретического политологического анализа, как максимально объективного языка для описания политической реальности, в частности, для чёткого определения предметного поля исследования, наиболее

[11] Ирхин Ю. В. Методология и методика современного политического анализа: подходы и проблемы. – 2012, с. 71-79.

ясного и, в тоже время, достаточно широкого для достижения поставленных задач.

Для рассмотрения политико-правовых основ обеспечения информационной безопасности методологически значимым для данной работы является интегративный подход (как особую методологию, его наиболее подробно раскрыли советские правоведы – В.Н.Кудрявцев и В.П.Казимирчук)[12,13], фиксирующий тесную взаимосвязь между правовыми и фактическими общественно-политическими отношениями. Большая часть работы, исходя из тематики исследования, построена на сочетании политологического, нормативного и сравнительно-правового нормативного анализов, а нормативной основой ВКР выступают правовые норм и институты российского и международного законодательства. Нормативной базой для раскрытия значительной части объекта могут служить конкретные положения Конституции РФ, федеральные конституционные и федеральные законы России, положения Гражданского кодекса РФ (далее – ГК), подзаконные нормативные акты, особое внимание уделено правовым политическим доктринам и нормам международного права.

Эмпирическую основу дипломной работы составили тексты государственных федеральных законодательных актов, законодательных актов субъектов Федерации, подзаконных установлений. В рамках распространенного подхода национальная безопасность как объект научного политологического знания рассматривается с точки зрения менеджмента возможных угроз. В рамках этого подхода к научному понимаю национальной безопасности также заслуживают внимания работы теоретика вопросов стратегии информационных войн, Почепцова Г.Г.[14, 15].

---

[12] Кудрявцев В. Н., Васильев А. М. Право: развитие общего понятия// СОВ. гос-во и право. 1985. № 7. С. 12–13.
[13] Казимирчук. В Л Социологические проблемы действия права в социалистическом обществе//Право и социология –М, 1973 С. – 60.
[14] Почепцов Г. Г. Информационные войны. Новый инструментарий политики. – М.: Алгоритм, 2015
[15] Почепцов Г. Г. Контроль над разумом. – К.: КМА, 2012. – 350 с.

Степень изученности темы исследования.

Относительно недавно проблема информационной безопасности вошла в область научных интересов исследователей политических процессов, традиционно оставаясь предметом исследования информатики и юриспруденции. Представители российской политической науки изучают различные политические аспекты и проблемы, связанные с функционированием и государственным регулированием крупных информационных сетей, в т. ч. сеть Интернет[16]. Таким образом, научные труды сотрудников факультета Политологии Санкт-Петербургского Государственного Университета (в особенности монографии И.В. Радикова, Н. А. Баранова)[17, 18] и прочих российских и зарубежных политологов о проблемах информационной безопасности в эпоху глобализации[19], которые проводят фундаментальный политологический анализ в тематических работах фокусируются на информационной безопасности как таковой. Другие же, например кандидат политических наук, преподаватель факультета политологии СПбГУ Денис Сергеевич Мартьянов, в своих научных трудах своё внимание останавливают на взаимодействии крупных, относительно автономных информационных сетей (основными акторами которых выступают крупные группы производителей и потребителей информации), в т.ч. и Интернет с государством[20], либо на правовом регулировании государством этих сетей, без какой-либо тематической привязки

[16] Гребенькова Л.А. Блокировка сайтов как метод борьбы с нарушением авторских и смежных прав в Интернете//Известия Юго-Западного государственного университета. Серия История и право № 4. – 2014

[17] Радиков И. В. Безопасность как ценностный императив мировой политики//Универсальные ценности в мировой и внешней политике/Под редакцией П.А. Цыганкова. – М.: Издательство Московского университета, 2012 – с. 51-59

[18] Баранов Н. А. Интегративный контекст национальной безопасности российского общества//Механизмы формирования гражданской идентичности в Российской Федерации: сборник статей и материалов Всероссийской научно-практической конференции «Механизмы формирования гражданской идентичности в Российской Федерации» (6-7 декабря 2013 г., г. Казань)/Под ред. А.Г.Большакова, Е.А.Терешиной. Казань: Казанский университет, 2014. – с. 172-182

[19] Глебов, И.Н. Национальная безопасность Российской Федерации: проблемы правового регулирования. – СПб, 2000. – 98 с.

[20] Мартьянов Д. С. Практика взаимодействия интернет-сообщества и политических акторов в современной России. Диссертация на соискание учёной степени кандидата наук. Спб – 214 с

государственного надзора в этой сфере к обеспечению информационной безопасности[21].

Над решением теоретических и практических проблем национальной безопасности в последние годы плодотворно работают представители и других наук. В диссертации В.А. Каламанова исследуется ряд вопросов, связанных с формированием национальных интересов России как важнейшей составляющей национальной идеологии, проводится классификация национальных интересов, дан анализ самого понятия национальной безопасности[22]. Также в диссертации Идрисова Р. Ф. рассмотрен комплекс проблем конституционного права, государственного управления, правовые аспекты анализа отношений, возникающих в области обеспечения национальной безопасности РФ, в том числе урегулирования международных и локальных конфликтов[23].

К проблемам национальной безопасности обращаются в рамках научных исследований в том числе и государственные деятели, политики. В частности, Д.О. Рогозиным, занимавшим различные государственные посты, от должности специального представителя президента Российской Федерации по проблемам Калининградской области, связанным с расширением Европейского союза до Заместителя председателя правительства РФ, историко-философскими методами были исследованы причины войн и военных конфликтов, связанных с исторической жизнедеятельностью России, разработаны методы, принципы и критерии по обеспечению ее национальной безопасности в условиях нового мирового порядка[24].

Указанные выше специалисты в своих узких областях научного знания при достаточно глубоком рассмотрении вопроса информационной безопасности сходятся в выделении следующей группы наиболее общих направлений

---

[21] Балашов А. Н. Правовое регулирование интернет-отношений: основные проблемы и практика реализации в России//Среднерусский вестник общественных наук. Том 11. Серия №2. – 2016

[22] Каламанов В.А. Национальная безопасность Российской Федерации и межнациональные конфликты (теоретико-правовой анализ). Диссертация на соискателя доктора юридических наук. – СПб.: 2001

[23] Идрисов Р. Ф. Теоретические и правовые проблемы обеспечения национальной безопасности Российской Федерации. Автореферат диссертации на соискателя кандидата доктора юридических наук. – М.: 2002

[24] Рогозин Д.О. Проблема национальной безопасности России на рубеже XXI века. Дисс. на соиск. докт. философ, наук. – М.: 2000

государственной политики в информационной сфере: защита собственного информационного пространства и вхождение в мировое информационное пространство; выявление и устранение причин информационной дискриминации; устранение негативных факторов распространения информационного пространства, информационной экспансии со стороны других государств; разработка и внедрение режимов получения, сохранения, распространения и использования общественно значимой информации.

Являясь авторитетным специалистом в изучении феномена информационных и «прокси-войн», представителем подхода менеджмента возможных угроз, Почепцов Г.Г. ещё в начале нового столетия определил угрозу информационной экспансии со стороны других государств, а также, что информационное пространство в первую очередь формируется существующими коммуникативными потоками[25].

Среди имеющихся работ, посвященных данной проблематике и написанных под авторством представителей различных гуманитарных наук, информационная безопасность рассматривается, во-первых, как неотъемлемое условие состояния и развития государственного устройства в сочетании с остальными сферами социальной жизни общества[26,27], где информационная безопасность предстает предметом политической, исторической или социологической наук, во-вторых, как правовой институт (элемент) в системе российского информационного права[28].

Выпускная квалификационная работа состоит из двух глав, объединяющих восемь параграфов, заключения и списка используемой литературы.

---

[25] Почепцов Г.Г. Национальная безопасность стран переходного периода. – Киев, 1996

[26] Баранов Н.А. Интегративный контекст национальной безопасности российского общества//Механизмы формирования гражданской идентичности в Российской Федерации: сборник статей и материалов Всероссийской научно-практической конференции «Механизмы формирования гражданской идентичности в Российской Федерации» (6-7 декабря 2013 г., г. Казань)/Под ред. А.Г.Большакова, Е.А.Терешиной. Казань: Казан. ун-т, 2014. – С. 172-182

[27] Радиков И. В. Безопасность как ценностный императив мировой политики//Универсальные ценности в мировой и внешней политике/Под редакцией П.А. Цыганкова. – М.: Издательство Московского университета, 2012 – с. 51-59

[28] Институты глобального управления: состояние и возможности//Внешняя политика в условиях глобальной неопределенности: монография/Под ред. П.А.Цыганкова. М.: Издательство Русайнс. 2017 С.116-133

Глава 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ НОРМАТИВНОГО РЕГУЛИРОВАНИЯ СЕТИ ИНТЕРНЕТ

1.1. Информационная безопасность государства с позиции политической науки

Национальная безопасность как комплексное явление политической, экономической, социальной, культурной жизни государств и международного сообщества в целом стала предметом достаточно многочисленных исследований историко-философского, правового, социологического, геополитического характера. Впервые понятие «национальная безопасность» в политике было употреблено в 1904 г. президентом США Т. Рузвельтом в послании к Конгрессу Именно интересами национальной безопасности обосновал президент Рузвельт присоединение зоны Панамского канала к территории США[29]. В последующие годы проблема национальной безопасности стала ведущей в политике и политической науке. Ею занимались такие известные политические исследователи и практики, как Г. Кан[30], Г. Киссинджер[31], Г. Лассуэлл[32], Дж. Шлезингер и др[33].

Национальная безопасность – явление многогранное. Представители различных наук (политологи, юристы, экономисты, социологи, историки и т.д.), исследующие национальную безопасность с позиций своей конкретной науки, могут давать этому термину собственные определения, отражающие специфическое понимание этого явления данной наукой. По определению российского политолога Н. А. Косолапова, национальная безопасность – это стабильность, которая может поддерживаться на протяжении длительного времени, состояние достаточно разумной динамической защищенности от

[29] Борщевский Г. А. Роль государства в формировании преемственного исторического сознания в контексте проблемы обеспечения национальной безопасности России // Информационный гуманитарный портал «Знание. Понимание. Умение». – 2012. – № 1 (январь – февраль)
[30] Herman Kahn On Thermonuclear War (1960)
[31] Kissinger H. A. The Necessity for Choice: Prospects of American Foreign Policy 1961
[32] Lasswell G. D. Propaganda Technique in the World War
[33] Glastris, Paul The powers that shouldn't be; five Washington insiders the next Democratic president shouldn't hire, The Washington Monthly (October 1987)

наиболее существенных из реально существующих угроз и опасностей, а также способности распознавать такие вызовы и своевременно принимать необходимые меры для их нейтрализации[34].

При этом отдельно стоит разобрать также научную концепцию национального интереса. В той мере, в какой задачи обеспечения национальной безопасности являются производными от национальных интересов, концепции национальной безопасности также связаны с теоретическим обобщением данных интересов. Концепция национального интереса относится к внешней политике и подчеркивает вторую сторону обеспечения власти – силу. Ее разработчик Г. Моргентау, американский политолог немецкого происхождения, один из основоположников школы «политического реализма», которая «базируется на трех постулатах: основным субъектом международных отношений является национальное государство, выражающее свои интересы в категориях силы (т.е. они обусловлены той силой, которой оно обладает); следствием этого внутренней пружиной, двигающей международные отношения, становится борьба государств за максимизацию своего влиянии во внешней среде; оптимальным ее состоянием видится международное (региональное) равновесие сил»[35]. В той мере, в какой задачи обеспечения национальной безопасности являются производными от национальных интересов, концепции национальной безопасности также связаны с теоретическим обобщением данных интересов.

Как отмечает отечественный политолог, доктор политических наук, профессор кафедры российской политики СПбГУ Иван Владимирович Радиков, «обеспечение безопасности конкретного объекта (в том числе государства) носит двойственный характер: а) обеспечение безопасности объекта в его существующей определенности; б) обеспечение безопасности в его качественной определенности». В монографии «Политика и национальная безопасность» он выделяет два типа обеспечения безопасности: первый, как

---

[34] Косолапов Н.А. Безопасность международная, национальная, глобальная: взаимодополняемость или противоречивость? // Мировая экономика и международные отношения. – 2006. – №9. – С.3-13

[35] Morgenthau Hans J. Politics Among Nations. The Struggle for Power and Peace. Second Edition, Alfred A. Knopf: New York, 1955.

форму борьбы с существующими конкретными опасностями, что является фактором, обеспечивающим поддержание существования того или иного объекта; а также второй, как стратегия и практика развития и укрепления самого объекта. Иными словами, обеспечение безопасности как отрицание опасностей и как утверждение безопасности объекта не тождественны[36].Вследствие этого могут реализовываться две стратегии обеспечения безопасности: а) стратегия защиты (отрицание отрицания, отрицание опасностей), при которой основание деятельности составляет обнаружение опасностей и их отрицание, а утверждение объекта в его безопасности является результатом отрицания опасностей; б) стратегия утверждения, укрепления безопасности, основывающаяся на самоутверждении природы самого объекта. Глубинные постсоветские преобразования российской жизни существенным образом изменили систему обеспечения безопасности страны[37].

Следует подчеркнуть, что национальная безопасность является одной из глобальных проблем человечества[38]. Национальная безопасность является многоплановым явлением. Ее следует рассматривать, исходя из масштабов обеспечения, как разновидность международной безопасности. Национальная безопасность органически связана с региональной и международной (глобальной) безопасностью. На наш взгляд, национальная безопасность представляет собой состояние защищенности совокупности жизненно важных интересов личности, общества и государства как от внутренних, так и от внешних угроз. Следовательно, она зависима от содержания национально-государственных интересов. Национальная безопасность характеризует положение страны, при котором ей не угрожает опасность войны либо других посягательств на суверенное развитие. Национальная безопасность – это

---

[36] Политика и национальная безопасность. – СПб.: Астерион, 2004.

[37] Гуторов В. А., Радиков И. В. Концепции национальной безопасности в политическом дискурсе современной России: проблемы теории и методологии анализа // Актуальные проблемы политической науки Вестник Санкт-Петербургского Университета СПб 2010 с. 130-139

[38] Кучерявый М. М. Национальной безопасности России в условиях современного глобального мира. Дисс. на соиск. докт. юрид. наук. – СПб.: 2014

состояние государства, при котором сохраняется его целостность и возможность быть самостоятельным субъектом системы международных отношений[39].

К основным компонентам национальной безопасности следует отнести военную, экономическую, социальную, экологическую и информационную безопасность. Сама по себе национальная безопасность представляет геополитический аспект безопасности вообще, охватывающий весь комплекс вопросов физического выживания государства, защиты и сохранения его суверенитета и территориальной целостности. Информационная составляющая служит важным компонентом национальной безопасности. В силу своей многогранности информационная безопасность затрагивает различные сферы общественной жизнедеятельности, в частности, является неотъемлемой частью военной безопасности, но не замыкается в ее рамках. Информационная безопасность в тоже время не ограничивается сугубо техническими и технологическими параметрами. Сфера общественной жизни, которая сведена к ним, именуется информационно-технической безопасностью[40].

При принятии попытки раскрыть содержание информационной безопасности на основе системного подхода, получится выделить следующие основные составляющие информационной безопасности[41]:

- Законодательная, нормативно-правовая и научная база.
- Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ.
- Организационно-технические и режимные меры и методы (политика информационной безопасности).
- Программно-технические способы и средства обеспечения информационной безопасности.

---

[39] Вишняков В. Т. Национальная безопасность Российской Федерации: проблемы укрепления государственно-правовых// Журнал российского права. – 2005. – № 2 с. 3-34

[40] Шушков Г.М., Сергеев И.В. Концептуальные основы информационной безопасности Российской Федерации // Актуальные вопросы научной и научно-педагогической деятельности молодых ученых: сборник научных трудов III Всероссийской заочной научно-практической конференции (23.11.2015 – 30.12.2015 г., Москва) / под общ. ред. Е.А. Певцовой; редколл.: Е.А. Куренкова и др. – М.: ИИУ МГОУ, 2016. – С. 69 – 76.

[41] Домарев В. В. Безопасность информационных технологий. Системный подход – К.: ООО ТИД Диа Софт, 2004. – 992 с.

Таким образом, информационная безопасность это по сути своей, не определённая цель и не конечное состояние сохранности данных, а скорее **процесс** обеспечения конфиденциальности, целостности и доступности информации. Под доступностью понимается обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Информационная безопасность – междисциплинарная область. Как научное направление, она имеет несколько аспектов, в частности, правовой, управленческий, экономический, психологический, культурологический, организационно-технический и иные. Однако за последнее время, когда в геополитическом пространстве мира информационные технологии и информация в целом получили определяющее значение, политический аспект изучения информационной безопасности личности, общества и государства выходит на первый план.

В современном обществе информационные технологии являются одной из важнейших движущих сил всех социальных изменений. В отечественной политологии возрастает интерес к изучению перспектив формирования информационного общества в России. Широкий круг проблемных явлений связан с информационной безопасностью личности, общества, государства. Наиболее общим определением информационной безопасности государства можно считать состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере.[42, 43]. В современном социуме информационная сфера имеет две составляющие: информационно-техническую, то есть искусственно созданный человеком мир техники, технологий, и информационно-психологическую – естественный мир живой природы, включающий и самого человека. Соответственно, в общем

[42] Шушков Г.М., Сергеев И.В. Концептуальные основы информационной безопасности Российской Федерации // Актуальные вопросы научной и научно-педагогической деятельности молодых ученых: сборник научных трудов III Всероссийской заочной научно-практической конференции (23.11.2015 – 30.12.2015 г., Москва) / под общ. ред. Е.А. Певцовой; редколл.: Е.А. Куренкова и др. – М.: ИИУ МГОУ, 2016. – С. 69 – 76.

[43] Домарев В. В. Безопасность информационных технологий. Системный подход – К.: ООО ТИД Диа Софт, 2004. – 992 с.

случае информационную безопасность общества и государства можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью[44].

При этом ни в одной из областей научного знания не наблюдается устоявшегося и общепринятого определения информационной безопасности как таковой. Более того, в научной литературе и правовых актах этот термин видоизменяется, и дополняется и несёт разную смысловую нагрузку. Так, понятие «информационная безопасность» (англ. information security) трактуется экономистами как «совокупность аспектов, связанных с определением, достижением и поддержанием конфиденциальности, целостности, доступности, подотчётности, аутентичности и достоверности информации или средств её обработки».[45] Непосредственно Федеральное агентство по техническому регулированию и метрологии, находящееся в ведении Министерства промышленности и торговли Российской Федерации определяет «безопасность информации данных» как «состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность»[46]. Достаточно часто встречается понятие «безопасность информации (данных)», которое определяется «отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе»[47].

---

[45] Борисов М. А., Романов О. А. Основы организационно-правовой защиты информации. (Гриф УМО по дополнительному профессиональному образованию). № 2. Изд.3, перераб. и доп. М.: Книжный дом «ЛЕНАНД», 2014. – 248 с.

[46] Национальный стандарт РФ «Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»

[47] Марков А. Некоторые аспекты информационной безопасности в контексте национальной безопасности // Вестник С.-Петерб. ун-та. Сер. 12. СПб., 2011. Вып. 1. С. 43-48.

С точки зрения междисциплинарных исследований на стыке политической и юридической науки «обеспечение информационной безопасности – это область государственного, политического управления, высшая форма сознательного регулирования процессами функционирования самой государственной системы»[48]. Информационная безопасность способна к развитию и саморазвитию, поэтому всякое научное знание о ней приобретает актуальное значение. Проблемный характер функционирования политической власти в России, необходимость поддержания механизма разделения государственной власти, превращение ее из поля борьбы различных политических сил в силу, консолидирующую общество, дефицит общественного согласия относительно целей и содержания реформирования самого государства и общества – все это делает научный анализ современной практики государственного обеспечения информационной безопасности в различных областях общественно-политической жизни, особенно в сферах защиты целостности и независимости самого государства, исключительно необходимым с точки зрения нового видения перспектив развития, совершенствования государства как политико-волевого стержня страны[49].

Эффективность реализации политической власти в любом государстве, в том числе и в Российской Федерации, в немалой степени зависит от его информационного обеспечения. Без информации невозможно представить позитивно функционирующую политическую структуру, развитие массового политического сознания, взаимодействие субъекта и объекта политики. В процессе информационно-коммуникативного воздействия в сознании народа формируется образ государственной власти, его политических институтов и лидеров, а управляющие функции государства осуществляются с наибольшим потенциалом и наименьшими энергетическими затратами лишь тогда, когда

[48] Бусленко Н. И. Политико-правовые основы обеспечения информационной безопасности Российской Федерации в условиях демократических реформ Диссертация на соискателя доктора юридических наук. – М.: 2004

[49] Там же.

достаточно хорошо развита система информационных связей между государством, гражданским обществом и личностью.

Информация имеет прямое отношение к политическим процессам в современном мире. Результаты развития информационных технологий позволяют надеяться на создание динамичной мировой информационной модели. Все последние годы неимоверно возрастала интенсивность потребления информации во всех сферах жизнедеятельности человека и общества – социальной, научно-технической, технологической, статистической, экономической и др. Процессы сбора, накопления, переработки и распространения информации становятся необходимым условием существующих структур политического и иного управления, осуществления эффективных политических воздействий, решения масштабных экономических задач[50].

Однако информация – это не только сила созидающая. К сожалению, она обладает дестабилизирующим общество потенциалом, если ее практически неограниченные возможности воздействия на человека и общество используются в интересах коалиционных сообществ, отдельных государств, политических группировок или отдельных лиц. Опыт новейшей истории мира вскрыл очевидность: информация может стать источником политической и социальной угроз. Этим вызвана необходимость государственно-правового и общественного регулирования информационными потоками, в частности, деятельностью средств массовой информации (СМИ). Возникла сфера политико-правовых отношений, обеспечивающих информационную безопасность личности, общества и государства[51].

---

[50] Шушков Г.М., Сергеев И.В. Концептуальные основы информационной безопасности Российской Федерации // Актуальные вопросы научной и научно-педагогической деятельности молодых ученых: сборник научных трудов III Всероссийской заочной научно-практической конференции (23.11.2015 – 30.12.2015 г., Москва) / под общ. ред. Е.А. Певцовой; редколл.: Е.А. Куренкова и др. – М.: ИИУ МГОУ, 2016. – С. 69 – 76

[51] Гончаров С.А. Национальная безопасность: проблемы и пути решения. – М.: 1999

1.2. Источники правового обеспечения информационной безопасности России

В отечественной политической науке возрастает интерес к изучению перспектив формирования информационного общества в России. Широкий круг проблемных явлений связан с информационной безопасностью личности, общества, государства.

Исследование информационного общества как научное направление сформировалось сравнительно недавно, и гуманитарные науки находятся лишь на подступах к его познанию. Отметим, что все ведущие страны мира сформулировали свою политику и стратегию построения и развития такого сложно-структурированного общества[52]. Во всех принятых программах в качестве отдельных глав ставятся вопросы политического и правового регулирования вопросов информационной безопасности[53]. Это объективно актуализирует теоретическую и практическую работу, направленную на решение научных задач, связанных непосредственным образом с формированием информационного общества в России.

Целенаправленная государственная политика в области контроля и защиты информации, её формирование и осуществление должны иметь в своём приоритете своевременное совершенствование правовых механизмов регулирования социальных отношений внутри информационной сферы. Поэтому в обязательном порядке, как законодателем, так и правоприменителем должна быть дана трезвая оценка эффективности применения существующих законов и прочих нормативных правовых актов, так или иначе регулирующих отношения в информационной сфере, и при неблагоприятном результате поставлена задача разработки программы их совершенствования. Процессу создания организационно-правовых механизмов обеспечения информационной

---

[52] Анисимова А.С. Анализ правотворческой политики зарубежных стран в сфере регулирования интернет-отношений // Вестник Саратовской государственной юридической академии. 2014. № 5. С. 38-44.

[53] Цаплин А. Ю. Политические характеристики информационного общества//Известия Саратовского университета. Новая серия. Социология. Политология. 2008

безопасности должно предшествовать определение правового статуса всех субъектов отношений в информационной сфере, а также установление их ответственности за несоблюдение закона. Критически важным для многофакторного обеспечения является создание информационно-справочной системы сбора и анализа данных об источниках её угроз. Государственная разработка нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по факсам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий также предполагается верным шагом на пути к совершенствованию правовой базы и механизмов регулирования отношений в этой сфере

Уже на данном этапе отдельные положения и законы (в том числе внутренние) ведомств, ответственных за разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности, подразумевают включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство РФ о государственной службе.

Учитывая выше сказанное, можно определить правовое обеспечение национальной безопасности как комплекс мер, осуществляемых органами государственной власти, коммерческими и некоммерческими, международными организациями, направленных на разработку законов и правовых норм, составление межгосударственных договоров, обеспечение законности и правопорядка[54]. Конкретные нормативные правовые акты и судебные прецеденты, «стиль» их использования государством в общественно-политической жизни, но главное – принципы и идеи, лежащие в их основе, составляют множественную «палитру» форм правового обеспечения информационной безопасности.

---

[54] Бусленко Н. И. Политико-правовые основы обеспечения информационной безопасности Российской Федерации в условиях демократических реформ Диссертация на соискателя доктора юридических наук. – М.: 2004

Согласно «Стратегии национальной безопасности Российской Федерации, до 2020 г.», обеспечение защищенности личности, общества и государства от целого ряда разнообразных угроз и состояние этой защищённость составляют предмет национальной безопасности. Это состояние позволяет человеку, гражданину и всему обществу, реализовывать конституционные права, свободы, достойные качество и уровень жизни. Особенно подчёркивается, важность обеспечения суверенитета, территориальной целостности и устойчивого развития страны, её обороны и безопасности, являющиеся системообразующими факторами её существования[55].

В Российской Федерации к **нормативно-правовым актам,** так или иначе, касающимся регулирования общественных отношений в области информационной безопасности относятся[56]: международные договоры РФ, Конституция РФ, акты федерального законодательства, законы федерального уровня (включая федеральные конституционные законы, кодексы), указы Президента РФ, постановления Правительства РФ, нормативные правовые акты федеральных министерств и ведомств, нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

К нормативно-методическим документам можно отнести: методические документы государственных органов России, Доктрину информационной безопасности РФ, руководящие документы ФСТЭК (Гостехкомиссии России), приказы Федеральной Службы Безопасности, а также стандарты информационной безопасности, из которых выделяют: международные стандарты, государственные (национальные) стандарты РФ, рекомендации по стандартизации, методические указания.

К числу государственных органов РФ, контролирующих деятельность в области защиты информации нужно отнести: Комитет Государственной думы по

---

[55] Официальный сайт Совета безопасности Российской Федерации // Стратегия национальной безопасности Российской Федерации до 2020 года. URL: http://www.scrf.gov.ru/docu-ments/1/99.html. (дата обращения: 08.02.2018)

[56] Лапина М. А., Ревин А. Г., Лапин В. И. Информационное право. М.: ЮНИТИ-ДАНА, Закон и право, 2004 - 335 с.

безопасности, Совет безопасности России, Федеральная служба по техническому и экспортному контролю (ФСТЭК России), Федеральная служба безопасности Российской Федерации (ФСБ России), Федеральная служба охраны Российской Федерации (ФСО России), Служба внешней разведки Российской Федерации (СВР России), Министерство обороны Российской Федерации (Минобороны России), Министерство внутренних дел Российской Федерации (МВД России), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Центральный банк Российской Федерации (Банк России), а также службы, организующие защиту информации на уровне предприятия: Служба экономической безопасности, Служба безопасности персонала (Режимный отдел), Кадровая служба, Служба информационной безопасности.

По мнению И. Л. Бачило, каждый из указанных выше органов исполнительной власти РФ находится в своей подсистеме государственного управления и в сфере ведения определенного вице-премьера (вице-премьеры имеют право решающего голоса в заседаниях правительства, участвуют в разработке его постановлений и распоряжений, контролируют их исполнение, координируют работу ведомств по вопросам определенной проблематики (например, экономики, социальной сферы и др., правительства входят также в президиум кабинета, вместе с министрами силового и экономического блока, министром иностранных дел и др., что должно подчеркнуть значимость проблемы усиления координации деятельности в сфере информатики и создания государственной структуры, которая бы могла по своему статусу обозревать весь комплекс проблем этой сферы и оказывать организующее воздействие на состояние дел[57]. Пока таким органом можно считать Совет Безопасности, но только относительно политики информационной безопасности.

К действующим в Российской Федерации законам, в той или иной степени применимыми к отношениям, связанным с Интернетом, относятся:

[57] Бачило И. Л. Информационное прав. Под редакцией Б. Н. Топорнина. – СПБ.: Юридический центр Пресс, 2011. – с. 632–663

– по наиболее общим вопросам правового режима функционирования информационных сетей и их государственного регулирования:

- Конституция Российской Федерации, Гражданский кодекс Российской Федерации;
- Федеральный закон «Об информации, информатизации и защите информации»;
- Федеральный закон «Об участии в международном информационном обмене»;
- Федеральный закон «О связи»;
- Федеральный закон «О средствах массовой информации»;

– по вопросам охраны исключительных прав в отношении информационных объектов, циркулирующих в Интернете:

- Федеральный закон «Об авторском праве и смежных правах»;
- Федеральный закон «О правовой охране программ для ЭВМ и баз данных»;
- Федеральный закон «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров»;
- Уголовный кодекс Российской Федерации;
- Патентный закон Российской Федерации;

– по иным вопросам, имеющим отношение к правовому режиму информации в Интернете и определению условий доступа к ней:

- Федеральный закон «О государственной тайне»;
- Федеральный закон «О федеральных органах правительственной связи и информации»;
- Федеральный закон «О рекламе»;
- Федеральный закон «Об оперативно-розыскной деятельности в Российской Федерации»;
- другие законодательные акты.

Особое место среди различных правовых источников занимает – Доктрина информационной безопасности Российской Федерации, в последней редакции

была утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646. Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. К составляющим национальных интересов Российской Федерации в информационной сфере в доктрине относится беспрекословное соблюдение конституционных прав и свобод человека в области получения пользования непротиворечащей закону информации. Информационное обеспечение государственной политики РФ, согласно документу, выражается через информирование международной общественности и граждан Российской Федерации о её государственной политике и выраженной документарным способом официальной позиции по значимым для страны и мира событиям. Эта составляющая национальных интересов реализуется на практике обеспечением открытого доступа к открытым государственным ресурсам. Другим важнейшим компонентом, указанным в Доктрине, стоит назвать развитие современных средств информатизации, телекоммуникации и связи отечественной индустрии, а также обеспечение ИТ внутреннего рынка России и выход на мировые рынки, защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем[58].

В общем и целом, доктрина, согласное её тексту, своей основной задачей устанавливает формирование государственной политики в области обеспечения информационной безопасности России. Однако в ней особое место уделяется потребности государства (причём как в широком, так и узком смыслах) в создании соответствующей инфраструктуры в целях формирования общества знаний, в котором преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение достоверной информации с учетом стратегических национальных приоритетов Российской Федерации.

[58] Доктрина информационной безопасности Российской Федерации. URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 15.01.2018)

Министерство связи и массовых коммуникаций Российской Федерации (далее по тексту – Минкомсвязь) является основным федеральным органом исполнительной власти, проводящим государственную политику и осуществляющим руководство службой государственного надзора за деятельностью в области связи и информатизации, управление находящимися в его ведении государственными предприятиями и учреждениями в области связи (электрической и почтовой) и информатизации, а также координацию в этой сфере деятельности иных федеральных органов исполнительной власти[59]. Основными задачами Минкомсвязи России являются: разработка и реализация государственной политики в области электросвязи, почтовой связи и информатизации; регулирование деятельности в области использования радиочастотного спектра и орбитальных позиций спутников связи гражданского назначения, за исключением вопросов, касающихся присвоения и эксплуатации полос радиочастот и орбитальных позиций спутников связи гражданского назначения для целей телерадиовещания, развития средств массовых коммуникаций и распространения средств массовой информации.

В структуру Минкомсвязи входит важнейшее подразделение в сфере надзора в сфере информационной безопасности, почти одноимённая, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). В задачи службы входят надзор за соблюдением Российского законодательства в сфере связи, информационных технологий и СМИ, а также надзор по защите персональных данных согласно закону о персональных данных в России и деятельность по организации радиочастотной службы[60].

В сложившихся условиях национальными интересами страны становятся развитие человеческого потенциала, обеспечение безопасности граждан и государства, повышение роли России в мировом гуманитарном и культурном

---

[59] Указ Президента РФ от 15.05.2018 «О структуре федеральных органов исполнительной власти».

[60] Указ Президента Российской Федерации от 12 мая 2008 г. № 724 г. Москва “Вопросы системы и структуры федеральных органов исполнительной власти”. URL: https://rg.ru/2008/05/13/struktura-vlasti-dok.html (дата обращения: 17.02.2018)

пространстве, развитие свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления, повышение эффективности государственного управления, развитие экономики и социальной сферы, формирование цифровой экономики.

1.3. Содержание термина интернет-право и его источники

Информация в любых её формах, как материальный и нематериальный предмет общественных отношений выступает элементом во всех правовых отношениях. Предпосылки формирования самостоятельной области права, объективные условия, связанные с превращением информации в формы, которые делают ее самостоятельным предметом производственных, интеллектуальных управленческих, экономических и идеологических отношений, и некоторые другие процессы выступают в качестве продукта деятельности человека и ресурса других социальных отношений, в качестве товара в обмене, объекта работ и услуг. Всё это позволяет выделить большой массив социальных отношений в самостоятельную предметную область правового регулирования. Призванная регулировать эти сложные общественные отношения, в системе права могла бы быть сформирована отдельная его отрасль – информационное право[61].

Многообразие форм выражения информации (устная, письменная, волновая, биологическая, визуально воспринимаемая и многие другие) бесконечно, поэтому раскрывая предмет информационного права, нужно понять и определить информационные ресурсы – т.е. запасы информации, зафиксированные тем или иным образом для её хранения и использования. Категория «информационные ресурсы» отличается от более широкого и менее

[61] Архипов, В. В. Интернет-право: учебник и практикум для бакалавриата и магистратуры / В. В. Архипов. — М.: Издательство Юрайт, 2016. — 249 с.

однозначного понятия «информация». Наиболее социализированной формой информации является знаковая и прежде всего письменная форма представления информации[62]. Поэтому первый принятый в Российской Федерации закон, посвященный исключительно информационным проблемам – Федеральный закон «Об информации, информатизации и защите информации», от 1995 г., предметом своего регулирования имеет документированную информацию, на основе которой формируются информационные ресурсы разных субъектов. Зарубежное законодательство, как правило, говорит о документе в качестве объекта регулируемых отношений в информационной сфере. Законом информационный ресурс определяется как синтетическая организационная форма представления информации, основанная на концентрации, индивидуализации, как правило, документированной информации, наиболее ярко выявляющей ей функциональное назначение.

В этих условиях информационное право формируется не только по признаку узкого предмета регулирования, но призвано также отразить процессы, затрагивающие такие проблемы как свобода, справедливость, права человека и гражданина, свою роль и информационную активность в формировании жизни общества; уже сложившихся веками институтов и систем государственного управления[63].

Всё перечисленное – совокупность существенных и показательных признаков качественного перехода социума в состояние «Информационного общества», а сегодня общества цифрового, которое и определяет комплексность и универсальность информационного права. При этом, темы развития информационного права касается и проблема глобализации. Практически она выражена в функционировании и развитии самой крупной информационной сети – Интернета.

---

[62] Рассолов И.М. Право и Интернет. Теоретические проблемы – М.: Норма, 2009. – 383 с

[63] Алфёров А. Н. Информационное право в системе отраслей права // Вопросы теории и истории государства и права. Сибирский юридический вестник №4 – Иркутск: 2007

Интернет представляет собой автономную часть мировой коммуникационной технологии. На сегодняшний день, этот сегмент глобальной информационной сети, претерпевает бурное развитие и, возможно, трансформацию в качественно новую информационную индустрию[64]. Выход Интернета в том числе и космическое пространство стало первым шагом нау пути к осуществлению подобной модификации. Немногочисленные специалисты в области интернет-права, уверенно заявляют, что мы переживаем переходный период, то, что можно назвать технологической «разминкой»[65]. Например, А. В. Даниленков и В. В. Архипов отмечают, что сегодня можно пересчитать по пальцам монографические и диссертационные работы, посвященные проблемам права и Интернета, правовому регулированию отношений в виртуальном пространстве[66]. «В большинстве опубликованных работ по информационному праву основное внимание уделяется прикладным аспектам Интернета и права, акцентируется внимание на естественнонаучной характеристике самого Интернета (как глобальной информационной системы) и на исследовании частных проблем интернет-права (вопросов электронной торговли, оказания интернет-услуг, использования электронной цифровой подписи в киберпространстве)» – заключает Даниленков в своей работе «Интернет-право»[67]. В то же время, за исключением небольшого количества работ узкого ряда специалистов, в юридической, а особенно политологической литературе проблемы системного исследования интернет-права и интернета в целом практически не рассматриваются, в особенности, как комплексный политико-правовой институт.

Интернет-право (далее по тексту – «ИП») как комплексная отрасль права представляет собой совокупность общепризнанных принципов и норм, сосредоточенных в различных источниках (международные и

---

[64] Рассолов И.М. Право и Интернет. Теоретические проблемы – М.: Норма, 2009. – 383 с

[65] Чумиков Л. Н. Бочаров М. П. Связи с общественностью: теория и практика. М., 2010. С. 393.

[66] Архипов, В. В. Интернет-право: учебник и практикум для бакалавриата и магистратуры / В. В. Архипов. – М.: Издательство Юрайт, 2016. — 249 с.

[67] Даниленков А. В. Интернет-право – М.: Юстицинформ, 2014 – С. 13 – 27.

внутригосударственные нормативно-правовые акты, судебные и административные прецеденты, локально-правовые акты некоммерческих организаций; академическая доктрина; обычаи делового оборота и т. д.) и регулирующих общественные отношения, возникающие в связи и по поводу[68]:

- осуществления заинтересованными лицами своих субъективных правомочий по владению, пользованию и распоряжению доменными именами, а также иными объектами прав и ресурсами, локализованными в сети;
- реализации органами публичной власти, саморегулируемыми организациями (в порядке делегирования им публично-властных полномочий) и уполномоченными (аккредитованными и т. д.) ими лицами функций по распределению адресно-номерного пространства сети Интернет;
- по разрешению споров между субъектами интернет-отношений; по обеспечению безопасности и охраны информации в сети Интернет;
- по цензурированию распространения определенных видов информации и т. д. (частно-публичная сфера ИП), а также – применения мер принудительного воздействия и юридической ответственности к недобросовестным участникам рынка доменных имен; пользователям сети Интернет и др. за действия (бездействия), нарушающие требования норм применимого права (публичная сфера ИП).

Специфика ИП состоит в том, что указанные выше сферы действия его норм в силу экстерриториальности отдельных сегментов сетевого пространства Интернета и разной правосубъектности участников сетевых отношений в виду подчинения их личного статуса или корпоративной правоспособности различным юрисдикциям иногда сплетаются в настоящий клубок коллизионных противоречий и проблем.

Помимо всего этого отрасль имеет очень специфический характер, соединяя в себе нормы сразу нескольких отраслей права. Так, по мнению американского юриста Роберта Дж. Амброги, ИП – это динамичная, гибкая и

---

[68] Ловцов Д.А. Информационные правоотношения: особенности и продуктивная классификация // Информационное право. 2009. № 1.

неизведанная сфера юридической практики, границы которой ещё предстоит определить[69]. В настоящее время это даже трудно назвать отраслью права – это скорее смесь теории и практики из интеллектуальной собственности, гражданских прав и свобод, деликатного, имущественного, уголовного, телекоммуникационного, коммерческого, международного торгового и частного права[70].

Отдельно, стоит выделить определение «киберпространства», неразрывно связанного с технической стороной правового регулирования Сети. Киберпространство – это сложный технический объект (набор технических и программных средств; совокупность информационных ресурсов и информационной инфраструктуры), обеспечивающий движение потоков информации. Ёмкое определение даётся В.В. Архипов в работе «Интернет-право». В его изложении, под киберпространством стоит понимать особоую социальную сферу деятельности, связанную с оборотом информации в глобальной информационной сети Инетрнет, а также в других информационно-коммуникационных сетях (региональных, опорных, ведомственных, корпоративных)[71].

На наш взгляд, интернет-законодательство – это совокупность законов, иных нормативных актов (национальных, например, России и зарубежных государств), регулирующих отношения в виртуальном пространстве Интернета. В качестве интернет- отношений выступают только те отношения, которые связаны с социально-правовым регулированием виртуального пространства (т.е. с регулированием этого пространства на основе норм права, морали, этики и других средств). Субъекты интернет-отношений – это провайдеры, владельцы серверов и другие лица, которые используют Интернет. Кибербезопасность определяется Г. Васильевым и Д. Забегалиным как состояние защищенности

[69] Ambrogi, Robert J.Chapter 12: Net Law: The Internet's Rules of the Road //The essential guide to the best (and worst) legal sites on the Web – 2nd edition. – N.Y.: ALM Publishing, 2004.
[70] Тедеев А.А. Предмет информационного права в условиях интернета//Республиканский НИИ интеллектуальной собственности «Информационное право»: Журнал. – М., 2006.
[71] Архипов, В. В. Интернет-право: учебник и практикум для бакалавриата и магистратуры / В. В. Архипов. — М. : Издательство Юрайт, 2016. — 249 с.

сбалансированных интересов личности, общества и государства от внутренних и внешних угроз в киберпространстве (части информационной сферы) на основе общепризнанных принципов и норм международного и национального права. При этом под защищенностью следует понимать активные действия субъектов интернет-права, направленные на достижение определенной степени безопасности объекта охраны в целях сохранения конфиденциальности, целостности и недоступности информации для третьих лиц во всемирном виртуальном пространстве[72].

Исходя из положений, изложенных выше, можно заключить, что в настоящее время интернет-право – это новое самостоятельное направление юридической науки, и прежде всего информационного права. Очевидно, что при определении содержания интернет-права важно определить и совокупность норм, регулирующих отношения в виртуальном пространстве Интернета, и основные источники интернет-права, которые характеризуют его особенности. При этом данные нормы охватывают либо могут охватывать своим воздействием разнообразные «среды» интернет-отношений, в соответствии с которыми может строиться вся система норм и положений, регулирующих сферу виртуального пространства, и те разделы законодательства, с которыми оно связано.

Система правовых актов как источников позитивного информационного права не отличается ничем от источников других отраслей. Она включает систему таких нормативных актов, как законы – Конституция Российской Федерации, федеральные конституционные законы, федеральные законы, в том числе кодексы, конституции и законы субъектов РФ; указы Президента РФ постановления Правительства РФ; нормативные правовые акты глав субъектов Федераций и акты правительств или администраций субъектов РФ; нормативные акты судебной власти; постановления Конституционного Суда Российской Федерации. К источникам информационного права относятся как

[72] Васильев Г.В., Забегалин Д.А. Правовое регулирование электронного бизнеса в России и за рубежом // Электронный бизнес и реклама в Интернете. М., 2008. с. 106 – 114.

международные, так и внутренние договоры Российской Федерации, а также ратифицированные международные акты. Примером могут быть Конвенция о создании Международного союза публикаций таможенных тарифов (5 июля 1890 г. с протоколом 1949 г.)[73, 74]; большое количество соглашений о системах космической связи; Европейская конвенция по вопросам авторских и смежных прав применительно к трансграничному спутниковому телевещанию (11 мая 1994 г., Страсбург)[75]; Конвенция об обмене официальными изданиями и правительственными документами между государствами (5 декабря 1958 г., Париж)[76]. Огромное количество подзаконных актов касается вопросов информации, связи, информатизации. Перечисленные виды нормативных правовых источников информационного права содержат, как правило, отдельные нормы или разделы, посвященные информационной проблематике. И только начиная с уровня федерального закона возможно говорить о законе в полном смысле, относящемся к данной отрасли права и целиком посвященном регулированию отношений в данной предметной сфере. Тем не менее, ряд норм, регулирующих отношения в виртуальном пространстве Интернета, может формулироваться в виде отдельных концепций, доктрин, деклараций. К их числу, можно отнести разработку актуальных проблем «киберэкономики» (электронные деньги, реклама, маркетинг, электронные публикации, электронные договоры, контракты, налог на передачу информации – см., например, ст. 160, 434, 847 ГК РФ); решение проблем правового регулирования электронного документооборота, а также разработку проблем информационной безопасности, повышения юридической ответственности участников

[73] Конвенция о создании международного союза публикаций таможенных тарифов (Брюссель, 5 июля 1890 г.) URL: http://base.garant.ru/2540219/ (дата обращения: 21.04.2018)

[74] Распоряжение Правительства РФ от 17 марта 2016 г. № 442-р “О прекращении действия Конвенции о создании Международного союза публикации таможенных тарифов”. URL: http://base.garant.ru/71354740/ (дата обращения: 21.04.2018)

[75] Европейская конвенция о трансграничном телевидении (ETS № 132) URL: http://docs.cntd.ru/document/901739192 (дата обращения: 21.04.2018)

[76] Конвенция об обмене официальными изданиями и правительственными документами между государствами URL: http://base.garant.ru/2540309/ (дата обращения: 19.04.2018)

правоотношений в Интернете (в частности, Доктрина информационной безопасности Российской Федерации)[77].

Однако отношения в сфере виртуального пространства Интернета регулируются в первую очередь нормами международного права. Эти отношения сегодня регулируются Хартией глобального информационного общества, принятой в июле 2000 г. в Окинаве[78], Конвенцией ООН об использовании электронных сообщений в международных договорах, принятой в Нью-Йорке 23 ноября 2005 г.[79], Декларацией о свободе обмена информацией в Интернете, принятой Советом Европы 28 мая 2003 г.[80], Европейской декларацией о правах человека и верховенстве права в информационном обществе 2005 г.[81], Будапештской конвенцией о киберпреступности 2001 г.[82], Европейской конвенцией о трансграничном телевидении от 5 мая 1989 г.[83], с изменениями, внесенными Протоколом от 1 октября 1998 г., Европейской конвенцией о защите детей от сексуальной эксплуатации и сексуального насилия 2007 г., Соглашением между Правительством РФ и Европейским сообществом о сотрудничестве в области науки и технологий от 16 ноября 2000 г.[84], Соглашением между странами СНГ о сотрудничестве в области информации от 9 октября 1992 г.[85], Соглашением между странами СНГ о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001

---

[77] Рассолов И.М. Право и Интернет. Теоретические проблемы – М.: Норма, 2009. – 383 с.

[78] Окинавская Хартия глобального информационного общества. UNESCO's Global Search Engine EN. URL: http://www.unesco.org/new/fileadmin/MULTIMEDIA/FIELD/Tashkent/pdf/okinawa_charter_ru.doc (дата обращения 16.11.2017)

[79] Россия приняла решение подписать Конвенцию. См.: распоряжение Правительства РФ от 27 декабря 2006 г. № 1821-р // СЗ РФ. 2007. № 1. Ч. II. Ст. 346. URL: http://www.consultant.ru/document/cons_doc_LAW_213218/ (дата обращения 12.12.2017)

[80] Декларация о свободе обмена информацией в Интернете. URL: http://base.garant.ru/71036560/ (дата обращения 12.12.2017)

[81] Европейская декларация о правах человека и верховенстве права в информационном обществе URL: http://www.ifap.ru/ofdocs/eu/dhrrlis.pdf (дата обращения 12.12.2017)

[82] Конвенция о преступности в сфере компьютерной информации (ETS № 185). (Будапешт, 23 ноября 2001 г.) URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526#09741658132188091 (дата обращения 12.12.2017)

[83] Распоряжение Правительства РФ от 26 июля 2006 г. № 1060-р // СЗ РФ. 2006. № 31. Ч. II. Ст. 3529. URL: http://docs.cntd.ru/document/901989933 (дата обращения 04.02.2018)

[84] Бюллетень международных договоров. 2001. № 11. URL: http://pravo.gov.ru/proxy/ips/?divisions&edition=203000001 (дата обращения 04.02.2018)

[85] Бюллетень международных договоров. 1993. № 10. URL: http://pravo.gov.ru/proxy/ips/?divisions&edition=203000001 (дата обращения 04.02.2018)

г.[86], Декларацией принципов построения информационного общества 2003 г. и Планом действий Тунисского обязательства 2005 г., принятыми Всемирным саммитом по информационному обществу, международными договорами между провайдерами России, США, Франции, Германии и других государств в сфере заключения и исполнения сделок, контрактов, оказания интернет-услуг и др.

Одним из важнейших международных договоров, как уже отмечалось, является Хартия глобального информационного общества, принятая в Окинаве 22 июля 2000 г., в которой сказано, что все люди повсеместно, без исключения, должны иметь возможность пользоваться преимуществами глобального информационного общества. Устойчивость глобального информационного общества зависит от поддержания человечеством в планетарных масштабах базовых демократических ценностей, в особенности, свободного обмен информацией и знаниями. Их стимулирующее влияние на развитие человека, было положено в основу других международных документов, принятых в последствии. Базируясь на общепризнанных принципах международного права, договаривающиеся стороны обязались осуществлять руководство в продвижении усилий правительств по укреплению соответствующей политики и нормативной правовой базы, стимулирующих конкуренцию и новаторство, обеспечение экономической и финансовой стабильности, содействующих сотрудничеству по оптимизации глобальных сетей, борьбе со злоупотреблениями, которые подрывают целостность Сети, сокращению разрыва в цифровых технологиях, инвестированию в людей и обеспечению глобального доступа и участия в этом процессе.

Хартия является прежде всего призывом ко всем (как в государственном, так и в частном секторе) ликвидировать международный разрыв в области информации и знаний. Солидная основа политики и действий в сфере информационных технологий должна изменить методы нашего взаимодействия по продвижению социального и экономического прогресса во всем мире.

[86] Информационный вестник Совета глав государств и Совета глав Правительств СНГ “Содружество”. № 1(37). С. 138 - 145.

Эффективное партнерство участников, включая совместное политическое и правовое сотрудничество, призвано стать ключевым элементом рационального развития информационного общества.

На данном этапе развития интернет-права, обычаи, в основе которого лежат принципы суверенитета и равенства государств, не являются обязательными для всех стран. Что же касается других обычаев, то они обязательны для того или иного государства в случае, если они им в какой-либо форме признаны. Например, правовой обычай делиться информацией между государствами о готовящихся киберпреступлениях, вытекающий из Конвенции по борьбе с киберпреступностью 2001 г., подписанной в Будапеште[87]. Россия на настоящий момент не подписала Конвенцию[88].

Кроме международно-правовых обычаев, в интернет-отношениях имеют место обычаи информационного обмена, контактов и др., которые в настоящее время широко применяются странами в виртуальном пространстве. Процессы формирования права, наблюдающиеся в интернет-сфере, можно сравнить с тем, что происходило на протяжении веков с морским правом и правом вооруженных конфликтов. Например, долгое время морское право регулировалось исключительно обычаями.

1.4. Теоретические методы и особенности правового регулирования сети Интернет

Вопрос о правовой природе отношений, возникающих, изменяющихся и прекращающихся в области использования сети Интернет, является самым дискуссионным и сложным. В целом общественные отношения представляют

---

[87] Конвенция Совета Европы о преступности в сфере компьютерной информации ETS №185 URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (дата обращения 01.04.2018)

[88] Распоряжение Президента РФ от 22.03.2008 №144-рп "О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. №557-рп "О подписании Конвенции о киберпреступности" URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=417185#08673649535062591 (дата обращения 01.04.2018)

собой форму организации человеческой деятельности – практику. Ещё в семидесятые года XX века информационные отношения (названные «диагональными») были определены А.Б. Венгеровым как «социальные отношения, имеющие технически-организационную сторону и социальное содержание, которые выделяются на определенном этапе развития общества (для целей автоматизации управления); это отношения, которые складываются в сфере управления народным хозяйством между работниками, их коллективами в процессе регистрации, сбора, передачи, хранения и обработки информации. Они носят объективный характер, т.е. облекаются в объективную материальную форму»[89].

Д.В. Грибанов, который считает, что общественные отношения, возникающие с использованием глобальных компьютерных сетей, выступают особыми информационными отношениями, направленными на организацию движения информации в обществе и обусловленными информационной природой самого общества. Эти особые отношения автор называет информационно-кибернетическими. Он доказывает, что участвовать в информационно-кибернетических отношениях можно только посредством ЭВМ, подключенной к компьютерной сети[90].

В современных условиях все же логичнее говорить об интернет-отношениях, используя, естественно, научные наработки по трактовке понятий «правоотношения в Интернете» и «информационные отношения в Интернете»[91]. Основываясь на обозначенных научных определениях, в настоящее время интернет- отношения можно определить таким образом: это часть отношений в виртуальном пространстве (включая моральные, этические и иные отношения),

---

[89] Венгеров А.Б. Право и информация в условиях автоматизации управления. Теоретические проблемы: Автореф. Дисс. на соиск. докт. юрид. наук. М., 1975

[90] Грибанов Д.В. Правовое регулирование кибернетического пространства как совокупности информационных отношений: Дисс. на соиск. докт. юрид. наук. Екатеринбург, 2003. с. 7 - 16

[91] Копылов В.А. Информационное право. С. 130 - 140; Булатецкий Ю.Е.
Правовое обеспечение электронной торговли // Коммерческое (торговое) право / Под ред.
Ю.Е. Булатецкого. М., 2002. С. 880 - 886.

участники которых выступают как носители субъективных прав и обязанностей в Интернете.

Стремительное развитие Интернета стимулировало возникновение или обострение ряда проблем, требующих нормативного регулирования. Вот лишь некоторые из них: возникновение новых способов давления на власть, проблема приватности, появление интернет-СМИ как нового ресурса массовой информации и др. Государственное управление в информационной сфере – специфический вид социального управления посредством реализации своих властных полномочий всеми органами государственной власти (в широком смысле), либо органами исполнительной власти (в узком смысле) по регулированию отношений, возникающих по поводу информации и в связи с ее оборотом в социальных системах.

Исходя из указанных выше особенностей правового регулирования можно выделить три достаточно полярные **позиции** по проблеме регулирования сети Интернет. Первая, представленная меньшинством, состоит в отказе от любого «внешнего» вмешательства в интернет-пространство, которое было бы способно самостоятельно все регулировать, например Дж. П. Барлоу[92] или Митчелл Капор[93]. Эта позиция опирается на двойное суждение о том, что киберпространство – это новая территория, качественно отличающаяся от физического пространства; нормативные регуляторы и судьи «реального мира» обречены быть неэффективными в этом «текучем» и неуловимом мире, существующем без формализма документов и без физических границ. Ряд исследователей рассматривает эту позицию как устаревшую. Доктор юридических наук, специалист в области информационного права, права и управления Илья Михайлович Рассолов утверждает, что пользователи Интернета –это вполне реальные физические и юридические лица, имеющие своё месторасположение и местопребывание не только в реальной жизни, но и в

[92] A Declaration of the Independence of Cyberspace. URL: https://www.eff.org/cyberspace-independence (дата обращения 16.12.2018)
[93] Rosenberg, Scott. Dreaming in Code: Two Dozen Programmers, Three Years, 4,732 Bugs, and One Quest for Transcendent Software (2007)

сети Интернет, обладающие при этом определённым правовым статусом. Это означает, что на практике экономически активные объекты, скажем, предприятия, обязательно носят такие атрибуты, как собственная инфраструктура, юридический адрес, банковские счета, и многие другие. Именно поэтому любые виды товарных, денежных, любых имущественных и неимущественных обменов, могут становится объектами множества как зафиксированных в законодательстве, так и непредусмотренные таковым, правонарушений в этой среде. Несмотря на «виртуальный» характер данного вида общественных взаимоотношений, последствия подобных правонарушений могут стать более чем ощутимыми для вполне реальных физических или юридических лиц и публично-правовых образований. Наработанный годами опыт международного сотрудничества в этой среде даёт основания полагать, что государство способно законно регулировать интернет-отношения с помощью норм права и обнаруживать правонарушителей, при наличии у него комплексной и детально проработанной системы регулирования сети Интернет, качество и результативность которых, в свою очередь, зависят от юридического статуса «интернет-права» в данной стране[94]. Вторая позиция сводится к тому, что любое государство, в лице его аппарата и институтов власти не может осуществлять правовое регулирование Интернета, в виду своей неповоротливости в вопросах решения животрепещущих и глубинных общественно-политических проблем, а также в виду естественной тенденции к бюрократизации, но не систематизации, лежащих в самой его (государства) сути. Государство, согласно доводам данного течения мысли, не может обеспечить необходимый для его бесперебойного, как технического так коммерческого, развития Интернета, поэтому должно остаться в существующих правовых рамках в вопросах регулирования глобальных информационных сетей. Сторонники этой точки зрения указывают на особое место всех участников экономических отношений в среде глобальных сетей, связанных с друг другом, заинтересованных в том, чтобы их рентабельность

[94] Рассолов И.М. Право и Интернет. Теоретические проблемы – М.: Норма, 2009. – 383 с.

базировалась на доверии потребителей, в сложной структуре экономического роста, во многом обеспеченного бесперебойным и высокоскоростным характером передачи информации между ними. Исходя из этого предположения, именно экономически активные субъекты отношений в информационной сфере предлагать, разрабатывать, даже обязывать вводить в сферу Интернета общеобязательные морально-этические кодексы и внедрять идеи саморегулирования, которые государство значительно позже (из-за инертности государственной машины) сможет затем путём закона и юриспруденции окончательно закрепить[95].

Следовательно, необходимы иные способы регулирования. Существуют и другие способы регулирования: государственные, корпоративные, индивидуальные. Но они иногда находятся в противоречии с формами рыночного саморегулирования. И, с другой стороны, общественная польза от них не будет только точкой соприкосновения между интересами экономических агентов и интересами платежеспособных потребителей. Следовательно, саморегулирование в Интернете будет играть существенную роль, но не будет занимать все мировое пространство регулирования. Иными словами, оно будет иметь свое место в системе правовых воззрений на интернет-отношения. Третья позиция (государство – «ночной сторож») сводится к следующему: существующие демократические учреждения и законодательные процессы вполне обнаруживают свою состоятельность в регулировании информационной среды. Согласно этой позиции, органы правосудия могут рассматривать индивидуальные споры в виртуальном пространстве и постепенно создавать судебную практику, а законодатель должен менять и толковать нормы интернет-права, там же где это необходимо, исключать их.

В настоящее время существуют две **системы регулирования** Интернета в целом и интернет-СМИ[96]. Одна из них (восточная) основана на жестком

---

[95] Пушкин Д. С. Интернет и противоправные деяния (теоретический аспект): автореф. дис.... канд. юрид. наук. М., 2003. С. 10.

[96] Балашов А. Н. Правовое регулирование интернет-отношений: основные проблемы и практика реализации в России//Среднерусский вестник общественных наук. Том 11. Серия №2. – 2016

установлении определенных рамок со стороны государства. Так, в Китае существует тотальная цензура, с помощью которой правительство жестко и тайно контролирует распространение в Интернете информации о деятельности оппозиционных политических группировок, критике китайского правительства и вождей китайской коммунистической партии и многих других, вплоть до сообщений BBC и CNN. Под жестким прессингом оказываются провайдеры интернет-услуг – они несут криминальную ответственность за то, чтобы на сайтах, размещаемых на их серверах, не содержалась запрещенная информация[97]. Кроме того, от владельцев интернет-кафе требуется отслеживать, какую информацию запрашивает каждый посетитель, хранить эти сведения в течение двух месяцев и по первому требованию предоставлять компетентным органам. В случае появления нежелательной информации в Интернете доступ к ней перекрывается при помощи аппаратных и программных фильтров. Причем, по китайскому законодательству, ответственность за распространение запрещенной информации несет ее автор, и разместивший на своем сервере, и лицо, воспользовавшееся ею. В результате самым эффективным средством фильтрации виртуальной информации стала самоцензура.

Другая система («европо-американская») подразумевает свободу и способность к саморегуляции. Интернет расценивается как источник знаний, к которому открыт доступ всем гражданам. Последние документы в данной области – это Совместная декларация представителя ОБСЕ по вопросам свободы СМИ «О гарантировании свободы СМИ в Интернете» от 18 июня 2005 года и план действий, выработанный на основе Декларации тысячелетия и Всемирной Встречи на высшем Уровне по вопросам Информационного Общества (ВВУИО) в Тунисе в 2005 году. Все регулирование Интернета должно исходить из главного принципа: «Любой закон о передаче электронной информации должен основываться на праве человека на свободу выражения» (ст. 19 Всеобщей

[97] GreatFire.org – Bringing Transparency To The Great Firewall Of China". URL: https://web.archive.org/web/20180518120336/https://en.greatfire.org/ (дата обращения: 14.04.2018)

Декларации Прав Человека)[98]. В соответствии с этим принципом, любые требования регистрации веб-сайтов неприемлемы, а выдача официальных лицензий в Интернете не оправдывается: все это может затруднять свободный обмен мнениями, идеями и информацией. Сами граждане, а не государство выступают в качестве фильтра электронного содержания информации (принцип свободного потока информации, единственное требование к которой – соответствие действующему законодательству страны происхождения Интернет контента («правило исходящего трафика»)). В таком случае статус судьи (а также электронного журналиста) высок – только он имеет право принимать решение о законности или незаконности сайта, а провайдер отвечает лишь за техническую сторону передачи и публикации сведений[99].

Все это нацелено на развитие полноценного информационного общества, строящегося в условиях сотрудничества и солидарности органами государственного управления, частного сектора и гражданского общества. Для достижения максимальных преимуществ информационного общества в социальной, экономической и экологической сферах органам государственного управления необходимо создавать надежную, прозрачную, недискриминационную правовую среду. Для этого органам государственного управления необходимо создавать условия, которые становились бы стимулами для инвестиций и развития общин в информационном обществе. Возможен переход от государственного к надгосударственному регулированию отношений в Интернете посредством создания специальной комиссии при ООН или Совете Европы[100].

---

[98] Всеобщая декларация прав человека" (принята Генеральной Ассамблеей ООН 10.12.1948). URL: http://www.consultant.ru/document/cons_doc_LAW_120805/ (дата обращения 08.04.2018)

[100] Аналитическая записка «Регулирование и развитие СМИ в интернете: европейский и российский опыт». ИКТ: ШАНС, УГРОЗА, ВЫЗОВ Российско-европейский центр междисциплинарных исследований Высшей Школы Экономики. URL: https://balticpractice.hse.ru/data/352/267/1240/Регулирование%20и%20развитие%20СМИ%20в%20Интернете_европейский%20и%20российский%20опыт.pdf (дата обращения 09.12.2017)

Таким образом, можно сделать вывод о том, что национальная безопасность – многогранное явление, представляющее собой в самом общем виде состояние защищенности от внутренних и внешних угроз жизненно важных интересов личности, общества и государства. Все существующие стратегии защиты национальной безопасности, основаны на обнаружении опасностей и их отрицании, или на утверждении, укреплении безопасности. Представляется разумным представить её двумя составными частями: информационно-технической безопасностью и психофизической безопасностью.

Интернет представляет собой часть мировой коммуникационной технологии, которая активно развивается и эволюционирует в совершенно комплексную информационную индустрию. Вопрос государственного регулирования Интернета сводится к трём общим позициям: первая – отказ от любого «внешнего» вмешательства в саморегулирующееся интернет-пространство, вторая – контроль государства за экономической жизнью общества в глобальных информационных сетях, третья – государство может выступать в этом вопросе, только как «ночной сторож». На основе данных позиций в мировой практике оперируют две крупнейшие **системы регулирования** Интернета: основанная на жестком установлении определенных рамок со стороны государства (в основном страны Ближнего Востока, Азии, Океании и Латинской Америки) и основанная на свободе и способности к саморегуляции (Северная и Центральная Европа, Северная Америка, Австралия).

Интернет-законодательство может быть представлено как совокупность законов, иных нормативных актов, регулирующих отношения в виртуальном пространстве Интернета. Учитывая ряд особенностей этой сферы общественных отношений, можно выделить достаточно полярные позиции по проблеме регулирования сети Интернет: от тотального контроля, до недопустимости влияния государство на «саморегулирующуюся» глобальную сеть.

Глава 2. РЕГУЛИРОВАНИЕ СЕТИ ИНТЕРНЕТ В РФ

2.1. Проблемы информационной безопасности в России в политической сфере

Несмотря на высокие темпы глобального развития ИКТ в последнее десятилетие, Россия не смогла сократить отставание от промышленно развитых стран в уровне информатизации экономики и общества. Отчасти такое положение вызвано общеэкономическими причинами (длительный кризис в экономике, низкий уровень материального благосостояния большинства населения). Вместе с тем недостаточное развитие информационных и коммуникационных технологий в России усугубляется целым рядом факторов, создающих препятствия для широкого внедрения и эффективного использования этих технологий в экономике. К числу таких негативных факторов относятся:

- несовершенная нормативная правовая база, разрабатывавшаяся без учета возможностей современных информационных и коммуникационных технологий;
- недостаточное развитие информационных и коммуникационных технологий в области государственного управления, неготовность органов государственной власти к применению эффективных технологий управления и организации взаимодействия с гражданами и хозяйствующими субъектами;
- отсутствие целостной информационной инфраструктуры и эффективной информационной поддержки рынков товаров и услуг, в том числе в сфере электронной торговли;
- недостаточный уровень подготовки кадров в области создания и использования информационных и коммуникационных технологий;
- барьеры, возникающие из-за недостатков в регулировании экономической деятельности при выходе российских предприятий и других организаций сферы информационных и коммуникационных технологий на российский и мировой рынки;

- высокий уровень монополизации сетей связи, создающий барьеры на пути их использования и приводящий к перекосам в тарифной политике.

Процессы информатизации уже активно идут на всех уровнях, многие мероприятия, направленные на развитие информационных и коммуникационных технологий, реализуются или планируются в рамках федеральных, региональных и ведомственных программ.

В условиях возрастающей роли информационной сферы значительно увеличивается количество угроз информационной безопасности РФ. Отечественные концепции, при определении указанного рода угроз ориентируются на их обособление, разделяя угрозы информационного характера и «традиционные» угрозы национальной безопасности РФ.

Представляет интерес безопасность социума как философско-методологическая проблема. Особую опасность для социума представляет использование новейших информационных технологий, поэтому исследователи обращают внимание на место искусственного разума в системе информационной безопасности, на перспективность космических систем связи как элемента генетического оружия, на проблемы психотропного оружия и психотропной войны[101].

Информационное воздействие в XXI веке приобретает еще большую значимость, так как его направленность влияет на поведение большого количества людей, у которых под влиянием той или иной информации могут возникать потребности как конструктивного, так и деструктивного характера, что существенным образом влияет на политическую ситуацию в стране и в мировом пространстве в целом. Недаром средства информационного воздействия называют информационным оружием, так как по своим разрушительным силам оно сопоставимо с обычными средствами вооружения, а иногда по своим последствиям превосходит их. В современном научном

[101] Радиков И. В. Безопасность как ценностный императив мировой политики // Универсальные ценности в мировой и внешней политике / Под редакцией П.А. Цыганкова. М.: Издательство Московского университета, 2012. С. 51 –59.

дискурсе под информационным оружием понимается «совокупность информации, а также специальных методов, устройств и средств манипуляции ею для скрытого воздействия на информационный ресурс противника с целью достижения поставленных целей и решения задач информационной борьбы (войны)»[102].

Сегодня государство по-прежнему занимает главенствующее положение по отношению к личности и обществу, при этом интересы личности еще не находятся в центре государственных интересов, а общество не вышло из состояния «огосударствления». Для создания условий полной и успешной самореализации личности и становления гражданского общества необходимо изменить положение личности и общества по отношению к государству, на что, прежде всего, должно быть направлено государственное регулирование, и в первую очередь нормотворчество[103]. Государство должно помогать становлению гражданского общества, в том числе и в информационной сфере; сводить к минимуму те процессы, инспирируемые государством, которые приводят к замещению государством гражданского общества; передавать определенные функции обеспечения интересов личности общественным институтам по мере их создания; определять степень своего участия в обеспечении защиты интересов личности и общества под их контролем; помогать создавать в обществе инструменты влияния на власть[104].

Очевидно, что продолжение прежней практики нормотворчества и правоприменения при отсутствии единой проработанной государственной

---

[102] Баранов Н.А. Интегративный контекст национальной безопасности российского общества//Механизмы формирования гражданской идентичности в Российской Федерации: сборник статей и материалов Всероссийской научно-практической конференции «Механизмы формирования гражданской идентичности в Российской Федерации» (6-7 декабря 2013 г., г. Казань)/Под ред. А.Г.Большакова, Е.А.Терешиной. Казань: Казан. ун-т, 2014. – с. 172-182

[103] Бачило И. Л. Информационное прав. Под редакцией Б. Н. Топорнина. – СПБ.: Юридический центр Пресс, 2011. – с. 632-663

[104] Вишняков, ВТ. Национальная безопасность Российской Федерации: проблемы укрепления государственно-правовых основ /.Л.И. Васильева, АЛ. Гравина, НМ. Казанцев, ТБ. Конюхова, ЕЛ. Минина, Е.Н. Трикоз, А.Н. Чертков // Журнал российского права. -2005. - № 2.

политики в информационной сфере блокирует реализацию конституционных прав граждан, делает трудновыполнимой задачу построения правового государства и информационного общества в России. Как следует из Доктрины информационной безопасности РФ, на сегодняшний день в нашей стране отсутствует чёткая государственная политика в области формирования единого национального информационного пространства. На низком уровне функционирования находится механизм организации международного информационного обмена, а также основы интеграции отечественного информационного пространства в мировое. В следствие слабой государственной поддержки деятельности российских СМИ по продвижению их продукции на общемировой информационный рынок, страдает не только отечественная экономическая сфера производства информации, но и сфера глобального информационного обмена, испытывающая серьёзные деформации в своей структуре[105]. Значительной урон по этой же причине был нанесен кадровому потенциалу научных и производственных коллективов, непосредственно участвующих в разработке и создании средств информатизации, телекоммуникации и связи, который вылился в твёрдую и восходящую тенденцию к уходу из этих коллективов наиболее квалифицированных специалистов, а зачастую и вовсе их миграция за рубеж, что нашло отражение в ставшем популярным выражении «утечка мозгов». Эти обстоятельства являются основными причинами вытеснения российских СМИ, экономических и социально-политических участников в этой сфере общественных отношений[106].

Необходимость в обеспечении сохранности сведений, составляющих государственную тайну, и отставании отечественных информационных технологий, а также закупка импортной техники и привлечение иностранных фирм при создании внутренних информационных сетей, повышение вероятности несанкционированного доступа к обрабатываемой информации и

---

[105] Там же

[106] Вишняков, ВТ. Национальная безопасность Российской Федерации: проблемы укрепления государственно-правовых основ /.Л.И. Васильева, АЛ. Гравина, НМ. Казанцев, ТБ. Конюхова, ЕЛ. Минина, Е.Н. Трикоз, А.Н. Чертков // Журнал российского права. -2005. - № 2.

роста зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения – наиболее яркие порождения наличествующей системы защиты информации в России[107].

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения «информационного оружия» против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании[108].

Доктрина информационной безопасности РФ с учетом сложившегося положения дел определяет в качестве безотлагательных действий в решении проблемы разработки и создания механизмов формирования и реализации государственной информационной политики России повышение эффективности участия государства в формировании информационной политики государственных и частных СМИ, усовершенствование существующей системы противодействия информационным угрозам, а также методов и средств выявления, оценки и прогнозирования этих угроз. Другим важным решением является разработка и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов РФ[109].

Гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и

---

[107] Гайдарева И. Н. Информационная составляющая национальной безопасности Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. Майкоп 2007

[108] Воронович Н. К. Интернет как угроза информационной безопасности России. Автореферат – Краснодар: 2012

[109] Доктрина информационной безопасности Российской Федерации. URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 15.01.2018)

специального назначения, разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности РФ, а также сертификации этих систем и средств в совокупности должно привести к совершенствованию нормативной правовой базы обеспечения информационной безопасности РФ, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации, а также к установлению закрепленной за должностными лицами федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления, юридических лиц и граждан ответственности за соблюдение требований информационной безопасности[110].

Специалисты отмечают, что столь бурное развитие отрасли не могло не породить целого ряда проблем, связанных с его законодательным регулированием. Так, по мнению Николая Константиновича Вороновича, информационные технологии развиваются семимильными шагами и понятно, что многие правовые нормы либо устаревают, либо просто не дают ответа на возникающие вопросы[111]. Например, Федеральные законы «Об информации, информатизации и защите информации», «О средствах массовой информации», «О рекламе» приняты были более 10 лет назад. За это время возникла потребность приведения их в соответствие, как с действующим гражданским законодательством, так и с реалиями современного этапа развития информационных технологий. Требуется более точное описание понятия информации как отдельного объекта гражданских прав, определение прав и обязанностей обладателя информацией и пользователя информационных систем и информационно-телекоммуникационных сетей.

---

[110] Гайдарева И. Н. Информационная составляющая национальной безопасности Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. Майкоп 2007

[111] Воронович Н. К. Интернет как угроза информационной безопасности России. Автореферат – Краснодар: 2012

2.2. Цели, задачи, принципы и механизмы правового регулирования сети Интернет в РФ

В наиболее общем виде целевые установки и принципы регулирования информационного, в том числе и сетевого пространства, в России в настоящий момент отражены в Доктрине информационной безопасности России, первая редакция которой была учреждена в сентябре 2000 года. 6 декабря 2016 г. опубликован указ президента РФ Владимира Путина об утверждении новой Доктрины информационной безопасности РФ. Предпосылкой этого стал стремительный рост влияния интернет-технологий, характеризующийся увеличением числа пользователей Сети, ростом доверия аудитории к виртуальным источникам информации и существенным приростом доменов в зоне «.ru».

Как уже указывалось ранее, Доктрина информационной безопасности РФ представляет собой систему официальных взглядов на обеспечение национальной безопасности государства в информационной сфере, под которой понимают совокупность информации, сайтов, сетей связи, а также государственных и частных компаний, обеспечивающих их работу. Сама Доктрина состоит из 38 тематических статей, которые в свою очередь разбиты на пять глав. Текст нормативного правового акта начинается с перечисления национальных интересов Российской Федерации в сфере национальной безопасности. К таковым, согласно тексту Доктрины, законодатель отнёс следующие[112]:

- Обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации.
- Обеспечение в России устойчивого и бесперебойного функционирования критической информационной инфраструктуры.

[112] Доктрина информационной безопасности Российской Федерации. URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 15.01.2018)

- Развитие в России отрасли информационных технологий и электронной промышленности.
- Продвижение достоверной информации о государственной политике России и ее официальной позиции по социально значимым событиям в стране и мире.
- Содействие формированию системы международной информационной безопасности.

Среди основных информационных угроз, согласно тексту документа, можно выделить возможности информационно-технического воздействия на информационную инфраструктуру в военных целях, дискриминацию российских СМИ за рубежом, рост числа кибер-преступлений, доминирование ряда стран в информационном пространстве и их усиливающаяся разведывательная деятельность в России, а также ряд других.

Исходя из вышеизложенного, стратегической целью обеспечения информационной безопасности в области обороны страны Доктрина определяет защиту жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Организационную основу системы обеспечения информационной безопасности, согласно документу, можно обозначить как иерархически устроенную совокупность органов государственной власти – Совет Федерации, Государственная дума, Правительство, Совет Безопасности, Федеральные органы исполнительной власти (федеральные службы и агентства), органы судебной власти, а также ряд других публично-правовых институтов, таких как: Центральный банк, Военно-промышленная комиссия, межведомственные

органы, создаваемые президентом и правительством, органы исполнительной власти субъектов, органы местного самоуправления.

В новом документе, по сравнению с доктриной 2000 года, больший акцент сделан на опасности «информационно-психологического воздействия» на индивидуальное и общественное сознание граждан РФ со стороны иностранных спецслужб, а также террористических и экстремистских организаций. В редакции 2000 г. понятие «экстремистские организации» отсутствовало, а в качестве источников угроз были названы «диверсионно-подрывная деятельность иностранных специальных служб» и «деятельность международных террористических организаций».

Особое место в борьбе с информационными угрозами российскому государству, обществу и личности уделено важнейшему нормативно правовому акту – 114-ФЗ «О противодействии экстремистской деятельности», претерпевшему ряд редакций, в частности закон «О внесении изменений в отдельные законодательные акты РФ (по вопросу о противодействии экстремистской деятельности в Российской Федерации)». Федеральный закон доказал свою высокую эффективность в отношении экстремистских материалов. Причём, по мнению его критиков, даже слишком высокую. Так против практически всех редакций федерального закона выступила Общественная палата РФ[113]. Общественная палата и другие активисты, также заявляли, что в отношении информации, размещенной на сайтах в сети Интернет, эффективность закона осталось достаточно слабой. Связано это, прежде всего, с достаточно сложным механизмом признания материалов экстремистскими, который требует вынесения судебного решения по каждому конкретному случаю. В результате информация откровенно экстремистского характера могла находиться на сайтах в течение достаточно длительного времени. И когда судебное решение по конкретному материалу, размещенному на сайте в сети

[113] Необходимо конкретизировать понятие экстремистской деятельности//Сайт Общественной палаты РФ. URL: http://oprf.ru/expert/newsitem/16126 (дата обращения 11.12.2017)

Интернет, принималось, нередко выяснялось, что она уже была многократно скопирована и размещена на других сайтах.

К тому же указанный федеральный закон имел достаточно узкую направленность, позволяя блокировать доступ далеко не ко всей потенциально вредоносной информации (поскольку, например, те же сайты, содержащие детскую порнографию, никак нельзя признать экстремистскими).

Согласно положениям данного закона, информационные материалы признаются экстремистскими судом по месту их обнаружения, распространения или нахождения организации, осуществившей производство таких материалов, на основании представления прокурора или при производстве по соответствующему делу об административном правонарушении, гражданскому или уголовному делу. Федеральный список экстремистских материалов подлежит размещению в международный компьютерной сети Интернет на сайте федерального органа государственной регистрации. В настоящее время этот список содержит почти 4 400 различных материалов экстремистской направленности, значительная часть которых размещалась в сети Интернет[114].

Последний пункт вызвал при принятии данного закона особо серьезную критику в силу полной неопределенности критериев вынесения такого решения суда. Между тем, факт признания информации потенциально вредоносной влечет за собой внесение содержащих ее доменных имен и (или) указателей страниц сайтов, а также сетевых адресов, позволяющих идентифицировать указанные сайты, в Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено. После этого владельцу сайта в сети Интернет даются сутки на то, чтобы уда лить интернет страницу, содержащую информацию, распространение которой в РФ запрещено, в противном случае доступ к такому сайту блокируется.

---

[114] Федеральный список экстремистских материалов Минюста РФ. URL: http://minjust.ru/ru/extremist-materials?field_extremist_content_value=&search (дата обращения: 12.01.2018).

Таким образом, механизм, предусмотренный данным законом, действительно позволяет государству оперативно реагировать на появление в российском сегменте Интернета потенциально опасной информации. Однако такая оперативность имеет как положительную, так и отрицательную стороны. Отнести информацию к потенциально опасной и заблокировать доступ к ней достаточно просто. В то же время разблокировка информации в случае, если разместившее ее лицо не согласно ее уда лить и считает, что о решение о прекращении доступа к ней было принято неверно, возможна только на основе судебного решения и требует достаточно длительного срока.

Наконец, серьезным недостатком сложившейся практики ограничения доступа к вредоносной информации, содержащейся в сети Интернет, является тот факт, что при обнаружении такой информации, как правило, блокируется доступ не к конкретной странице сайта (хотя такая возможность законом и подзаконными актами предусмотрена), а весь сайт в целом.

Надо сказать, что данная проблема появилась отнюдь не с внесением рассматриваемых изменений в федеральные законы «Об информации, информационных технологиях и о защите информации» и ««О противодействии экстремистской деятельности»». Судебная трактовка федерального закона «Об экстремистской деятельности», когда при признании конкретных материалов экстремистскими суды выносили решения о запрещении доступа к сайту в целом, неоднократно вызывало крайне негативную реакцию всё той же Общественной палаты РФ[115, 116].

Что же касается, механизма регулирования, в частности блокировки, Интернет-ресурсов, то помимо блокировки решением суда, существует система досудебной (или внесудебной) блокировки сайтов. Ведомством, осуществляющим такую блокировку, является Роскомнадзор. С момента создания в 2008 г. и до 2012 г., наиболее важной задачей ведомства надзор за

---

[115] Законопроект о досудебной блокировке сайтов принят в первом чтении. Сайт Общественной палаты Российской Федерации. URL: https://www.oprf.ru/press/832/newsitem/23494 (дата обращения 11.04.2018)

[116] Божий дар или 282-я статья? Сайт Общественной палаты Российской Федерации. URL: https://www.oprf.ru/press/news/2013/newsitem/23228 (дата обращения 11.04.2018)

СМИЮ, в том числе выдача предупреждений о нарушениях. Так, медиа, получившее два и больше предупреждений, может быть закрыто. После принятия в 2012 г. поправок в закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и внедрения «Единого реестра доменных имен, указателей страниц», то есть список сайтов с «запрещенной информацией», ведомство смогло в полной мере осуществлять надзор над нарушением законодательства в информационной сфере, в том числе в национальном сегменте сети Интернет.

Согласно федеральному закону № 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” выделяется три типа «вредоносных» материалов, за которые Роскомнадзор блокирует сайты: детская порнография (и объявления о поиске несовершеннолетних для таких съемок); инструкции по изготовлению наркотиков и необходимых для этого веществ, а также по выращиванию наркотических растений вроде конопли; призывы покончить с собой и информация о методах суицида. Кроме того, Роскомнадзор блокирует страницы за экстремистские материалы и нарушение авторских прав[117].

Помимо собственного мониторинга запрещённой информации, ведомство получает информацию о нарушении подведомственного ему законодательства от судов, простых граждан и экспертов других государственных надзорных ведомств. Суд может заблокировать любой сайт, если сочтет, что материалы ресурса противоречат закону. Роскомнадзор обязан исполнять подобные судебные решения. Граждане имеют возможность пожаловаться на запрещенные материалы на сайте «Единого реестра». Эти сообщения фильтруют в ведомствах, заинтересованных в ограничении «вредоносной» информации – в самом Роскомнадзоре, Роспотребнадзоре, службе по борьбе

[117] 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” https://rg.ru/2012/07/30/zakon-dok.html

с наркотиками, Генпрокуратуре. Эти ведомства и сами занимаются мониторингом – у них есть специальные сотрудники, которые ищут запрещенные материалы в интернете. На основе сообщений граждан и собственного мониторинга чиновники отправляют в Роскомнадзор экспертные заключения через «Единую систему электронного взаимодействия с государственными органами власти» – о каждом сайте составляется отдельный документ. Основываясь на экспертных заключениях других ведомств Роскомнадзор, вносит сайты с запрещенной информацией в «Единый реестр». Последнюю подпись перед внесением ресурса в «черный список» ставит замглавы ведомства.

Далее Роскомнадзор отправляет уведомление хостинг-провайдеру, на котором размещен сайт. Хостинг-провайдер должен, в свою очередь, уведомить владельцев сайта, на это дается три дня. Иногда ведомство напрямую обращается к администрации ресурса. Получив уведомление, владельцы должны в течение трех дней удалить запрещенную информацию. Если речь идет об экстремистских материалах, правила строже: сайт блокируют без всяких предупреждений.

Существует также проработанная система санкций для тех провайдеров, кто отказывается от блокировки ресурса по требованию ведомства – это административное правонарушение, которое карается штрафом. Законодатель установил, что некоторые типы контента необходимо заблокировать как можно быстрее. К таким типам законодатели отнесли экстремистские материалы и призывы к несанкционированным общественным акциям, наущающим общественный и государственный порядок. Любую Интернет-страницу можно разблокировать, если владелец удалит противоправный контент, и эксперты Роскомнадзора смогут получить доказательства.

В начале 2016 г. вступил в силу «Закон о забвении», обязывающий интернет-поисковики удалять по требованию граждан ссылки на страницы в Интернете, содержащие не соответствующую действительности или

устаревшую информацию о заявителе[118]. Закон предусматривает возможность удаления неактуальной информации независимо от того, наносит ли она вред чести и достоинству заявителя. Под неактуальной информацией следует понимать информацию, утратившую своё значение в силу последующих действий заявителя или событий. В данном случае таким действием стала смена места работы –в результате информация о предыдущей работе в деловом справочнике просто перестала быть актуальной.

Федеральный закон № 97-ФЗ принятый 5 мая 2014 года «О внесении изменений в Федеральный закон „Об информации, отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей», также известный как «Закон о блогерах», стал точкой накала отношений органов государственного надзора в сфере Интернет-коммуникаций и, так называемой, либеральной общественности[119]. Закон, обязывающий авторов интернет-ресурсов (сайтов, блогов и пр.) с аудиторией «свыше 3000 пользователей в сутки» регистрироваться в Роскомнадзоре и накладывающий ряд ограничений на содержимое этих ресурсов[120]. Однако с 29 июля 2017 г. федеральным законом от № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» утратили силу законодательные нормы, регулировавшие деятельность блогеров. Так, признаны утратившими силу ст. 10.2 закона № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» и п. 2 ст. 1 закона № 97-ФЗ от 05.05.2014 г. «О внесении изменений в федеральный закон «Об информации, информационных технологиях и о защите информации» и

---

[118] Федеральный закон от 13 июля 2015 г. № 264-ФЗ “О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации”. URL: https://rg.ru/2015/07/16/informacia-dok.html (дата обращения 24.02.2018)

[119] Дмитриев Ю. А. Российский блогер — враг народа или иностранный агент? // Право и жизнь. — 2014. — № 191. – с. 103-107.

[120] Федеральный закон от 5 мая 2014 г. № 97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей». URL: https://rg.ru/2014/05/07/informtech-dok.html (дата обращения 24.02.2018)

отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей». «Закон о блогерах», вызвавший острую реакцию общественности прекратил, своё существование», что не позволяет судить о формирующейся в России системе государственного надзора в сфере информационной безопасности, как о некой репрессивной машине.

Одним из последних нормативно правовых актов значительно расширившим критерии и уточнившим виды запрещенной информации, представляющей угрозу информационной безопасности России, стал Федеральный закон “ О безопасности критической информационной инфраструктуры Российской Федерации” от 26.07.2017 № 187-ФЗ, который, воплощая цели и задачи заложенные в тексте Доктрины информационной безопасности 2016 г., впервые в законодательной практике России, утвердил государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Сама эта система определяется как «единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»[121]. Закон также закрепил внедрение особого реестра значимых объектов критической информационной инфраструктуры, который ведется в установленном им порядке.

Логичным продолжением воплощения в реальность идей, изложенных Доктриной информационной безопасности, в рамках информационной сферы национальной безопасности России, стало принятие федерального закона от 23.05.2015 № 129-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», согласно которому, нежелательной может быть признана неправительственная организация, которая представляет угрозу

[121] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 26.04.2018)

безопасности государства и основам конституционного строя[122]. Закон, в частности, запрещает функционирование Интернет-ресурсов признанными таковыми организациями.

Другим важнейшим направлением деятельности в сфере формирования единой системы государственной охраны информационной безопасности стало законодательное закрепление в ГК РФ понятия открытых лицензий. Использование открытых (свободных) лицензий, регулируется статьей ГК РФ «Открытая лицензия на использование произведения науки, литературы или искусства». В этой статье закреплено, что автор или иной правообладатель может предоставить пользователю открытую (простую, неисключительную) лицензию на использование его произведения. Открытая лицензия является договором присоединения, и условия такой лицензии должны быть доступны широкой общественности и размещаться таким образом, чтобы пользователь (лицензиат) мог ознакомиться с ними перед началом использования произведения[123].

2.3. Источники правового регулирования интернета в России

Характер и содержание политических процессов, структура политических, экономических, правовых, информационных и иных отношений в реформирующемся обществе России составляет на сегодняшний день сложный конгломерат взаимодействий и взаимовлияний различных сил, требующих пристального изучения и осмысления. Любая сфера жизни общества в

[122] Федеральный закон от 23.05.2015 № 129-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». URL: http://publication.pravo.gov.ru/Document/View/0001201505230001?index=0&rangeSize=1 (дата обращения: 23.04.2018)

[123] Федеральный закон от 12 марта 2014 г. № 35-ФЗ “О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации и отдельные законодательные акты Российской Федерации”. URL: https://rg.ru/2014/03/14/izm-gk-dok.html (дата обращения: 26.04.2018)

Российской Федерации регулируется в первую очередь её Конституцией, что прямо следует из её учредительного характера, а также статусы высшей юридической силы (ст. 15 Конституции РФ). Информационная сфера общества не составляет исключения, поэтому наиболее общие положения её регулирования закреплены в ряде статей основного закона. Так Конституция устанавливает, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст. 24). Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Гарантируется свобода массовой информации. Цензура запрещается (ст. 29). Информация и связь находятся в ведении РФ (ст. 71). Реализация указанных прав может быть сопряжена с ограничениями, установленными законом и необходимыми в демократическом обществе для уважения прав и репутации других лиц, охраны государственной безопасности и общественного порядка, что также закреплено в Конституции РФ[124].

Более того, среди основополагающих документов, регулирующих общественные отношения, важное место занимают международные договоры, подписанные Россией (в т. ч. как правопреемницей Советского Союза). Важнейших из них – Конвенция О Защите Прав Человека и Основных Свобод (ЕКПЧ). Россией Конвенция и протоколы к ней были ратифицированы и вступили в законную силу с 1998 года. В статье 10 Конвенции декларируется право любого человека свободно выражать и придерживаться своего мнения, а также распространять информацию и идеи без каких-либо ограничений. Статья подробно оговаривает те случаи, в которых государства вправе устанавливать ограничения в распространении информации. Наиболее приемлемым способом рассматривается лицензирование конкретного рода информации, но предусматриваются и другие. Тем не менее, протоколы 6, 12, 13 и 16 по

[124] Текст Конституции Российской Федерации на официальном сайте Президента РФ. URL: http://constitution.kremlin.ru (дата обращения 02.02.2018)

состоянию на январь 2018 год остаются не ратифицированными[125]. Одним из важнейших международных договоров, как уже отмечалось, является Хартия глобального информационного общества, принятая в Окинаве 22 июля 2000 г., в которой сказано, что все люди повсеместно, без исключения, должны иметь возможность пользоваться преимуществами глобального информационного общества[126].

К концу первого десятилетия XXI века Россия, присоединившись к основополагающим конвенциям Совета Европы, стала полноправным членом СБСЕ для долгосрочного сотрудничества по многим вопросам, но в первую очередь, по вопросам коллективной безопасности. Как показал уже накопленный солидный опыт развития отношений Россия – ЕС, такой комплексный подход отвечает интересам безопасности как Российской Федерации, так и ЕС, и входящих в него стран.

Первым посвященным исключительно информационным проблемам нормативным правовым актом стал Федеральный закон «Об информации, информатизации и защите информации» 1995 г., имевший предметом правового регулирования всю документированную информацию, на основе которой формируются информационные ресурсы самых разных разнообразных субъектов[127]. Однако положения Федерального закона «Об информации, информатизации и защите информации» утратили свою законную силу в связи с принятием Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», где все требования к защите информации изложены аналогично[128].

---

[125] Конвенция о защите прав человека и основных свобод" (Заключена в г. Риме 04.11.1950). URL: http://www.consultant.ru/document/cons_doc_LAW_29160/ (дата обращения: 22.01.2018)

[126] Окинавская Хартия глобального информационного общества. UNESCO's Global Search Engine EN. URL: http://www.unesco.org/new/fileadmin/MULTIMEDIA/FIELD/Tashkent/pdf/okinawa_charter_ru.doc (дата обращения 16.11.2017)

[127] Федеральный закон от 20.02.1995 № 24-ФЗ (ред. от 10.01.2003) "Об информации, информатизации и защите информации". URL: http://base.garant.ru/10103678/ (дата обращения 06.04.2018)

[128] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.04.2018) "Об информации, информационных технологиях и о защите информации URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 23.04.2018)

С 1993 г. подведомственные Минсвязи России предприятия разработали более 17 ГОСТ Р, утверждённых Госстандартом России. Ещё в конце 1999 г. по заданию Минсвязи России разработаны «Основные направления стандартизации в сфере информатизации на 1999-2002 гг.»[129]. В этом документе были определены основные направления стандартизации: обеспечение работы в сетях и соответствующих соединений, сбор данных и системы идентификации, сервисы управления данными, обеспечение программной инженерии и языков программирования, обеспечение представления информации, геоинформационные технологии, текстовые и учрежденческие системы, безопасность информационных технологий и др. Стандарты общего назначения содержат нормативную базу, обеспечивающую поддержку работы по отдельным направлениям, а также унифицируют терминологию. Технический комитет, действовавший при Министерстве связи и информатизации РФ до середины 90-х годов, принимал активное участие в разработке международных стандартов, создаваемых на основе, как правило, европейских стандартов (CEN), национальных стандартов США (ANSI) и международных технических спецификаций (ITS) Ассоциации производителей средств автоматической идентификации[130]. Таким образом, отраслевым министерством и подведомственными органами проводилась колоссальная работа в области формирования правовой базы, а также практики обеспечения информационной безопасности.

Углубляясь в изучение вопроса доступа в Интернет, учитывая характер и содержание указанных выше документов, можно констатировать, что доступ в Сеть является неотъемлемым правом человека. Такой вывод был также сделан в докладе ООН от 16 мая 2011 г. В докладе рассматриваются основные тенденции и проблемы в отношении реализации права каждого человека искать, получать и распространять информацию и идеи любого рода через Интернет. Намеренное

---

[129] Никитин В. В. Автоматизация процесса разработки образовательных стандартов профессионального образования для сферы информационно-коммуникационных технологий. Автореферат – СПб: 2009.

[130] Фадеев Л. А. Правовое регулирование бюджетно-надзорной деятельности федеральных органов исполнительной власти. Автореферат – М.:2007

лишение людей в различных регионах мира возможности выйти в Интернет отныне является нарушением прав человека[131].

В то же время, разумеется, право на доступ в сеть Интернет, так же, как и любое другое право человека, может быть в определенных случаях ограничено. И это вполне естественно, т.к. никакое право не может быть безграничным хотя бы потому, что в таком своем раз витии оно неизбежно рано или поздно начинает затрагивать права других лиц.

Общие подходы к ограничению права на доступ к Интернету сформулированы в том же докладе ООН[132]:

- ограничение должно быть предусмотрено законом, который ясен и доступен каждому (принципы предсказуемости и прозрачности).
- ограничение должно преследовать одну из целей, указанных в п. 3 ст. 19 международного пакта «О гражданских и политических правах», а именно: для защиты прав и репутации других лиц; для охраны государственной безопасности или общественного порядка, здоровья или нравственности населения (принцип законности).
- необходимость ограничения должна быть доказана и использована в качестве исключительного средства, необходимого для достижения предполагаемой цели (принципы необходимости и пропорциональности).

Данные требования к ограничению права на доступ к Интернету в целом соответствуют требованиям к ограничению конституционных прав граждан, вытекающим из ч. 3 ст. 55 Конституции РФ[133]:

- ограничение может быть установлено только федеральным законом;

---

[131] “Internet should remain as open as possible – UN expert on freedom of expression”. Geneva: UN Office of the High Commissioner for Human Rights. 3 June 2011. URL: http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=11108&LangID=E (дата обращения: 17.12.2017)

[132] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. URL: http:// www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (дата обращения 21.12.2017)

[133] Постановление Конституционного суда РФ от 30.10. 2003 № 15 – П «По делу о проверке конституционности отдельных положений Федерального закона “Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации” в связи с запросом группы депутатов Государственной думы и жалобами граждан С.А. Бунтмана, К.А. Катаняна и К.С. Рожкова». СЗ РФ, 2003, № 44, ст. 4358.

- любое ограничение должно решать одну из общественно значимых задач и добиваться определённую конституционную цель – защиты основ конституционного строя, прав и свобод человека и гражданина, обеспечение обороноспособности и безопасности России;
- всякое ограничение должно быть соразмерно этой цели.

Помимо этого, доклад содержит особое исключение из принципа общедоступности информации, распространяемой посредством сети Интернет – оно касается случаев распространения детской порнографии. Авторы доклада также призывают государства сосредоточить свои усилия на преследовании лиц, ответственных за производство и распространение детской порнографии, а не только на мерах по блокированию материалов с детской порнографией в Интернете. Таким образом, в докладе сформулированы основные принципы, на которых должны строиться правовые конструкции ограничения распространения информации в сети Интернет:

- ограничения применяются в качестве исключительной меры, и ровно такие же, какие приняты для информации, распространяемой за пределами сети Интернет;
- должен быть установлен понятный порядок и условия ограничения, решение об ограничении должен принимать суд;
- в законодательстве необходимы гарантии против злоупотреблений;
- исключение допустимо в отношении детской порнографии.

Поскольку указанный выше доклад ООН носит, вполне естественно, рекомендательный характер, конкретные основания и процедуры ограничения распространения информации в сети Интернет, а также доступа к ней должны устанавливаться национальными законодательствами. Отечественное законодательство в этой сфере является, в целом, разрозненным, хотя нельзя не отметить, что именно в последние годы законодателями предпринимаются

достаточно заметные и значимые шаги по установлению надзора за Интернетом со стороны различных государственных органов[134].

Долгое время в Российской Федерации единственным законом, который устанавливал условия и порядок ограничения передачи информации в сети Интернет, являлся федеральный закон «О противодействии экстремистской деятельности»[135]. Для соблюдения закона в сфере связи, ИКТ, а также зашиты персональных данных, в 2008 году указом президента России Дмитрием Медведевым была создана Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее по тексту – Роскомнадзор), входящую в структуру Минкомсвязи. Так, существовавшая до этого в ведении Минкомсвязи Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия (Россвязьохранкультура), была разделена на два органа: Федеральную службу по надзору в сфере связи и массовых коммуникаций (Россвязькомнадзор) и Федеральную службу по надзору за соблюдением законодательства в области охраны культурного наследия (Росохранкультура), перешедшую к Министерству культуры. Россвязькомнадзор был преобразован в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций[136].

В 2010 г. был принят комплексный федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию», положения которого были распространены в т.ч. и на информацию, размещаемую в сети Интернет. Согласно ст. 14 данного закона доступ к информации, распространяемой посредством информационно телекоммуникационных сетей, в т.ч. сети Интернет, в местах, доступных для детей, предоставляется лицом, организующим доступ к сети Интернет в таких местах (за исключением операторов связи, оказывающих эти услуги связи на основании договоров об

---

[134] Петров Д.Е. Ограничение распространения информации в сети Интернет. М.: Юридический мир, 2012, № 1, с. 32.

[135] Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 23.11.2015) “О противодействии экстремистской деятельности”. URL: http://base.garant.ru/12127578/ (дата обращения: 28.04.2018)

[136] Указ Президента РФ № 724. URL: http://www.consultant.ru/document/cons_doc_LAW_76855/ (дата обращения: 19.02.2018)

оказании услуг связи, заключенных в письменной форме), другим лицам при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию[137]. Сайт в информационно телекоммуникационной сети Интернет, не зарегистрированный как средство массовой информации, может содержать знак информационной продукции (в т.ч. в машиночитаемом виде) и/или текстовое предупреждение об ограничении ее распространения среди детей, соответствующие одной из категорий информационной продукции, установленных данным законом. Классификация сайтов осуществляется их владельцами самостоятельно.

Наконец, в 2012 г. были внесены изменения в федеральный закон «Об информации, информационных технологиях и о защите информации»[138], а также в закон «О защите детей от информации, причиняющей вред их здоровью и развитию», получившие широкий общественный резонанс, в частности из-за того, что вводили особый реестр запрещенных сайтов – «Единый реестр доменных имен, указателей страниц», то есть список сайтов с «запрещенной информацией», составляемый экспертами надзорных органов: Роскомнадзора, Федеральной службой Российской Федерации по контролю за оборотом наркотиков (далее по тексту – ФСКН) и Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека (далее по тексту – Роспотребнадзор). За время, прошедшее с принятия закона о «черных списках сайтов», Роскомнадзор заблокировал 52 тысячи страниц[139]. Центром компетенции, который мог бы одновременно работать и с интернет-компаниями, и с операторами связи стал Роскомнадзор. Этими изменениями, по сути, впервые в юридической практике нашей страны был предусмотрена жесткая процедура

---

[137] Федеральный закон от 29.12.2010 № 436- ФЗ (ред. от 05.04.2013) «О защите детей от информации, причиняющей вред их здоровью и развитию». СЗ РФ, 2011, № 1, ст. 48.

[138] Федеральный закон от 27.07.2006 № 149 – ФЗ (ред. от 05.04.2013) «Об информации, информационных технологиях и о защите информации». СЗ РФ, 2006, № 31 (ч. 1), ст. 3448.

[139] Единый Реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено. URL: https://eais.rkn.gov.ru/ (дата обращения: 19.02.2018)

оперативного реагирования государственных органов (а также иных лиц и организаций, осуществляющих размещение информации в сети Интернет либо предоставление доступа к ней) при случае выявления потенциально вредоносной информации в Интернете. Таковой, согласно ч. 5 ст. 15.1 «Об информации, информационных технологиях и о защите информации» являются:

- материалы порнографического характера несовершеннолетних, либо привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;
- информация о способах изготовления и использования наркотических веществ и их прекурсоров, местах приобретения таких средств;
- информация о способах совершения самоубийства, а также призывы к совершению самоубийства;
- любая другая информация, в отношении которой имеется вступившее в законную силу решение суда о признании ее информацией, распространение которой в Российской Федерации запрещено.

Еще на этапе принятия этого закона в общественном мнении появились замечания о данном нормативном правовом акте, как вводящем цензуру в российском сегменте сети Интернет, что откровенно противоречит ст. 29 Конституции[140]. Действительность, впрочем, оказалась достаточно далека от таких мрачных прогнозов. Практика применения норм, содержащихся в ст. 15.1 федерального закона «Об информации, информационных технологиях и о защите информации», показала, что применяются они не так уж часто и преимущественно на основании данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (то есть, в отношении тех видов вредоносной информации, которые прямо указаны в законе). При этом блокировалась, как правило, информация, опасный характер которой был очевиден и без судебного разбирательства, и применение ограничения доступа к ней не вызывало каких-либо серьезных протестов.

---

[140] Госдума приняла «драконовский» закон о блокировке сайтов без суда (Гаечный ключ — оружие депутата). Сего дня - Московский Комсомолец № 26416 (21 декабря 2013).

2.4. Проблема реализации конституционных прав и свобод российских граждан в интернет-среде

Учитывая выше сказанное, можно констатировать, что на череду брошенных информационной безопасности Российской Федерации вызовов, был дан уверенный ответ в виде формирования целостной, но дифференцированной системы государственной защиты в информационной среде, что нашло отражение в целой череде подписанных Россией международных норм и конвенций и принятием внутри страны комплекса правовых мер, реорганизации ведомств исполнительной власти, и в целом привлечение внимания широкой общественности к угрозам, представшими не только перед Россией, но и перед всем человечеством, в связи с вхождением в эпоху постиндустриальной (или информационной) эпохи развития всего общества. Тем не менее, несмотря на то, что все нормативно правовые акты РФ, регулирующие эту сферу общественных отношений, а в особенности, специализированные (Конституция РФ, федеральные законы, Доктрины безопасности), нацелены на поиск некого «здравого баланса» между обеспечением прав и свобод человека и гражданина, разумного компромисса между обеспечением прав пользователей, правообладателей и информационных посредников, отдельные случаи использования рассмотренного выше правового механизма и политической практики в ограничении доступа к информации получили широкий общественный резонанс в силу неоднозначности оснований такого ограничения, что позволило выявить их слабые места. Ситуацию осложняет и тот факт, что информационная сфера, а в особенности сеть Интернет, стала для более чем двух

миллиардов человек (несмотря на существующий колоссальный разрыв между «богатым севером» и «бедным югом») системообразующим фактором жизни[141].

Тем не менее, активное её влияние на состояние политической, экономической, оборонной и других составляющих безопасности всех стран, как в системе общепланетарного сотрудничества наций, так и для каждой суверенной нации в отдельности. По степени причиняемых человеку проблем и страданий решение об отключении от интернета сопоставимо с лишением свободы и чаще всего существенно затрудняет профессиональную деятельность[142].

Для существующей на данной момент системы регулирования сети Интернет в России, существует ряд правовых проблем, а также проблем в реализации охранительного права. В частности, закрытие доступа к всему сетевому ресурсу в целом, а не отдельным его страницам, содержащим запрещённую к распространению информацию (на чём в подавляющем большинстве случаев настаивают органы власти), не только не оправданно нарушает права его владельцев, но и провоцирует их на обход такой блокировки[143].

Так, например, администраторы веб-сайта «Луркоморья» (http://lurkmore.co/) после блокировки этого сайта по IP 85.17.124.180 сменили домен, после чего сайт продолжал благополучно функционировать. Таким образом, действия ФКСН и Роскомнадзора в данном случае способствовали лишь повышению популярности сетевой энциклопедии из-за возникшего в связи с публичными и судебными прениями сторон информационного повода. Более того, ФСКН России, возбудившая данное дело, в связи с возложенными на себя обязанностями мониторинга запрещённой информации, заявила о наличие на

---

[141] Internet access is «essential» human right, rules German court. URL: http://www.globalpost.com/dispatch/news/140business/technoloogy/130128/internet-access-essential-rulesgerman-court (дата обращения 14.12.2017)

[142] Левова И. Д. Права интернет-пользователей: Россия и мир, теория и практика. Аналитический доклад. М.: Ассоциация интернет-издателей; «Кабинетный учёный», 2013. – 144 с.

[143] Интернет вступился за «Луркоморье». URL: http://www.dp.ru/a/2012/11/12/Internet_vstupilsja_ za_Lu/ (дата обращения: 14.04.2018)

сайте «Луркоморье» пропаганды наркотических веществ (борьба с которыми, входила в прямую обязанность этого ведомства, вплоть до реформирования и упразднения этого ведомства). Однако пропагандой наркотиков ФСКН посчитала размещенные на сетевом ресурсе статьи о марихуане и ее действии[144]. Таким образом, создаётся правовой прецедент, когда под запрет можно подвести все энциклопедии, медицинские, биологические, химические и иные справочники, содержащие информацию о наркотических и психотропных веществах, не пропагандирующих их оборот, потребление или хранение в прямом виде.

Были претензии у администраторов сайта и к процедуре принятия решения о его блокировке. Так, в соответствии с ч. 7 ст. 15.1 федерального закона «Об информации, информационных технологиях и о защите информации» в течение суток с момента получения от оператора реестра уведомления о включении доменного имени и (или) указателя страницы сайта в сети Интернет в реестр провайдер хостинга обязан проинформировать об этом обслуживаемого им владельца сайта в сети Интернет и уведомить его о необходимости незамедлительного удаления интернет страницы, содержащей информацию, распространение которой в РФ запрещено. Однако, по уверениям администрации «Луркоморья», никакого уведомления ни о внесении сайта в реестр, ни о причинах такого внесения они не получали[145].

Во всех приведенных случаях органы государственной власти получали критические замечания от представителей гражданского общества, заключавшиеся в одной идеи в том, что должностные лица, принимающие решения о блокировке IP-адресов сайтов, содержащих вредоносную информацию, вместо блокировки конкретной страницы по ее IP исходят из какой-то презумпции противоправных намерений всех владельцев сайтов.

---

[144] ФСКН объяснила причины блокировки «Луркоморья». URL: http://www.interfax.ru/russia/news. asp?id=275427 (дата обращения: 14.04.2018)

[145] Интернет вступился за «Луркоморье». URL: http://www.dp.ru/a/2012/11/12/Internet_vstupilsja_ za_Lu/ (дата обращения: 14.04.2018)

Подобного рода законодательные инициативы ставят принципиальный вопрос о соблюдении принцип соразмерности совершенного правонарушения и понесенного наказания.

В связи с этим, ряд отечественных исследователей, указывает на необходимость внесения изменений в ряд федеральных законов[146], в частности, в ст. 15.1 федерального закона «Об информации, информационных технологиях и о защите информации», а также в подзаконные акты, регулирующие порядок блокировки информации, признанной запрещенной к распространению в РФ, указав в них, что блокировке по общему правилу подлежит конкретная страница (URL), содержащая вредоносную информацию. Весь сайт под лежит блокировке лишь в том случае, если он в целом имеет направленность на распространение вредоносной информации, причем это обстоятельство должно быть соответствующим образом мотивировано надзирающим органом.

Таким образом, глубокое изучение интернет-права Российской Федерации позволяет выделить следующие особенности регулирования отношений в виртуальном пространстве Интернета:

- социальное регулирование этой среды является не чисто правовым, нормативным. Оно использует как нормативные (нормы морали, этики и др.), так и ненормативные регуляторы (ценностный, директивный, информационный, технический);
- поскольку мировые сети не могут быть собственностью одного субъекта (человека, организации, страны и др.), то социальное регулирование основывается на принципах правового регулирования, саморегулирования и со-регулирования;
- деятельность участников базируется на новых, ранее неизвестных для правовой науки понятиях – «Интернет», «сайт», «провайдер», «доменные

[146] Щербович А.А. Свобода слова в Интернете: конституционно-правовой аспект. Монография. М.: ТЕИС, 2013. – 160 с.

имена», «электронная торговля» и др., без использования которых наша страна не войдет в глобальные международные структуры;

- информационно-правовая деятельность различных субъектов права в Интернете зачастую носит международную окраску и осуществляется на базе норм международных договоров и национального законодательства;
- в процессе правоприменения выявляются компьютерные и иные правонарушения, а виновные наказываются на основе норм международного и национального законодательства;
- оценка эффективности правового регулирования интернет-отношений осуществляется субъектами разных стран; можно прогнозировать, что в скором времени станет возможным выведение единых показателей эффективности регулирования в области всемирного виртуального пространства.

Также, как было определено, что: во-первых, ограничение права на доступ в сети Интернет может быть установлено федеральным законом и в той степени, в которой это необходимо для защиты прав и законных интересов общества, государства и личности. Во-вторых, в последние годы наблюдалось ужесточение законодательства в данной сфере, не были учтены позиции и предложения со стороны общественных организаций, а также зарубежный опыт. В-третьих, законодательно расширяется дискреция административных органов по принятию решения об ограничении доступа. Между тем, судебный порядок ограничения доступа к информации следует считать приоритетным. В-четвертых, остаются нерешенными актуальные проблемы технического характера, такие как массовые блокировки по IP-адресу, в ходе которых ограничивается доступ и к добросовестным ресурсам, а также появление значительного количества способов обхода блокировок.

Однако этими особенностями регулирования отношений в сфере виртуального пространства характеристика особенностей интернет-права не исчерпывается. Необходимо иметь в виду, что перед Россией по-прежнему стоит задача адаптации к существованию в цивилизованном информационном обществе и

ликвидации отставания в развитии информационно-коммуникативных технологий страны, в связи с чем предстоит дальнейшая законотворческая работа в области подготовки международных актов и договоров, касающихся регулирования своего сегмента всемирного виртуального пространства. Из этого следует, что интернет-право должно стать важнейшим компонентом глобального информационного общества и правового демократического государства[147].

[147] Федеральная целевая программа «Электронная Россия (2002–2010 годы)», утв. Постановлением Правительства РФ от 28 января 2002 г. № 65 // СЗ РФ. 2002. N 5. Ст. 531; Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г.

ЗАКЛЮЧЕНИЕ

В ходе изучения предмета исследования научной работы была определено решающие влияние ИКТ на жизнедеятельность всего общества в XXI веке, вызванное, в первую очередь, невероятной динамикой развития информационно-телекоммуникационных сетей, в особенности сети Интернет. С ростом влияния на все сферы жизни общества ИКТ, неизбежно встаёт вопрос об необходимости администрировании глобальных информационных сетей, защищённости законных прав личности и общества в информационной сфере, сохранности информационных ресурсов государства.

Поэтому неотъемлемым компонентом обеспечения безопасности функционирования информационной инфраструктуры любой страны, в том числе России, становится комплексная система регулирования, контроля и подержания общественных отношений (деятельность физических, юридических лиц и государственных образований) в сфере и по поводу сети Интернет.

Для выявления особенностей действующей в нашей стране системы правового регулирования сети Интернет, выявления политических и юридических особенностей этого регулирования (его принципов и методов), а также существующих проблем в функционировании, как неотъемлемого компонента общей структуры информационный безопасности России, было определено предметное поле информационной безопасности в рамках политической науки. Придерживаясь использования метода теоретического политологического анализа, как максимально объективного языка для описания политической реальности было дано определение национальной безопасности как многогранного явления, представляющего собой в самом общем виде состояние защищенности от внутренних и внешних угроз жизненно важных интересов личности, общества и государства.

Основываясь на совокупности поставленных задач, было также определено понятие «интернет-права». Интернет, согласно наиболее часто

встречающимся в рамках юридической науки подходам, представляет собой часть мировой коммуникационной технологии, которая активно развивается и эволюционирует в совершенно комплексную информационную индустрию.

Существующие на сегодняшний день механизмы правового регулирования сети Интернет в России можно в наиболее общем виде свести к трем: лицензирование, судебная блокировки, а также досудебная блокировка запрещённой к распространению информации.

Ставится вопрос о пределах необходимых вмешательств государства в область Интернет-сетей для обеспечения конституционных прав и свобод гражданина и личности с одной стороны, и обеспечения ее национальной безопасности в условиях нового мирового порядка с другой. В ходе поиска этого предела было установлено, что ограничение права на доступ в сети Интернет может быть установлено федеральным законом и в той степени, в которой это необходимо для защиты прав и законных интересов общества, государства и личности.

В последние годы наблюдается ужесточение законодательства в данной сфере, законодательно расширяется дискреция административных органов по принятию решения об ограничении доступа. Между тем, судебный порядок ограничения доступа к информации остаётся приоритетным.

В методологическом плане выпускная квалификационная работа построена на использовании теоретико-фундаментального политического анализа (общий анализ политики), формально-юридического, а также сравнительно-правового методов.

Подводя итоги, следует отметить, что оно вносит определенный вклад в разработку вопроса, касающегося функционально-концептуального описания данной темы, но, все же, остается достаточно большое количество вопросов по обозначенной теме, требующих научного обоснования. Относительно формулирования понятийного аппарата темы исследования, в работе предпринята попытка толкования ключевых понятий непосредственно относящихся к вопросу выработки концептуальных основ информационной

безопасности РФ, в частности, считаем существенным определение и обоснование понятия информационная безопасность РФ, но большинство из понятий осталось неосвещенными, и предполагают проведение дальнейших исследований, ориентированных на переосмысление концептуальных основ информационной безопасности РФ с позиций подхода «включения» угроз информационного характера в общее понимание «традиционных» угроз национальной безопасности РФ.

Тем не менее, были определены и подробно рассмотрены основы правового обеспечения информационной безопасности Российской Федерации в сфере регулирования сети Интернет, его цели, задачи и принципы, проведя подробный анализ нормативно-правовых актов, как федерального, так и международного уровня, выявив механизмы его правового регулирования, а именно нормативные правовые акты Российской Федерации, регулирующие и контролирующие деятельность физических, юридических лиц и государственных образований в сфере и по поводу сети Интернет, как неотъемлемый компонент обеспечения безопасности функционирования информационной инфраструктуры России.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. Бюллетень международных договоров. 1993. № 10. URL: http://pravo.gov.ru/proxy/ips/?divisions&edition=203000001 (дата обращения 04.02.2018)

2. Бюллетень международных договоров. 2001. № 11. URL: http://pravo.gov.ru/proxy/ips/?divisions&edition=203000001 (дата обращения 04.02.2018)

3. Всеобщая декларация прав человека" (принята Генеральной Ассамблеей ООН 10.12.1948). URL: http://www.consultant.ru/document/cons_doc_LAW_120805/ (дата обращения 08.04.2018)

4. Декларация о свободе обмена информацией в Интернете. URL: http://base.garant.ru/71036560/ (дата обращения 12.12.2017)

5. Доктрина информационной безопасности Российской Федерации. URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 15.01.2018)

6. Европейская декларация о правах человека и верховенстве права в информационном обществе URL: http://www.ifap.ru/ofdocs/eu/dhrrlis.pdf (дата обращения 12.12.2017)

7. Европейская конвенция о трансграничном телевидении (ETS № 132) URL: http://docs.cntd.ru/document/901739192 (дата обращения: 21.04.2018)

8. Конвенция о защите прав человека и основных свобод" (Заключена в г. Риме 04.11.1950). URL: http://www.consultant.ru/document/cons_doc_LAW_29160/ (дата обращения: 22.01.2018)

9. Конвенция о преступности в сфере компьютерной информации (ETS № 185). (Будапешт, 23 ноября 2001 г.) URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526#09741658132188091 (дата обращения 12.12.2017)

10. Конвенция о создании международного союза публикаций таможенных тарифов (Брюссель, 5 июля 1890 г.) URL: http://base.garant.ru/2540219/ (дата обращения: 21.04.2018)

11. Конвенция об обмене официальными изданиями и правительственными документами между государствами URL: http://base.garant.ru/2540309/ (дата обращения: 19.04.2018)

12. Конвенция Совета Европы о преступности в сфере компьютерной информации ETS №185 URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (дата обращения 01.04.2018)

13. Конституция Российской Федерации. URL: http://constitution.kremlin.ru (дата обращения 02.02.2018)

14. Национальный стандарт РФ «Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»

15. Окинавская Хартия глобального информационного общества. UNESCO's Global Search Engine EN. URL: http://www.unesco.org/new/fileadmin/MULTIMEDIA/FIELD/Tashkent/pdf/okinawa_charter_ru.doc (дата обращения 16.11.2017)

16. Постановление Конституционного суда РФ от 30.10. 2003 № 15 – П «По делу о проверке конституционности отдельных положений Федерального закона “Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации” в связи с запросом группы депутатов Государственной думы и жалобами граждан С. А. Бунтмана, К. А. Катаняна и К. С. Рожкова». СЗ РФ, 2003, № 44, ст. 4358.

17. Распоряжение Правительства РФ от 17 марта 2016 г. № 442-р “О прекращении действия Конвенции о создании Международного союза публикации таможенных тарифов”. URL: http://base.garant.ru/71354740/ (дата обращения: 21.04.2018)

18. Распоряжение Правительства РФ от 26 июля 2006 г. № 1060-р // СЗ РФ. 2006. № 31. Ч. II. Ст. 3529. URL: http://docs.cntd.ru/document/901989933 (дата обращения 04.02.2018)

19. Распоряжение Президента РФ от 22.03.2008 №144-рп “О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. №557-рп “О подписании Конвенции о киберпреступности” URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=417185#0867 3649535062591 (дата обращения 01.04.2018)

20. Россия приняла решение подписать Конвенцию. См.: распоряжение Правительства РФ от 27 декабря 2006 г. № 1821-р // СЗ РФ. 2007. № 1. Ч. II. Ст. 346. URL: http://www.consultant.ru/document/cons_doc_LAW_213218/ (дата обращения 12.12.2017)

21. Указ Президента Российской Федерации от 12 мая 2008 г. № 724 г. Москва “Вопросы системы и структуры федеральных органов исполнительной власти”. URL: https://rg.ru/2008/05/13/struktura-vlasti-dok.html (дата обращения: 17.02.2018)

22. Указ Президента РФ № 724. URL: http://www.consultant.ru/document/cons_doc_LAW_76855/ (дата обращения: 19.02.2018)

23. Указ Президента РФ от 15.05.2018 «О структуре федеральных органов исполнительной власти».

24. Федеральная целевая программа “Электронная Россия (2002–2010 годы)”, утв. Постановлением Правительства РФ от 28 января 2002 г. № 65 // СЗ РФ. 2002. N 5. Ст. 531; Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г.

25. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 26.04.2018)

26. Федеральный закон от 12 марта 2014 г. № 35-ФЗ “О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации и отдельные законодательные акты Российской Федерации”. URL: https://rg.ru/2014/03/14/izm-gk-dok.html (дата обращения: 26.04.2018)

27. Федеральный закон от 13 июля 2015 г. № 264-ФЗ “О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации”. URL: https://rg.ru/2015/07/16/informacia-dok.html (дата обращения 24.02.2018)

28. Федеральный закон от 20.02.1995 № 24-ФЗ (ред. от 10.01.2003) “Об информации, информатизации и защите информации”. URL: http://base.garant.ru/10103678/ (дата обращения 06.04.2018)

29. Федеральный закон от 23.05.2015 № 129-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». URL: http://publication.pravo.gov.ru/Document/View/0001201505230001?index=0&rangeSize=1 (дата обращения: 23.04.2018)

30. Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 23.11.2015) “О противодействии экстремистской деятельности”. URL: http://base.garant.ru/12127578/ (дата обращения: 28.04.2018)

31. Федеральный закон от 27.07.2006 № 149 – ФЗ (ред. от 05.04.2013) «Об информации, информационных технологиях и о защите информации». СЗ РФ, 2006, № 31 (ч. 1), ст. 3448.

32. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.04.2018) “Об информации, информационных технологиях и о защите информации URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 23.04.2018)

33. 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” URL: https://rg.ru/2012/07/30/zakon-dok.html (дата обращения 04.02.2018)

34. Федеральный закон от 29.12.2010 № 436- ФЗ (ред. от 05.04.2013) «О защите детей от информации, причиняющей вред их здоровью и развитию». СЗ РФ, 2011, № 1, ст. 48. URL: http://docs.cntd.ru/document/902254151 (дата обращения 04.02.2018)

35. Федеральный закон от 5 мая 2014 г. № 97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей». URL: https://rg.ru/2014/05/07/informtech-dok.html (дата обращения 24.02.2018)

36. Федеральный список экстремистских материалов Минюста РФ. URL: http://minjust.ru/ru/extremist-materials?field_extremist_content_value=&search (дата обращения: 12.01.2018).

37. A Declaration of the Independence of Cyberspace. URL: https://www.eff.org/cyberspace-independence (дата обращения 16.12.2018)

Книги и периодические издания

1. Алфёров А. Н. Информационное право в системе отраслей права // Вопросы теории и истории государства и права. Сибирский юридический вестник №4 – Иркутск: 2007

2. Анисимова А. С. Анализ правотворческой политики зарубежных стран в сфере регулирования интернет-отношений // Вестник Саратовской государственной юридической академии. 2014. № 5. С. 38-44.

3. Архипов, В. В. Интернет-право: учебник и практикум для бакалавриата и магистратуры / В. В. Архипов. — М.: Издательство Юрайт, 2016. — 249 с.

4. Балашов А. Н. Правовое регулирование интернет-отношений: основные проблемы и практика реализации в России//Среднерусский вестник общественных наук. Том 11. Серия №2. – 2016

5. Балуев, Д. Г. «Серые зоны» мировой политики. Очерки текущей политики/Д. Г. Балуев, А. А. Новоселов; отв. ред. М. А. Троицкий. – М.: Научно-образовательный форум по международным отношениям, 2010. – Выпуск 3. – 40 с.

6. Баранов Н. А. Интегративный контекст национальной безопасности российского общества//Механизмы формирования гражданской идентичности в Российской Федерации: сборник статей и материалов Всероссийской научно-практической конференции «Механизмы формирования гражданской идентичности в Российской Федерации» (6-7 декабря 2013 г., г. Казань)/Под ред. А.Г.Большакова, Е.А.Терешиной. Казань: Казанский университет, 2014. – с. 172-182

7. Бачило И. Л. Информационное прав. Под редакцией Б. Н. Топорнина. – СПБ.: Юридический центр Пресс, 2011. – с. 632–663

8. Борисов М. А., Романов О. А. Основы организационно-правовой защиты информации. (Гриф УМО по дополнительному профессиональному образованию). № 2. Изд.3, перераб. и доп. М.: Книжный дом «ЛЕНАНД», 2014. – 248 с.

9. Борщевский Г. А. Роль государства в формировании преемственного исторического сознания в контексте проблемы обеспечения национальной безопасности России // Информационный гуманитарный портал «Знание. Понимание. Умение». – 2012. – № 1 (январь – февраль)

10. Бусленко Н. И. Политико-правовые основы обеспечения информационной безопасности Российской Федерации в условиях демократических реформ Диссертация на соискателя доктора юридических наук. – М.: 2004

11. Васильев Г. В., Забегалин Д.А. Правовое регулирование электронного бизнеса в России и за рубежом // Электронный бизнес и реклама в Интернете. М., 2008. с. 106 – 114.

12. Венгеров А. Б. Право и информация в условиях автоматизации управления. Теоретические проблемы: Автореф. Дисс. на соиск. докт. юрид. наук. М., 1975

13. Вишняков В. Т. Национальная безопасность Российской Федерации: проблемы укрепления государственно-правовых// Журнал российского права. – 2005. – № 2 с. 3-34

14. Васильева Л. И., Гравина АЛ.// Журнал российского права. -2005. - № 2.

15. Возженников А. В. Национальная безопасность России: методология исследования и политика обеспечения: Монография. – М.: Изд-во РАГС, 2002. – 424 с.

16. Воронович Н. К. Интернет как угроза информационной безопасности России. Автореферат – Краснодар: 2012

17. Гайдарева И. Н. Информационная составляющая национальной безопасности Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. Майкоп 2007

18. Глебов, И. Н. Национальная безопасность Российской Федерации: проблемы правового регулирования. – СПб, 2000. – 98 с.

19. Гончаров С. А. Национальная безопасность: проблемы и пути решения. – М.: 1999

20. Гребенькова Л. А. Блокировка сайтов как метод борьбы с нарушением авторских и смежных прав в Интернете//Известия Юго-Западного государственного университета. Серия История и право № 4. – 2014

21. Грибанов Д. В. Правовое регулирование кибернетического пространства как совокупности информационных отношений: Дисс. на соиск. докт. юрид. наук. Екатеринбург, 2003. с. 7 – 16

22. Гуторов В. А., Радиков И. В. Концепции национальной безопасности в политическом дискурсе современной России: проблемы теории и методологии

анализа // Актуальные проблемы политической науки Вестник Санкт-Петербургского Университета СПб 2010 с. 130-139

23. Даниленков А. В. Интернет-право – М.: Юстицинформ, 2014 – С. 13 – 27.

24. Дмитриев Ю. А. Российский блогер — враг народа или иностранный агент? // Право и жизнь. — 2014. — № 191. – с. 103-107.

25. Домарев В. В. Безопасность информационных технологий. Системный подход – К.: ООО ТИД Диа Софт, 2004. – 992 с.

26. Идрисов Р. Ф. Теоретические и правовые проблемы обеспечения национальной безопасности Российской Федерации. Автореферат диссертации на соискателя кандидата доктора юридических наук. – М.: 2002

27. Институты глобального управления: состояние и возможности//Внешняя политика в условиях глобальной неопределенности: монография/Под ред. П.А.Цыганкова. М.: Издательство Русайнс. 2017 С.116-133

28. Информационный вестник Совета глав государств и Совета глав Правительств СНГ “Содружество”. № 1(37). С. 138 - 145.

29. Ирхин Ю. В. Методология и методика современного политического анализа: подходы и проблемы. – 2012, с. 71-79.

30. Казаковцев, А. В. НАТО и Кибербезопасность//Вестник Волгоградского государственного университета. Серия 4: История. Регионоведение. Международные отношения. – 2012. С. 109-114.

31. Казимирчук. В Л Социологические проблемы действия права в социалистическом обществе//Право и социология –М, 1973 С. – 60.

32. Каламанов В. А. Национальная безопасность Российской Федерации и межнациональные конфликты (теоретико-правовой анализ). Диссертация на соискателя доктора юридических наук. – СПб.: 2001

33. Копылов В. А. Информационное право. С. 130 - 140; Булатецкий Ю.Е.

34. Косолапов Н. А. Безопасность международная, национальная, глобальная: взаимодополняемость или противоречивость?// Мировая экономика и международные отношения. – 2006. – №9. – С.3-13

35. Кудрявцев В. Н., Васильев А. М. Право: развитие общего понятия// СОВ. гос-во и право. 1985. № 7. С. 12–13.

36. Кучерявый М. М. Национальной безопасности России в условиях современного глобального мира. Дисс. на соиск. докт. юрид. наук. – СПб.: 2014

37. Лапина М. А., Ревин А. Г., Лапин В. И. Информационное право. М.: ЮНИТИ-ДАНА, Закон и право, 2004 – 335 с.

38. Левова И. Д. Права интернет-пользователей: Россия и мир, теория и практика. Аналитический доклад. М.: Ассоциация интернет-издателей; «Кабинетный учёный», 2013. – 144 с.

39. Ловцов Д. А. Информационные правоотношения: особенности и продуктивная классификация // Информационное право. 2009. № 1.

40. Марков А. Некоторые аспекты информационной безопасности в контексте национальной безопасности // Вестник С.-Петерб. ун-та. Сер. 12. СПб., 2011. Вып. 1. С. 43-48.

41. Мартьянов Д. С. Практика взаимодействия интернет-сообщества и политических акторов в современной России. Диссертация на соискание учёной степени кандидата наук. Спб – 214 с.

42. Никитин В. В. Автоматизация процесса разработки образовательных стандартов профессионального образования для сферы информационно-коммуникационных технологий. Автореферат – СПб: 2009.

43. Никифоров А. А. Возможности и ограничения протестной мобилизации через социальные сети // Право и политика. – 2014. – № 12. – С. 1903-1909.

44. Петров Д. Е. Ограничение распространения информации в сети Интернет. М.: Юридический мир, 2012, № 1, с. 32

45. Политика и национальная безопасность. – СПб.: Астерион, 2004

46. Почепцов Г. Г. Контроль над разумом. – К.: КМА, 2012. – 350 с.

47. Почепцов Г. Г. Информационные войны. Новый инструментарий политики. – М.: Алгоритм, 2015

48. Почепцов Г.Г. Национальная безопасность стран переходного периода. – Киев, 1996

49. Правовое обеспечение электронной торговли // Коммерческое (торговое) право / Под ред. Ю.Е. Булатецкого. М., 2002. С. 880 - 886.

50. Пушкин Д. С. Интернет и противоправные деяния (теоретический аспект): автореф. дис. канд. юрид. наук. М., 2003. С. 10.

51. Радиков И. В. Безопасность как ценностный императив мировой политики//Универсальные ценности в мировой и внешней политике/Под редакцией П.А. Цыганкова. – М.: Издательство Московского университета, 2012 – с. 51-59

52. Рассолов И. М. Право и Интернет. Теоретические проблемы – М.: Норма, 2009. – 383 с

53. Рогозин Д. О. Проблема национальной безопасности России на рубеже XXI века. Дисс. на соиск. докт. философ, наук. – М.: 2000

54. Тедеев А. А. Предмет информационного права в условиях интернета//Республиканский НИИ интеллектуальной собственности «Информационное право»: Журнал. – М., 2006.

55. Фадеев Л. А. Правовое регулирование бюджетно-надзорной деятельности федеральных органов исполнительной власти. Автореферат – М.:2007

56. Цаплин А. Ю. Политические характеристики информационного общества//Известия Саратовского университета. Новая серия. Социология. Политология. 2008

57. Чумиков Л. Н. Бочаров М. П. Связи с общественностью: теория и практика. М., 2010. С. 393.

58. Шариков П. А. Информационный комплекс / П. А. Шариков // Безопасность Европы / Ин-т Европы РАН. - М.: Весь мир, 2011. - С. 581-591.

59. Шерстюк В. П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты

обеспечения информационной безопасности. – М.: Информационное общество, 1999, вып. 5, с. 3 – 5.

60. Шушков Г. М., Сергеев И. В. Концептуальные основы информационной безопасности Российской Федерации // Актуальные вопросы научной и научно-педагогической деятельности молодых ученых: сборник научных трудов III Всероссийской заочной научно-практической конференции (23.11.2015 – 30.12.2015 г., Москва) / под общ. ред. Е. А. Певцовой; редколл.: Е. А. Куренкова и др. – М.: ИИУ МГОУ, 2016. – С. 69 – 76.

61. Щербович А. А. Свобода слова в Интернете: конституционно-правовой аспект. Монография. М.: ТЕИС, 2013. – 160 с.

62. Ambrogi R. J. Chapter 12: Net Law: The Internet's Rules of the Road //The essential guide to the best (and worst) legal sites on the Web – 2nd edition. – N.Y.: ALM Publishing, 2004.

63. Cornish P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks//Directorate-General for External Policies of the Union/Policy Department. – Brussels: European Parliament, 2009. – 34 p.

64. Geers K. Strategic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence, 2011. – 169 p.

65. Glastris P. The powers that shouldn’t be; five Washington insiders the next Democratic president shouldn’t hire, The Washington Monthly (October 1987)

66. Herman K. On Thermonuclear War, 1960.

67. Kissinger H. A. The Necessity for Choice: Prospects of American Foreign Policy, 1961.

68. Lasswell G. D. Propaganda Technique in the World War,1923

69. Morgenthau H J. Politics Among Nations. The Struggle for Power and Peace. Second Edition, Alfred A. Knopf: New York, 1955.

70. Rosenberg, Scott. Dreaming in Code: Two Dozen Programmers, Three Years, 4,732 Bugs, and One Quest for Transcendent Software, 2007.

Электронные ресурсы

1. Аналитическая записка «Регулирование и развитие СМИ в интернете: европейский и российский опыт». ИКТ: ШАНС, УГРОЗА, ВЫЗОВ Российско-европейский центр междисциплинарных исследований Высшей Школы Экономики. URL: https://balticpractice.hse.ru/data/352/267/1240/Регулирование%20и%20развитие%20СМИ%20в%20Интернете_европейский%20и%20российский%20опыт.pdf (дата обращения 09.12.2017)

2. Божий дар или 282-я статья? Сайт Общественной палаты Российской Федерации. URL: https://www.oprf.ru/press/news/2013/newsitem/23228 (дата обращения 11.04.2018)

3. Госдума приняла «драконовский» закон о блокировке сайтов без суда (Гаечный ключ — оружие депутата). Сего дня - Московский Комсомолец № 26416 URL: http://www.mk.ru/politics/russia/article/2013/12/20/962896-gosduma-prinyala-drakonovskiy-zakon-o-blokirovke-saytov-bez-suda.html (дата обращения: 21 декабря 2013).

4. Единый Реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено. URL: https://eais.rkn.gov.ru/ (дата обращения: 19.02.2018)

5. Законопроект о досудебной блокировке сайтов принят в первом чтении. Сайт Общественной палаты Российской Федерации. URL: https://www.oprf.ru/press/832/newsitem/23494 (дата обращения 11.04.2018)

6. Интернет вступился за «Луркоморье». URL: http://www.dp.ru/a/2012/11/12/Internet_vstupilsja_ za_Lu/ (дата обращения: 14.04.2018)

7. Необходимо конкретизировать понятие экстремистской деятельности//Сайт Общественной палаты РФ. URL: http://oprf.ru/expert/newsitem/16126 (дата обращения 11.12.2017)

8. Официальный сайт Совета безопасности Российской Федерации // Стратегия национальной безопасности Российской Федерации до 2020 года. URL: http://www.scrf.gov.ru/docu-ments/1/99.html. (дата обращения: 08.02.2018)

9. ФСКН объяснила причины блокировки «Луркоморья». URL: http://www.interfax.ru/russia/news.asp?id=275427 (дата обращения: 14.04.2018)

10. GreatFire.org – Bringing Transparency To The Great Firewall Of China". URL: https://web.archive.org/web/20180518120336/https://en.greatfire.org/ (дата обращения: 14.04.2018)

11. Internet access is «essential» human right, rules German court. URL: http://www.globalpost.com/dispatch/news/140business/technoloogy/130128/internet-access-essential-rulesgerman-court (дата обращения 14.12.2017)

12. Internet should remain as open as possible – UN expert on freedom of expression. Geneva: UN Office of the High Commissioner for Human Rights. 3 June 2011. URL: http://www.ohchr.org/Documents/HRBodies/SP/Facts_Figures2011.pdf (дата обращения: 17.12.2017)

13. Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. URL: http:// www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (дата обращения 21.12.2017).