ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ ПАТРИСА ЛУМУМБЫ»

На правах рукописи

ТИМЕРБУЛАТОВ Тагир Алифович

ГОСУДАРСТВЕННАЯ ПОЛИТИКА РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ИСТОРИЧЕСКИЙ ОПЫТ И РЕАЛИЗАЦИЯ (1991– 2021 гг.)

Специальность 5.6.1. Отечественная история

ДИССЕРТАЦИЯ

на соискание ученой степени
кандидата исторических наук

Научный руководитель:
доктор исторических наук,
профессор Блохин В.В.

Москва – 2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. В XXI в. быстрыми темпами происходит формирование глобальной информационной цивилизации и становление постиндустриальных технологических, финансово-экономических и социальных систем при одновременном росте геополитической конкуренции. В этих условиях вопросы информационной безопасности приобретают особую значимость как в контексте более широких задач обеспечения национальной безопасности Российской Федерации, так и в сфере бизнеса, правопорядка, частной жизни россиян. Обеспечение информационной безопасности выступает одним из ключевых приоритетов государственной политики современной России, что нашло свое отражение в тексте Стратегии национальной безопасности Российской Федерации, утвержденной 2 июля 2021 г.[1]

Особую актуальность проблема защиты информационной безопасности России приобрела в связи с современными тенденциями в сфере международных отношений. В настоящее время, Российская Федерация, вставшая на путь последовательного отстаивания своих государственных интересов, реализует свою внутреннюю и внешнюю политику в условиях обострения глобальной геополитической конкуренции, одним из проявлений которой во второй половине 2010-х – начале 2020-х гг. стало фактическое развертывание идеологической и технологической информационной войны против России.

Президент России В.В. Путин в ходе заседания Совета безопасности РФ 20 мая 2022 г., посвященного вопросам надёжности работы отечественных информационных систем и сетей связи, а также мерам противодействия внешним угрозам в данной сфере, отметил, что данная тема является крайне актуальной и имеющей первостепенное значение для обеспечения суверенитета и безопасности, стабильности общественного

[1] Стратегия национальной безопасности Российской Федерации. Утверждена Указом

развития России.[2] Глава страны подчеркнул, что весной 2022 г. были успешно отражены предпринятые из-за рубежа массированные кибератаки на российские стратегически значимые информационные ресурсы государства, отечественной экономики, средств массовой информации. Успешная защита информационной безопасности России была обеспечена благодаря системным мерам, осуществленным в стране предшествующий период, однако стремительное развитие цифровых технологий в современном мире требует уделять постоянное внимание держать вопросам защиты информационной безопасности России.[3]

В данном контексте существенное научно-практическое и теоретическое значение приобретает изучение и осмысление новейшего исторического опыта формирования и реализации государственной политики России в сфере информационной безопасности. Комплексное освоение данной проблемы позволяет внести вклад в историографию российских реформ 1990 – 2000-х гг., в создание объективных научных представлений об эволюции системы государственного управления, образования, науки и технологий, социального пространства России на рубеже XX – XXI вв.

Следует отметить, что вопросы информационной безопасности и информационной войны присутствуют в истории человечества, в том числе в истории России, в течение многих столетий. Использование криптографии в дипломатии, военном деле, коммерции, сбор сведений и дезинформация противника в период военных действий, известные со времен античности, получали все более широкое распространение во всем мире в XIX – XX вв. по мере развития средств связи, коммуникационных технологий, международной прессы. Идеологические компоненты антироссийской информационной войны ярко проявлялись в период военных конфликтов,

---

[2] Вступительное слово Президента России В.В. Путина на заседании Совета Безопасности РФ «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства». 20 мая 2022 г. [Электронный ресурс] // Совет Безопасности РФ. Официальный сайт. URL: http://www.scrf.gov.ru/council/session/3241/ (Дата обращения: 23.05.2022)

[3] Там же.

например, в ходе Крымской войны 1853-1856 гг. когда в иностранной печати и средствах наглядной агитации (лубок, карикатура) формировался негативный образ России и российской армии.

В данном контексте важное научно-практическое и теоретическое значение приобретает исследование исторического опыта формирования и реализации государственной политики России в сфере информационной безопасности.

Степень изученности проблемы. В исследовании обозначенной проблемы правомерно выделить несколько историографических комплексов. К первой группе работ, вышедших в 1990-2000-х гг. *относятся исследования по истории становления государственной информационной политики Российской Федерации* феномену информационного общества в России, что нашло отражение в работах А.И. Ракитова[4], Г.Т. Артамонова, А.В. Волокитина, В.А Галатенко, Г.В. Емельянова, А.А. Стрельцова, Д.С. Черешкина и других специалистов в области цифровых технологий.[5] В этих публикациях впервые ставились вопросы формирования государственной информационной политики России и обеспечения информационной безопасности страны в новых государственно-правовых и экономических условиях.

В течение периода 1990 – 2000-х гг. научные школы изучения проблем информационной безопасности России сложились в Санкт-Петербургском государственном университете, МГУ им. М.В. Ломоносова, РУДН, МГИМО МИД России, РГГУ, Уфимском университете науки и технологий, ИНИОН РАН и ряде других центров вузовской и академической науки, в

---

[4] *Ракитов А.И.* Философия компьютерной революции. М.: Политиздат, 1991. 287 с. и др.

[5] *Артамонов Г.Т., Голубков А.С., Черешкин Д.С.* О государственной политике информатизации // Вестник Российского общества информатики и вычислительной техники. 1994. № 4-5. С.67; *Галатенко В.А.* Информационная безопасность – основы [Электронный ресурс] // Системы управления базами данных. 1996. № 1 URL: https://www.osp.ru/dbms/1996/01/13031466 (Дата обращения: 15.01.2022); *Волокитин А.В., Кристальный Б.В., Черешкин С.Д.* Россия: от информатизации – к информационному обществу // Информационное общество. 1999. № 3. С. 12-15; *Емельянов Г.В., Стрельцов А.А.* Проблемы обеспечения безопасности информационного общества // Информационное общество. 1999. № 2. С.15-16.

аналитических центрах МВД России, ФСБ, Министерства обороны РФ и ряда других ведомств, решающих задачи обеспечения национальной безопасности страны. С 1993 г. наблюдается постоянный рост количества и расширение тематического спектра публикаций, связанных с проблемами информационной безопасности. Данная тенденция была обусловлена, с одной стороны, все более интенсивной интеграцией Российской Федерации в систему глобальных информационных связей, внедрением новых коммуникационных технологий, с другой – подготовкой и принятием ряда законодательных актов, регулирующих сферу государственной безопасности в целом и непосредственно – информационной безопасности Российской Федерации, что обусловило развитие научных дискуссий по данной теме. Так, в 1990-е гг. были опубликованы статьи Д.Г. Черешкина, А.П. Курило и других авторов, посвященные проблемам обеспечения защиты баз данных, конфиденциальной информации в бизнесе и частной жизни пользователей Интернета[6], вышли в свет работы В.Б. Вехова по проблемам борьбы с киберпреступностью[7]. Данные публикации имели преимущественно технологический, либо юридический характер, но при этом нередко содержали материалы, отражавшие общую динамику информатизации российской экономики и общества, в том числе процесс формирования государственной политики РФ в области информационной безопасности.

Многогранные аспекты проблемы обеспечения информационной безопасности раскрыты в работах ученых кафедры информационной безопасности РГГУ- Шевцовой Г.А., Батищева С.А., Русецкой И.А. Важно, что в фокусе исследований не только актуальные проблемы информационной

---

[6] *Черешкин Д.Г., Курило А.П.* О проблеме защиты персональных данных в Российской Федерации // Проблемы информатизации. 1995. № 1. С. 32-34; *Герасименко В.Г., Сергеев В.В.* О проблеме информационной безопасности в банках России: потери, прогноз развития и некоторые пути решения // Вопросы защиты информации 1996. № 2. С. 52-56 и др.

[7] *Вехов В.Б.* Некоторые способы совершения преступлений с использованием техники // Современные проблемы правоохранительной деятельности: Межвузовский сборник научный трудов. Волгоград: Высшая школа МВД РФ, 1995. С. 69-74; *Он же.* Компьютерные преступления: Способы совершения и раскрытия. М.: Право и Закон, 1996. 182 с.

безопасности, но и глубоко осмыслен мировой исторический опыт защиты государственных секретов.[8]

Во второй половине 1990-х – 2010-е гг. в российской научной литературе утверждается проблематика ретроспективного изучения и прогнозирования информационных войн, что нашло отражение в статьях И.И. Завадского, Д.С. Черешкина, Г.Л. Смоляна, В.Н. Цыгичко и др.[9], монографиях В.Н. Лопатина, Д.Б. Фролова и др.[10]

Многие авторы разрабатывают вопросы информационной политики России в ракурсах международного права и теории военных наук, учитывая глобальный характер информационных процессов и возникающих в этой связи потенциальных угроз национальной безопасности страны[11]. Информационные факторы формирования исторического сознания, т.н.

---

[8] *Арутюнов В.В.* Об итогах IV Международной научно-практической конференции «Информационная безопасность: вчера, сегодня, завтра» // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2021. № 7. С. 37-40; *Arutyunov V.V* Application of artificial intelligence methods in solving information security problems: effectiveness and relevance of research results of Russian scientists // Научные и технические библиотеки**.** 2021. № 11. С. 105; *Шевцова Г.А., Батищев С.А.* Информационное общество: особенности развития. //Теория и практика экономики предпринимательства. Труды XVIII Всероссийской с международным участием научно-практической конференции. Симферополь, 2021. С. 387-391; *Они же.* Информационное пространство Российской Федерации как безопасная информационная среда// Информационная безопасность: вчера, сегодня, завтра. Сборник статей по материалам IV Международной научно-практической конференции. Под редакцией В.В. Арутюнова. Москва, 2021. С. 82-91; *Русецкая И.А.* Криптография: от прошлого к будущему // Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика. 2021. № 4. С. 47-57.; *Русецкая И.А.* Защита государственных секретов в Чешской Республике // Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика. 2019. № 3. С. 36-50.

[9] *Черешкин Д.С. и др.* Реалии информационной войны // Конфидент. 1996. №4. С. 9-12; Завадский И.И. Информационная война – что это такое? // Защита информации. Конфидент. 1997. № 4. С.13-20.

[10] *Лопатин В.Н., Цыганков В.Д.* Психотронное оружие и безопасность России. Москва, 1999; *Фролов Д.Б., Воронцова Л.В.* Информационное противоборство: история и современное состояние. Москва: Горячая линия – Телеком, 2004; *Медовкина Л.Ю.* Эволюция информационных войн от древности к современности // Известия Тульского государственного университета. Гуманитарные науки. 2017. № 3. С. 15-24 и др.

[11] *Лисичкин В.А., Шелепин Л.А.* Третья мировая информационно-психологическая война. М.: Академия социальных наук, 1999; *Медовкина Л.Ю.* Геополитический аспект информационного противостояния РФ и США // Via in tempore. История. Политология. 2020. Т. 47. № 3. С. 618-629 и др.

«войны памяти» обстоятельно исследованы в работах В.Э. Багдасаряна[12]. При этом юридический и технологический подходы к проблемам информационной безопасности дополняются исследованиями политико-философского и социального профиля[13]. В начале XXI в. вышли в свет монографии В.Н. Лопатина и А.А. Стрельцова, подводящие определенный итог формированию правовой базы и институционализации государственной политики России в области информационной безопасности на начальном этапе рыночных преобразований[14].

Тема фальсификации истории Великой Отечественной войны 1941 – 1945 гг. как одного из компонентов современной информационной войны Запада против России нашла отражение в научных работах доктора исторических наук, профессора В.В. Блохина и ряда других авторов[15].

---

[12] *Багдасарян В.Э., Ларионов А.Э., Реснянский С.И.* Информационные факторы формирования исторического сознания молодежи (на примере изучения представлений о Великой Отечественной войне) // Вопросы истории. 2022. № 8-1. С. 34-49; *Багдасарян В.Э., Балдин П.* Перспективы развития искусственного интеллекта в актуальной повестке политических и социальных рисков глобальных трансформаций// Журнал политических исследований. 2020. Т. 4, № 2. С. 10-22.

[13] *Расторгуев С.И.* Философия информационной войны / Российская академия образования, Московский психолого-социальный институт. М.: МПСИ, 2003. 495 с. и др.

[14] *Лопатин В.Н.* Информационная безопасность России / МВД РФ; Санкт-Петербургский государственный университет. СПб: Университет, 2000. 424 с.; *Стрельцов А.А.* Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовничего, В.П. Шерстюка. МГУ им. М.В. Ломоносова. Кафедра информационной безопасности. М.: МЦНМО, 2002. 289 с.

[15] *Блохин В.В.* Фальсификация истории Великой Отечественной войны и русофобия в современном политическом контексте либеральных историках, свободе мнений и адвокатах гитлеризма. (современные фальсификаторы Великой Отечественной войны против России) // Вестник МНЭПУ. 2021. № 2. С. 179-185; *Он же.* «Холодная война» в историческом сознании: фальсификация Великой Отечественной войны в работах Б.В. Соколова // Патриотическое воспитание в системе высшего образования: Материалы Всероссийской научно-практической конференции с международным участием, посвященной 75-летию начала контрнаступления советских войск в битве под Москвой, Москва, 01 - 02 декабря 2016 года / Ответственный редактор З.З. Мухина. Москва: Национальный исследовательский технологический университет «МИСиС», 2017. С. 12-20; Войны памяти вместо памяти о войне: исторические уроки прошлого и политические вызовы современности: Сборник материалов всероссийской научно-практической конференции с международным участием, посвящённой 80-й годовщине начала Великой Отечественной войны, Ростов-на-Дону, 29 апреля 2021 года. Ростов-на-Дону: Ростовский государственный медицинский университет, 2021. 457 с. и др.

Другой комплекс исследований работ связан с проблематикой свободы СМИ и их роли и места в обеспечении информационной безопасности российского общества. В том числе выходят в свет труды Т.М. Горяевой по истории политической цензуры в СССР[16], книги и статьи И.М. Дзялошинского, посвященные российской журналистике в постсоветский период[17]. В публикациях Е.И. Прохорова, А.В. Россошанского, Ф.В. Ахмадиева и др. раскрывается формирование социальной ответственности отечественных СМИ в контексте проблем защиты государственной тайны, конфиденциальности частной жизни, коммерческих секретов[18].

Третья группа исследований включает работы по истории советских и российских спецслужб, систем организации специализированной связи, научных и образовательных организаций информационно-технологического профиля. К этой группе относятся публикации С.А. Воронцова, Е.М. Стригина и других авторов, в которых затрагиваются вопросы организационного и технологического обеспечения информационной безопасности государства в СССР и постсоветской России[19]. А.В. Бабаш, Е.К. Баранова и Д.А. Ларин освещают применение в России систем криптографии с эпохи раннего Средневековья до современности; и др.

Отдельные аспекты исследуемой проблемы затрагиваются в изданиях, посвященных истории научных и образовательных организаций

---

[16] *Горяева Т.М.* Политическая цензура в период стагнации и кризиса власти и идеологии в СССР (1969 – 1991 гг.) // Политическая цензура в СССР. 1917-1991. М.: РОССПЭН, 2009.

[17] *Дзялошинский И.М.* Российский журналист в посттоталитарную эпоху. Москва: Издательский дом «Восток», 1995. 300 с.; *Он же.* Медиапространство России: коммуникационные стратегии социальных институтов. Москва: Изд-во АПК и ППРО, 2013. 479 с. и др.

[18] *Прохоров Е.П.* Средства массовой информации и информационная безопасность // Информационное общество. 1997. Вып. 4-6. С.36-42; *Россошанский А.В*. Средства массовой информации как институт системы информационной безопасности // Известия Саратовского университета. Серия: Социология. Политология. 2008. Вып.1. С. 121; *Ахмадиев Ф.В.* Свобода слова и ответственность журналиста // Вестник Башкирского университета. 2011. Т. 16. № 2. С. 529-530 и др.

[19] *Стригин Е.М.* От КГБ до ФСБ (поучительные страницы истории). М., 2005; *Миркин В.В.* Эволюция отечественных систем радиорелейной связи // Вестник Томского государственного университета. Серия: История. 2013. № 372. С.123-125 и др.

информационно-технологического профиля[20]. В том числе важный вклад в научно-теоретическую разработку истории развития государственной политики России в области информатизации и обеспечения информационной безопасности вносят труды д.и.н. Р.Г. Юсупова, под научным руководством которого в Башкирском госуниверситете были подготовлены публикации Т.А. Тимербулатова и других авторов по данной тематике[21], в том числе обоснована постановка проблемы настоящего диссертационного исследования в рамках исторической науки[22].

В конце 2000-х – 2010-е гг. выходят в свет работы А.В. Короткова, В.В. Кристального, Г.Л. Смоляна, Д.С. Черешкина, А.А. Чеботаревой, И.Л. Бачило, М.А. Вуса и других авторов, посвященные развитию государственной информационной политики Российской Федерации. В большинстве данных публикаций затрагивались и различные аспекты обеспечения информационной безопасности[23].

---

[20] МИЭТ 50 лет. Годы, люди, события. М.: МИЭТ, 2015. 392 с.; *Абакумов Е.М., Кожевников Н.О. Петунин С.А.* В век высоких технологий: к юбилею отделения информационных технологий и информационной безопасности ФГУП «ВНИИА» / Под ред. Ю.Н. Бармакова. Всероссийский научно-исследовательский институт автоматики им. Н.Л. Духова. – Москва: Кодекс, 2016. 204 с. и др.

[21] *Юсупов Р.Г., Чинаев Т.В* Утверждение принципа информационной открытости государственных и муниципальных учреждений // Государственное управление в России: историко-правовые аспекты: Монография / Коллектив авторов; под научной редакцией Р.Г. Юсупова. Москва: ИНФРА-М, 2018; *Тимербулатов Т.А., Юсупов Р.Г.* Предпосылки развития правовых основ информационной безопасности в 1991-1993 гг. (по материалам Республики Башкортостан): исторический обзор // Современная наука: актуальные проблемы теории и практики. Серия: Гуманитарные науки. 2020. № 3-2. С. 23-28; *Тимербулатов Т.А.* Развитие принципов информационной безопасности и информационного законодательства РФ в 1990-е и 2000-е годы: сравнительно-исторический аспект // Власть истории и история власти. 2020. Т. 6. № 5(23). С. 750-762.

[22] *Тимербулатов Т.А., Юсупов Р.Г.* Информационная безопасность: об актуальности исторического исследования проблемы // Инновационная наука. 2019. № 9. С. 23-27 и др.

[23] Государственная политика Российской Федерации в области развития информационного общества / *А.В. Коротков, Б.В. Кристальный, И.Н. Курносов*; под науч. ред. А.В. Короткова. М.: Трейн, 2007. 469 с.; *Смолян Г.Л., Черешкин Д.С.* Двадцать лет спустя (От Концепции информатизации советского общества к Стратегии развития информационного общества в Российской Федерации) // Информационные ресурсы России. 2009. № 2(108). С. 11-18; *Балашова М.А.* Информационное общество: теоретическая база и российская практика // Известия Иркутской государственной экономической академии. 2013. № 5. С. 5-12; *Чеботарева А.А.* Информационная политика России в обеспечении информационной безопасности личности: история и современность // История государства и права. 2015. № 24. С. 24-28; Информационные технологии:

Вопросы формирования информационной политики Российской Федерации нашли отражение в научных публикациях представителей научной школы гуманитарных и социальных наук РУДН Д.В. Юркова, С.А. Моргуновой и др.[24] Большое научно-теоретическое и прикладное значение имеют исследования в области теории и истории международных отношений специалистов РУДН К.П. Курылева, Д.В. Станис, М.А. Шпаковской и др., в которых, в том числе рассматриваются вопросы обеспечения внешней информационной безопасности России, освещается сотрудничество стран СНГ, ЕАЭС и ШОС в области информационных коммуникаций, глобальные информационные процессы[25].

Во второй половине 2010-х – начале 2020-х гг. выходят в свет работы, посвященные проблемам трансформации сущностных основ государственно-общественных отношений в условиях глобальной информационной цивилизации. Так, в трудах С.Н. Федорченко на основе осмысления мирового опыта развития цифровых социально-политических коммуникаций,

---

инновации в государственном управлении / *Алферова Е.В., Бачило И.Л.* Москва: ИНИОН РАН, 2016; *Вус М.А., Макаров О.С.* Четверть века законодательного регулирования института государственной тайны на постсоветском пространстве // Новый юридический вестник. 2017. № 2 (2). С. 1-7 и др.

[24] *Юрков Д.В.* Проблемы информационно-психологической безопасности общества в контексте обеспечения национальных интересов России в информационной сфере // Вестник РУДН. Серия: Государственное и муниципальное управление. 2016. № 1. С. 39-49; *Кравчук Н.Ю., Юрков Д.В.* Государственные информационные ресурсы Российской Федерации на современном этапе: проблемы и перспективы развития // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2017. № Т.4. № 2. С.116-129; Информационно-коммуникационные технологии третьего тысячелетия / П.*В. Меньшиков, Е.Е. Юсупова, В.С. Новикова, С.А. Моргунова и др.* М.: МГИМО (университет) МИД Российской Федерации, 2020. 460 с. и др.

[25] *Курылев К.П., Цаканян В.Т.* Цифровая зависимость НАТО // Вестник Московского государственного областного университета. Серия: История и политические науки. 2018. № 1. С. 45-53; *Курылев К.П., Пархитько Н.П., Смолик Н.Г.* Национальные режимы регулирования сети Интернет в странах СНГ // Постсоветские исследования. 2021. Т. 4. № 8. С. 705-718; *Курылев К.П., Шпаковская М.А., Станис Д.В., Петрович-Белкин О.К.* Культурно-гуманитарное сотрудничество государств ЕАЭС как инструмент евразийской интеграции в 2015-2021 гг. // Вопросы истории. 2021. № 11-1. С. 120-126; *Курылев К.П., Малышев Д.В., Хотивришвили А.А., Шабловский В.С.* ШОС и ЕАЭС в контексте Евразийской интеграции // Мировая экономика и международные отношения. 2021. Т. 65. № 2. С. 81-88; *Паредес Д.С., Станис Д.В.* Теория информационной конвергенции в системах как один из подходов к осмыслению государственных и социальных проблем // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2016. № 2. С. 50-62 и др.

разрабатываются теоретические аспекты взаимодействия человека и власти[26]. Эволюция информационной политики государства и СМИ в контексте глобальных технологических и геополитических трансформаций рубежа второго и третьего десятилетий XXI века рассматривается в исследованиях П.В. Меньшикова, В.С. Новиковой и других специалистов МГИМО МИД России[27]. Вклад России и стран СНГ в формирование системы международной информационной безопасности (МИБ) нашел отражение в фундаментальном труде А.В. Крутских, Е.С. Зиновьева и др. «Международная информационная безопасность: подходы России», подготовленном под эгидой МГИМО в 2021 г.[28]

В 2010-е гг. продолжается утверждение междисциплинарных подходов к проблемам защиты информации. Так, вопросы государственной политики обеспечения информационной безопасности России в сфере культуры нашли отражение в совместных публикациях представителей Министерства культуры РФ, РГГУ, МФТИ, ВНИИ проблем вычислительной техники и информатизации и др.[29]

За рубежом тема информатизации, включая оценки и прогнозы ее воздействия на мировую экономику, социальные процессы и геополитику, активно разрабатывается в 1980-е – 1990-е гг. Ряд наиболее значимых работ

---

[26] *Федорченко С.Н.* Сетевая легитимация политических режимов: теория и технологии. М.: Московский государственный областной университет. 2018. 202 с.; *Он же.* Феномен искусственного интеллекта: гражданин между цифровым аватаром и политическим интерфейсом // Журнал политических исследований. 2020. Т. 4, № 2. С. 34-57 и др.

[27] Основы теории и практики интегрированных коммуникаций и медийной политики в «новой реальности» / *П.В. Меньшиков, В.С. Новикова, А.А. Агрба и др.* М.: МГИМО (университет) МИД Российской Федерации, 2022. 461 с. и др.

[28] Международная информационная безопасность: подходы России / А.В. Крутских, Е.С. Зиновьева, В.И. Булва и др. М.: МГИМО (Университет), 2021. 47 с.

[29] *Кондратьев Д.В. и др.* Проблемы сохранения цифрового культурного наследия в контексте информационной безопасности // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2013. № 14(115). С. 36-52; *Конявский В.А. и др.* Формирование системы обеспечения информационной безопасности Российской Федерации в сфере культуры // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2015. № 12(155). С. 24-42 и др.

по данной проблематике был переведен на русский язык[30]. Среди новейших публикаций западных авторов, анализирующих универсальные проблемы информационной безопасности в эпоху цифровых технологий, выделяется монография Дж. Каравелли и Н. Джоунса, вышедшая в 2019 г. [31]. В XXI в. в научных кругах США и Евросоюза все более популярной становится тема информационных и гибридных войн[32], подходы к изучению которой на Западе в 2010-е гг. приобретают резко политизированный характер и риторику в духе «холодной войны», уделяя основное внимание цифровому военному потенциалу России и Китая[33].

Самостоятельный сегмент мировой научной литературы, посвященной теоретическим проблемам информатизации и глобальной международной безопасности, составляют труды ученых Китайской Народной Республики, реализующей внутреннюю политику «Сильного сетевого государства» и проводящей в сотрудничестве с Россией курс поддержки глобальной информационной безопасности в форматах ООН, ШОС и БРИКС[34].

Таким образом, к настоящему времени сложился обширный и разнородный комплекс научных исследований, отражающий процесс развития государственной информационной политики России в постсоветский период, включая ряд аспектов обеспечения информационной

---

[30] *Стоуньер Т.* Информационное богатство: профиль постиндустриальной экономики // Новая технократическая волна на Западе / Под ред. П.С. Гуревича. М.: Прогресс, 1986; *Тэпскотт Д.* Электронно-цифровое общество: Плюсы и минусы эпохи сетевого интеллекта / Дон Тапскотт; Пер. с англ. И. Дубинского под ред. С. Писарева. Москва, 1999. 403 с.

[31] *Caravelli J., Jones N.* Cyber Security: Threats and Responses for Government and Business (Praeger Security International). Praeger, 2019. 245 p.

[32] *Libicki M.* Conquest in cyberspace. National security and information warfare. Santa Monica: RAND, 2007. 307 p.; *Rid T., Hecker M.* War 2.0: Irregular Warfare in the Information Age (Praeger Security International). Praeger, 2009, 280 p.; *Jason R. Fritz.* China's Cyber Warfare Lexington Books, 2017. 216 p.

[33] См.: *Ермикова М.С.* Американская школа исследований информационных войн // Политическая экспертиза: ПОЛИТЭКС. 2018. Т. 14. № 1. С. 117-138.

[34] *Понька Т.И., Рамич М.С., У Ю.* Информационная политика и информационная безопасность КНР: развитие, подходы и реализация // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2020. Т. 20. № 2. С. 382-394; *Ромашкина Н., Задремайлова В.* Эволюция политики КНР в области информационной безопасности // Пути к миру и безопасности. 2020. № 1(58). С. 122-138.

безопасности страны, главным образом, в историко-правовом и технологическом контексте. Тема государственной политики Российской Федерации в области обеспечения информационной безопасности в 1991 – 2021 гг. еще не ставилась и не изучалась в качестве комплексной проблемы исторической науки, что подтверждает научную актуальность предпринятого диссертационного исследования.

Предметом исследования является процесс формирования концептуальных, правовых и организационных основ государственной политики Российской Федерации в области информационной безопасности, развитие и деятельность институтов информационной безопасности государства, общества и бизнеса.

Объектом исследования являются концепции и программы государственной политики РФ в области информационной безопасности, государственные структуры, коммерческие предприятия, общественные организации, научные и академические центры, IT-бизнес-сообщества, участвовавшие в формировании и реализации государственной политики России в области информационной безопасности в 1991-2021 гг.

Целью исследования является реконструкция исторического опыта становления и реализации государственной политики РФ в сфере информационной безопасности в 1991 – 2021 гг.

Для достижения поставленной в работе цели автором решаются следующие **задачи**:

- исследовать эволюцию концепций и правовых норм государственной политики РФ в области информационной безопасности в рассматриваемый период;

- раскрыть содержание общественных дискуссий в России по проблемам информатизации и защиты информации;

- выявить специфику становления и деятельности государственных и коммерческих институтов информационной безопасности на разных этапах российского исторического процесса;

- проанализировать процесс формирования в начале XXI в. современной системы организационного и кадрового обеспечения информационной безопасности государства, экономики и общества России;

- определить роль и место информационной безопасности в культурной, экономической и общественной жизни российского общества;

- выявить особенности и специфику национальной модели государственной политики РФ в области внутренней и международной информационной безопасности в условиях глобальных технологических и геополитических трансформаций XXI в.

Хронологические рамки диссертации. Нижняя граница исследования определяется 1991 г., связанным с началом нового периода отечественной истории, обусловившим становление новых подходов к обеспечению информационной безопасности российского государства и общества. Верхняя хронологическая граница определяется реализацией геополитической стратегии последовательного отстаивания Россией своих национальных интересов в условиях растущих внешних, в том числе информационных угроз, что нашло отражение в принятой в 2021 г. «Стратегии национальной безопасности Российской Федерации».

В работе и более ранние исторические периоды, что позволило более глубоко проанализировать процессы трансформации государственной политики России в области информационной безопасности в начальный период рыночных преобразований, показать истоки общественного восприятия феномена информатизации в этот период, характер реформирования органов информационной безопасности и др.

В диссертации затрагиваются также наиболее важные аспекты современного этапа развития системы информационной безопасности России, логически связанные с основным содержанием исследования и характеризующие результаты государственной политики в данной сфере в 1991 – 2021 гг.

Источниковая базы исследования. Диссертация базируется на комплексе разнообразных архивных и опубликованных исторических источников.

Архивные документы, использованные в диссертации, отражают предысторию и начальный этап становления государственной политики Российской Федерации в области информационной безопасности. Так, в фонде ЦК КПСС (Ф. 17), хранящемся в составе Российского государственного архива социально-политической истории (РГАСПИ), имеются делопроизводственные документы КПСС (протоколы и стенограммы партийных пленумов и конференций, собраний областных парторганизаций конца 1980-х – начала 1990-х гг.), а также эпистолярные источники, такие, как письма граждан и трудовых коллективов, которые показывают, как воспринималась в обществе политика «гласности», отмена цензуры, появление свободных СМИ, установление информационных контактов с Западом. Данные документы отражают возникшие в условиях российских реформ начала 1990-х гг. расхождения в понимании государственной, в том числе информационной безопасности, представителями различных общественно-политических сил в стране.

Ценный материал по теме диссертационного исследования содержится в документах начала 1990-х гг. из личного фонда Б.Н. Ельцина в Архиве Президента РФ (Ф.6). В рабочих заметках и черновиках выступлений Б.Н. Ельцина на встречах с сотрудниками президентской Администрации по экономическим и политическим вопросам, на совещаниях с руководством российских спецслужб отражен процесс формирования концепций информационной безопасности страны, законодательства о защите государственной тайны и другой конфиденциальной информации, создания и определения функций Совета Безопасности и др.

Комплекс опубликованных источников включает законодательно-нормативные, делопроизводственные документы, публицистику и мемуарную литературу.

В группу нормативно-законодательных актов входят базовые правовые акты Российской Федерации периода 1991 – 2021 гг., регулирующие сферу информационной безопасности: Закон РФ от 21 июля 1993 г. «О государственной тайне**»,** Федеральный закон от 27 июля 2006 «Об информации, информационных технологиях и о защите информации», Федеральный закон от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации» и др.; указы Президента России, постановления и распоряжения Правительства РФ аналогичной направленности; тексты стратегических документов – Концепции национальной безопасности РФ (1997), Доктрин информационной безопасности России 2000 г и 2016 г., Стратегии национальной безопасности РФ (2021) и др.

В источниковую базу исследования входят тематические сборники документов, в том числе издания, посвященные журналистике в постсоветской России, вопросам международной информационной безопасности и др.[35]

Использованные в диссертации делопроизводственные документы наглядно отражают процесс формирования и функционирования системы органов власти и управления России, обеспечивающих реализацию государственной политики в области информационной безопасности. В данной группе представлены стенограммы заседаний Совета безопасности РФ[36], протоколы и резолюции комитета Государственной Думы России по

---

[35] Российская журналистика: свобода доступа к информации / Комиссия по свободе доступа к информации. Сост. И. Дзялошинский. Москва: КСДИ, 1996. 267 с.; История советской политической цензуры. Документы и комментарии / Сост. Горяева Т.М. М.: РОССПЭН, 1997. 672 с.; Международная информационная безопасность: Теория и практика. Т. 2: Сб. док. / Под общ. ред. А.В. Крутских. 2-е изд., доп. М.: Аспект Пресс, 2021. 784 с.

[36] Заседание Совета Безопасности РФ «О противодействии угрозам национальной безопасности в информационной сфере». 1 октября 2014 г. [Электронный ресурс] // Совет безопасности РФ. Официальный сайт. URL: http://www.scrf.gov.ru/council/session/2059/ (Дата обращения: 15.04.2022).

информационной политике[37], приказы и материалы коллегий Минкомсвязи, Банка России и др.[38] Основной массив данных документов находится в составе текущих электронных архивов Государственной Думы РФ, Президента и Правительства России, министерств и ведомств. Ряд законодательных и делопроизводственных материалов по вопросам информационных безопасности опубликован в специализированных периодических изданиях и сборниках документов.

Значительное место в комплексе источников по теме диссертации занимают публицистические документы, которые представлены текстами выступлений, заявлений и интервью Президента России В.В. Путина, Секретаря Совета Безопасности России Н.П. Патрушева, руководителя Службы внешней разведки РФ С.Е. Нарышкина и других официальных лиц[39]; интервью, публикации в СМИ и социальных сетях экспертов в области цифровых технологий, блогеров, руководителей IT-компаний и др.; информационные сообщения об официальных мероприятиях, деловых форумах, конференциях по вопросам информационной безопасности[40].

Важным компонентом источникового комплекса диссертации выступает мемуарная литература, которая позволяет раскрыть позиции ведущих государственных деятелей по ключевым проблемам развития

---

[37] Парламентские слушания «Средства массовой информации в системе информационной безопасности» // Думский вестник. 1996. № 5 (20). С. 90-103 и др.

[38] Заседание коллегии ФСБ России. 24 февраля 2021 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: http://www.kremlin.ru/events/president/news/65068 (Дата обращения: 20.04.2022)

[39] Поздравление Президента России В.В. Путина с Днем работника российских спецслужб 20 декабря 2020 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: http://www.kremlin.ru/events/president/news/64681 (Дата обращения: 18.04.2022); Интервью Секретаря Совета Безопасности Российской Федерации Н.П. Патрушева // Российская газета. Федеральный выпуск. 23 декабря 2015 г. № 6861; *Нарышкин С.Е.* Об обеспечении национальной безопасности и устойчивого социально-экономического развития государств в условиях роста «гибридных» угроз: Выступление на 10-й международной встрече высоких представителей, курирующих вопросы безопасности. Уфа, 18 июня 2019 г. [Электронный ресурс] // МИД России. Официальный сайт. 28 июня 2019 г. URL: https://www.mid.ru/foreign_policy/international_safety/regprla/-/asset_publisher/YCxLFJnKuD1W/content/id/3704728 (Дата обращения: 23.11.2021); и др.

[40] Направления прорыва. Из руин – к информационному обществу // Российская газета. 10 января 1991 г.; Оружие, которое может быть опаснее ядерного // Независимая газета. 18 ноября 1995 г. и др.

страны, связанным с информатизацией и информационной безопасностью в начальный период рыночных реформ[41], охарактеризовать отражение государственной политики информационной безопасности в профессиональной деятельности и повседневной жизни россиян, раскрывает социально-культурный облик и менталитет представителей IT-сообщества, журналистов и других социально-профессиональных групп, вовлеченных в процесс формирования в России информационного общества[42].

В диссертации использованы также материалы справочного характера: перечни нормативных документов, обзоры деятельности государственных учреждений, вузов, IT-компаний, материалы специализированных сайтов по информационным технологиям и системам безопасности и др.

Таким образом, источниковая база диссертации характеризуется высокой степенью репрезентативности, включает все основные виды исторических источников, содержащих широкий круг данных о процессе становления и эволюции государственной политики России в области информационной безопасности, что позволяет осуществить комплексное решение поставленных в диссертации цели и задач.

Методология исследования базируется на теоретических положениях теории модернизации, позволяющей рассматривать общественное развитие в качестве поступательного процесса, сопровождающегося институциональными и системными изменениями всех сторон общества. В рамках указанной теории информационная сфера рассматривается в качестве фактора российской модернизации. Одновременно информационная среда является особой подсистемой общества, отличной от других, но оказывающей существенное влияние на динамику и характер экономических, социально-политических и культурных преобразований. Поскольку сценарии

---

[41] *Ельцин Б.Н.* Президентский марафон: Размышления, воспоминания, впечатления. М.: АСТ, 2000; *Исаков В.Б.* Председатель Совета Республики. Парламентские дневники. 1990-1991. Екатеринбург, 1997; *Нечаев А.* Россия на переломе. Записки первого министра экономики. М.: Русь-Олимп, 2010 и др.

[42] «Это было лучшее время»: каким был интернет в России 90-х [Электронный ресурс] // Lenta.ru. 24 октября 2020 г. URL: https://lenta.ru/articles/2020/10/14/beeline_90e/

вхождения в информационное общество зависят от различных переменных, уровня, характера социально-экономических процессов, геополитических аспектов в исследовании прослеживается не только эволюция политики государства в данной сфере, но и ее «концептуальное наполнение». [43]

Методы исследования. Исследование выполнено на основе общенаучных методов – анализа, синтеза, применения элементов сравнительно-исторического и системного подходов, позволивших рассмотреть государственную политику РФ в области информационной безопасности как целостное явление, проанализировать эволюцию ее структурных компонентов и характеристик во всей их совокупности и взаимосвязях.

Применение *сравнительно-исторического метода* позволяет сравнить качественные ступени и этапы в развитии государственной политики по обеспечению информационной безопасности, определить ее тенденции в течение определенного исторического периода.

Использование *системного подхода* дает возможность рассматривать общество как систему, состоящую из совокупности элементов, связанных между собой в единую целостность. С этой точки зрения категория «информационная безопасность» рассматривается в качестве элемента, подсистемы общественного целого, позволяющего государству влиять на окружающую среду определенным образом с целью защиты важнейших национальных интересов.

Выбор *междисциплинарного подхода* обусловлен свойствами предмета исследования, связью информационных систем с различными классами явлений- социальными процессами, государственным управлением, международными отношениями, каждый из которых в отдельности не может быть осмыслен в парадигме отраслевого подхода классической науки.

---

[43] *Чернова Е.Н.* Информационное общество и модернизация в России//Теория и практика общественного развития.2013.N.12 [Электронный ресурс] URL: https://cyberleninka.ru/article/n/informatsionnoe-obschestvo-i-modernizatsiya-v-rossii. (дата обращения 05.04.2023)

Наряду с применением общенаучных методов в работе применены специальные исторические методы – периодизации, ретроспекции, историко-типологический и др.

Научная новизна диссертационного исследования заключается в следующем:

- впервые в отечественной историографии исследован исторический опыт формирования и реализации государственной политики Российской Федерации в сфере информационной безопасности во всех ее составляющих: правовой, организационной, технологической, финансовой, социокультурной, образовательной;

- раскрыта взаимосвязь политики информационной безопасности с характером социально-экономической модернизации как внутри страны, так и с интеграцией России в глобальные информационные процессы;

-прослежена эволюция концептуальных и правовых основ системы информационной безопасности в России 1991–2021 гг.;

-исследовано влияние реформ на сферу информационной безопасности;

- показано, что представления о информационной безопасности страны стали значимым фактом социального дискурса в социокультурном и деловом пространстве страны;

- прослежен процесс становления и выявлены основные параметры системы подготовки кадров специалистов в области информационной безопасности;

- раскрыты важнейшие направления и формы деятельности институтов информационной безопасности России – Совета Безопасности РФ, специализированных федеральных ведомств, научно-технологических центров и фирм, общественных организаций и др.;

- введен в научный оборот ряд новых исторических источников по проблеме исследования, позволивших глубоко исследовать концептуальные подходы формирования политики информационной безопасности.

Теоретическая значимость исследования заключается в постановке и разработке автором важной проблемы отечественной истории новейшего времени, не получившей ранее комплексного освещения в научной литературе, в исследовании факторов формирования концепции развития государственной политики Российской Федерации в области информационной безопасности в 1991 – 2021 гг.

В работе обобщен и проанализирован большой объем фактического материала, представляющего информационную ценность для специалистов в области отечественной истории новейшего времени. Диссертация вносит вклад в историю российских модернизаций конца XX – начала XXI вв., раскрывая один из существенных аспектов перехода страны на современный уровень информационно-технологического развития.

Практическая значимость исследования. Результаты проведенного исследования могут быть использованы в процессе подготовки государственных федеральных и региональных программ обеспечения информационной безопасности, совершенствования систем зашиты корпоративных и персональных данных. Полученные результаты могут найти применение при разработке лекционных курсов и практических занятий по проблемам обеспечения информационной безопасности, государственного управления, а также подготовке курсов по проблемам информационных войн.

Положения, выносимые на защиту:

1. Государственная политика Российской Федерации в области информационной безопасности в 1991 – 2021 гг. развивалась как неотъемлемая составляющая модернизации системы государственного управления, экономики и социальной сферы.

2. Начальный период реформ в России 1990-х гг. ознаменовался демократизацией информационного пространства страны, становлением независимых СМИ и активным вхождением российского общества и бизнеса в систему международных информационных коммуникаций, что создавало

как новые риски (военно-политического, коммерческого, социального характера), так и новые технологические возможности в сфере обеспечения защиты информации. Приоритетами в сфере информационной безопасности в эти годы было обеспечение коммерческой тайны, корпоративной и частной конфиденциальной информации.

3. В рамках укрепления современной российской государственности осуществляется нормативно-правовое и институциональное строительство системы обеспечения информационной безопасности, включающей Совет Безопасности РФ, ФСБ России, Федеральную службу по техническому и экспортному контролю (ФСТЭК) и ряд других специальных структур. Обновляется законодательство о государственной тайне, развиваются новые направления нормативного регулирования.

4. В 2010-е гг. происходит обновление концептуальных подходов к обеспечению информационной безопасности как одного из приоритетных направлений национальной безопасности Российской Федерации в контексте геополитических трансформаций XXI в. На данной основе осуществляется дальнейшая модернизация правовой базы государственной политики в сфере информатизации и информационной безопасности, приняты меры организационного и технологического обеспечения защиты критической информационной инфраструктуры (КИИ) государственной власти и управления, промышленности, коммуникационных систем, российского общества в целом.

5. На протяжении всего рассматриваемого периода магистральным направлением развития государственной политики РФ в области информационной безопасности являлось обеспечение баланса между двумя в равной мере необходимыми компонентами современного информационного общества – правом граждан и СМИ на свободный доступ к информации и необходимостью ограничения доступа к определенным видам данных в интересах национальной безопасности России, борьбы с

киберпреступностью, защиты детей и молодежи от деструктивных явлений в Интернете и др.

6. Создание концепций и механизмов государственной политики России в области информационной безопасности в 1991 – 2021 гг. происходило при непосредственном участии ведущих отечественных специалистов в области цифровых технологий, криптографии и других направлений защиты информации, которые являлись представителями российских спецслужб, крупных IT-компаний (Лаборатория Касперского и др.), НИИ, университетов и ведомственных вузов. Процесс формирования и реализации государственной политики России в области информационной безопасности тем самым явился одним из стимулов развития в стране высоких технологий, инновационных направлений бизнеса, науки и образования.

Соответствие паспорту специальности. Диссертация соответствует специальности 5.6.1. Отечественная история, поскольку предпринятое в работе изучение государственной политики Российской Федерации в области информационной безопасности в 1991 – 2021 гг. является компонентом тематического направления в рамках данной специальности «История взаимоотношений власти и общества, государственных органов и общественных институтов России и ее регионов», а также непосредственно затрагивает такие разделы специальности 5.6.1. Отечественная история как «Предпосылки формирования, основные этапы и особенности развития российской государственности» и «Исторический опыт российских реформ» за период XX – XXI вв.

Достоверность и научная обоснованность результатов диссертационного исследования и аргументированность выводов обусловлена репрезентативностью источниковой базы, привлечением информативного комплекса исторических источников, включая впервые введенные в научный оборот в контексте поставленной проблемы архивные документы, применением современных исследовательских методик,

соблюдением научных принципов и использованием комплекса методов исторического исследования.

Апробация результатов исследования. Основные результаты и выводы диссертации отражены в 7 публикациях автора, в том числе три статьи выпущены в научных изданиях, в которых должны быть опубликованы основные результаты исследований в рамках диссертаций, представляемых к защите в диссертационных советах РУДН. Ряд положений диссертации был апробирован в ходе Международной научной конференции HNRI «National development» (Санкт-Петербург, 27–31 октября 2018 г.), Трудах VII Всероссийской научной конференции, с приглашением зарубежных ученых (Уфа, Уфимский государственный авиационный технический университет, 28-30 мая 2019г.), Всероссийской научной конференции с международным участием «V Валеевские чтения», посвященной 80-летию со дня рождения доктора философских наук, члена-корреспондента Академии наук Республики Башкортостан Д.Ж. Валеева (Уфа, Башкирский государственный университет, 24 апреля 2020 г.).

Структура диссертационного исследования. Диссертация состоит из введения, трех глав, заключения, списка использованных источников и литературы.

ГЛАВА I. ЭВОЛЮЦИЯ КОНЦЕПТУАЛЬНЫХ ОСНОВ И ПРАВОВОЙ БАЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ В 1991 – 2021 гг.

1.1. Исторический опыт создания и деятельности системы информационной безопасности в СССР

Особенности формирования государственной политики постсоветской России в сфере информационной безопасности были в значительной мере предопределены событиями и тенденциями предшествующего периода, которые можно разделить на три основных группы: политико-идеологические, правовые и технологические.

В СССР система государственной информационной безопасности складывалась, во-первых, из институтов и мер защиты государственной тайны, подход к которой был в целом обусловлен объективными задачами обеспечения обороноспособности и экономической независимости страны; во-вторых, определялась спецификой советской информационной политики, то есть предусматривала наличие тотального идеологического контроля и цензуры. Так, секретными являлись данные, овладение которыми могло быть использовано в целях ослабления военной или экономической мощи СССР, в том числе информация о функционировании военно-промышленного комплекса и связанных с ним научно-исследовательских учреждений, технологических оборонных системах, численности и дислокации советских войск, освоении космоса, о месторождениях полезных ископаемых и т.п.

Следует отметить, что определенное ограничение доступа в публичное пространство информации, связанной с военными технологиями, с работой спецслужб, функционированием промышленных объектов, обладающих стратегической значимостью, а также потенциальной опасностью для окружающей среды (атомные станции, химические заводы и т.п.), является неотъемлемой частью обеспечения безопасности любого государства. (Необходимость информационной защиты жизненно важной общественной

инфраструктуры наглядно проявилась во всем мире в 2000-е гг., когда возникла глобальная угроза международного терроризма).

Как отмечает доктор юридических наук М.В. Зеленов, характер существования категории государственной тайны в Советском Союзе не имел принципиальных отличий от практики других государств[44]. Специфика отражения правового режима тайны в советском законодательстве и практике заключалась, главным образом, в отсутствии ряда норм, свойственных государствам с рыночной экономикой (коммерческая тайна)[45]. Кроме того, помимо государственной тайны (частью которой являлась военная тайна) в СССР фактически существовала также партийная тайна, охранявшая информационную безопасность КПСС как надгосударственного института власти. При этом законов, регулирующих область государственной тайны, в СССР не было. В данной сфере применялись подзаконные акты, в большинстве своем носившие закрытый характер[46].

Еще в довоенный период в СССР была разработана система защиты государственной информационной безопасности, построенная на разработке и периодическом обновлении «Перечней» сведений, которые представляли собой военную и государственную тайну. (Модернизированная в соответствии с нормами правовой государственности данная система применяется и в настоящее время). В 1920 – 1980-е гг. базовый «Перечень», действовавший в тот или иной период времени, утверждался Советом министров СССР. Кроме того, министерства и государственные комитеты СССР и РСФСР формировали собственные перечни, которые определяли круг ведомственных сведений, предназначавшихся для служебного пользования, и согласовывались со специальным органом исполнительной

---

[44] *Зеленов М.В.* Военная и государственная тайна в РСФСР и СССР и их правовое обеспечение (1917 – 1991 гг.) // Ленинградский юридический журнал. 2012. Вып. 1. С. 144.
[45] См.: *Фатьянов А.А.* Тайна как социальное и правовое явление. Ее виды // Государство и право. 1998. № 6. С.5-14.
[46] *Вус М.А., Макаров О.С.* Четверть века законодательного регулирования института государственной тайны на постсоветском пространстве // Новый юридический вестник. 2017. № 2 (2). С. 1.

власти, обеспечивавшим контроль информационного пространства Советского Союза – Главным управлением по охране государственных тайн в печати при Совмине СССР (Главлит СССР)[47].

В период конца 1980-х – начала 1990-х гг. вопросы защиты государственной тайны в СССР регулировались решениями органов исполнительной власти. В том числе были утверждены «Перечень сведений, запрещенных к опубликованию в открытой печати, передачах по радио и телевидению» (1987) и «Перечень сведений, запрещенных к опубликованию» (1990), которые дополнялись рядом уточняющих указаний Главлита[48].

В условиях «холодной войны» государственная политика СССР в сфере информационной безопасности включала противодействие иностранным спецслужбам в сфере защиты внутренней информации научно-технологического и производственного характера. В послевоенные десятилетия соревнование СССР и Запада в сфере информационных технологий происходило по линии развития криптографии[49], радиосвязи, в том числе цифровых радиорелейных систем в 1970-е – 1980-е гг.[50], гидроакустики[51], радиолокации и оптико-электронных устройств в рамках воздушно-космической разведки[52] и др. Соответственно, обеспечение информационной безопасности предполагало максимальную защиту

---

[47] *Батурин Ю.М.* Феноменология юридического чуда / Под ред Федотова М.А. М.: РОССПЭН, 2012. С.5-7; *Зеленов М.В.* Военная и государственная тайна в РСФСР и СССР. С. 144-155.

[48] *Зеленов М.В.* Военная и государственная тайна в РСФСР и СССР. С. 155.

[49] *Бабаш А.В., Баранова Е.К., Ларин Д.А.* Информационная безопасность. История защиты информации в России. М.: Изд. центр ЕАОИ, 2012. С. 688-733.

[50] *Миркин В.В.* Эволюция отечественных систем радиорелейной связи // Вестник Томского государственного университета. Серия: История. 2013. № 372. С.123-125.

[51] *Бабкин С.Г.* Развитие систем звукоподводной связи в России / С.Г. Бабкин, В.А. Попов, И.А. Селезнев // Прикладные технологии гидроакустики и гидрофизики: сб. трудов Всероссийской конференции. М.: Институт океанологии им. П.П. Ширшова РАН, 2016. С. 45-47.

[52] *Kalic Sean N.* (2012) US Presidents and the Militarization of Space, 1946 – 1967, College Station, TX: Texas A&M University Press; Маилян П.Г. США и СССР: военное использование космического пространства в 1957–1983 годы // Известия вузов. Северо-Кавказский регион. Серия: Общественные науки. 2012. № 5 (170). С. 41-45; Космические разведчики. Советские и российские спутники – шпионы // Военное обозрение. 8 января 2014 г.

внутреннего пространства СССР от угроз со стороны иностранной агентуры и новейших разведывательных технологий[53]. На практике это находило выражение в создании закрытых территорий, и отдельных закрытых (секретных) заводов, НИИ и конструкторских бюро (на советском сленге именовавшихся «почтовыми ящиками» или просто «ящиками»), в запрете выезда их сотрудников за границу и обязательном контроле контактов с иностранцами на территории СССР, в агентурной работе советских спецслужб. С другой стороны, органами госбезопасности СССР предпринимались действия по выявлению технологических достижений противника в области развития информационных технологий, создания систем противодействия им и собственных технологических разработок[54]. Данные функции осуществлялись такими структурами как Первое главное управление (ПГУ) КГБ СССР и Главное разведывательное управление (ГРУ) Министерства обороны СССР.

Создание закрытых административно-территориальных образований (ЗАТО), которое связывается исследователями с началом советского атомного проекта, вплоть до начала 1990-х гг. осуществлялось в режиме строгой секретности и регулировалось секретными нормативными документами высших партийных и государственных органов. В настоящее время некоторые из этих документов упоминаются и цитируются в публикациях, посвященных истории отечественной науки и технологий[55]. ЗАТО строились вблизи промышленных городов с соответствующими

---

[53] Разведка США в действии. Шпионаж, тайные операции, саботаж: Сборник материалов американской печати: Пер. с англ. М.: Прогресс, 1988.

[54] См.: *Вартанесян В.А.* Радиоэлектронная разведка М.: Воениздат, 1975; *Игнатенко Ю.М., Кикнадзе В.Г* На страже радиоэфира // Военно-исторический журнал. 2007. № 9. С. 31-35; Безопасность государства и развитие науки, техники, промышленности России (СССР) во второй половине XX в.: вопросы истории и политики / *А.В. Лосик, В.Н. Скворцов, А.М. Судариков, А.Н. Щерба*, под ред. В.Н. Скворцова. Санкт-Петербург: Изд-во Ленинградского государственного университета (ЛГУ) им. А.С. Пушкина, и др.

[55] *Киселев Г.В., Русковец Н.А.* Краткий очерк создания синхроциклотрона Гидротехнической лаборатории АН СССР (ЛЯП ОИЯИ) и итоги первого этапа физических исследований. Обзор архивных документов // Физика элементарных частиц и атомного ядра (ЭЧАЯ). 2012. Т. 43. Вып. 4. С. 861-864.

дублирующими названиями («Арзамас-16», «Красноярск-26», «Свердловск-45», «Челябинск-70», и др.). Часть из них была привязана к Москве, Новосибирску и другим крупным научно-образовательных центрам. При этом местонахождение закрытых поселений не обозначалось на советских географических картах общего пользования, информация о них не размещалась на транспортных указателях, упоминания об этих объектах нельзя было обнаружить в справочной и иной литературе и документах, не имевших грифа «секретно»[56]. Информация о внутренней повседневной жизни ЗАТО подвергалась легендированию, позволявшему проживавшим там лицам сохранять режим секретности во время отпуска, общения с родственниками и знакомыми за пределами закрытых поселений; практиковались различные приемы размывания информации, например, номера маршрутов городского транспорта продолжали уже действующие в областных центрах, к которым были приписаны ЗАТО[57]. Доступ на территорию ЗАТО разрешался только при наличии соответствующих пропусков и разрешений, подъездные пути были перекрыты контрольно-пропускными пунктами. В СССР было также создано большое количество наукоградов[58] с менее высоким уровнем секретности – Обнинск, Дубна, Жуковский, Королев, Зеленоград, Краснообск и др., которые были закрыты для посещения иностранцами. На их территории располагались предприятия и организации, никогда не упоминавшиеся в открытой печати[59].

ЗАТО и научные городки в 1960 – 1980-е гг. характеризовались автономностью технологических систем, высоким уровнем комфортности городского пространства, наличием социальных преимуществ, таких, как

---

[56] *Нарыков Д.Н.* Исторический аспект создания в России закрытых административно-территориальных образований // Мир науки, культуры, образования. 2012. № 1 (32). С. 247.

[57] Закрытые города СССР (ЗАТО) и их судьба в РФ [Электронный ресурс]. URL: https://leon-rumata.livejournal.com/3868057.html (Дата обращения: 25.11.2021)

[58] Считается, что термин «наукоград» был введен в оборот в 1991 г. С.П. Никаноровым и Н.К. Никитиной (г. Жуковский Московской области) при создании общественного движения «Союз развития наукоградов»

[59] Наукограды. История развития [Электронный ресурс] // Сайт Союза развития наукоградов. URL: https://naukograds.ru/ (Дата обращения: 20.11.2021)

надбавки к заработной плате, лучшее, чем на основной территории страны, снабжение продуктами питания и товарами повседневного спроса[60]. Преимущества жизни и работы в ЗАТО и наукоградах сохранялись до конца 1980-х гг., когда финансово-экономический кризис в СССР оказал негативное влияние на состояние всей бюджетной сферы, включая научно-исследовательские и научно-производственные центры[61]. Соответственно, работники секретных предприятий, сотрудники закрытых НИИ и конструкторских бюро имели высокий социальный статус и были заинтересованы в его сохранении, одним из условий которого была работа в режиме секретности.

Самостоятельную роль в системе информационной безопасности СССР в сфере обеспечения военной тайны, а также в деятельности внешнеполитических ведомств и разведывательных спецслужб, играли технологии криптографии или шифрования (дешифровки) информации, которые разрабатывались специальными подразделениями. В структуре Вооруженных Сил СССР шифровальная служба с 1941 г. была возложена на Восьмое управление Генерального штаба, действующее под этим наименованием и в настоящее время. Аналогичное Восьмое управление было создано в КГБ СССР. Кроме того, шифровальные службы существовали в МИД СССР и ряде других ведомств, а также в ЦК КПСС (4-й сектор Общего отдела)[62]. Огромный опыт криптографической работы был накоплен армейскими шифровальными службами СССР в годы Великой Отечественной войны. В послевоенные десятилетия в процессе противостояния Организации Варшавского договора и НАТО происходило дальнейшее совершенствование советских технологий криптоанализа,

---

[60] *Лысая Д.А.* Наукограды России: история развития от научных поселений до инновационного центра «Сколково» // Architecture and Modern Information Technologies. 2017. №3(40). С. 178-199 [Электронный ресурс] URL: https://marhi.ru/AMIT/2017/3kvart17/14 Nsaia/indexphp (Дата обращения: 20.11.2021)

[61] Там же.

[62] Шифровальная служба СССР/России в годы войны и послевоенный период [Электронный ресурс] // Призма. Армия и ВПК. URL: https://prizmablog.ru/shifrsluzhba-sssr-rossii-ch2/ (Дата обращения: 12.11.2021)

включая электронные методы, а также разведывательные операции по добыванию иностранных шифров и криптографических устройств[63]. Все криптографические материалы советских спецслужб подлежали строгой секретности, в том числе не передавались союзникам по социалистическому лагерю[64].

В системе Вооруженных Сил СССР действовал ряд структур (органов военной цензуры), деятельность которых была направлена на защиту военной тайны, включая материалы СМИ, содержащие информацию о вооружениях, армейских подразделениях и т.п., документооборот между военным и гражданскими ведомствами, личную переписку военнослужащих[65]. Данные функции выполнялись Управлением военной цензуры Генштаба Вооруженных Сил Советского Союза, которое в 1990 г. было преобразовано в отдел, занимавшийся контролем публикаций в СМИ, связанных с оборонной и военно-технической тематикой.

В СССР вплоть до 1990 г. охрана государственной тайны была неотделима от политической цензуры, являвшейся по институциональным параметрам и тотальности охвата всех сфер жизни советского общества и государства, ключевым компонентом системы информационной безопасности[66]. Данное явление определялось представлениями власти о необходимости жесткого ограничения любой информации, противоречащей господствующей идеологической доктрине, либо раскрывающей системные недостатки и проблемы советского строя. Высокая степень секретности окружала информацию о внутреннем пространстве и деятельности партийно-политической элиты СССР, за исключением фасадных официальных

---

[63] Шифровальные машины СССР 1931-1991 гг. (Обзор) [Электронный ресурс] // Призма. Армия и ВПК. URL: https://prizmablog.ru/shifrovalnye-mashiny-sssr-1931-1991-gg-obzor/; Криптология в Холодной войне // Там же. URL: https://prizmablog.ru/kriptologiya-v-holodnoj-vojne/ (Дата обращения: 12.11.2021)

[64] Там же.

[65] *Смыкалин А.С.* Перлюстрация почтовой корреспонденции и почтовая военная цензура в России и СССР. М.: Русайнс, 2015. С. 130.

[66] История советской политической цензуры. Документы и комментарии / Сост. Горяева Т.М. М.: РОССПЭН, 1997. 672 с.

мероприятий и документов. Фактически советская система информационной безопасности государства включала подсистему по информационной защите КПСС и ее институтов. В то же время, цензура действовала в целях предотвращения попадания в открытые источники сведений, представляющих интерес для агентуры стран НАТО и других иностранных государств для сбора разведывательной информации. В интервью М.С. Горбачева 4 февраля 1986 г. французской газете «Юманите», получившем широкий международный резонанс, в том числе в связи с тем, что в нем впервые официально признавалось наличие в СССР цензуры, советский лидер подчеркивал, что информационный контроль обусловлен, прежде всего, задачами защиты государственной и военной тайны[67].

Цензурная функция выполнялась Главлитом СССР и системой подведомственных ему региональных управлений и уполномоченных. Инфраструктура Главлита обладала огромным штатом, позволявшим осуществлять надзор над процессом создания, выпуска печатной продукции в СССР и распространения ее за рубежом, контролировать информационные материалы, поступавшие в страну из-за границы. При отсутствии массового Интернета и независимых СМИ техническая сторона ограничения внешних информационных потоков на территорию СССР была довольно проста, обеспечиваясь работой таможенных служб и цензурой личной переписки определенных лиц[68], а также глушением западных радиостанций «Голос Америки», радио «Свобода» и др.

В системе государственных архивов и библиотек существовала система «спецхранов», в которые включались документы и печатные издания ограниченного и полностью закрытого доступа[69]. Поскольку цензура

---

[67] *Горбачев М.С.* Ответы на вопросы газеты «Юманите» 4 февраля 1986 г. М.: Политиздат, 1986. 31 с.

[68] *Миркин В.В.* Средства связи как инструмент политической цензуры в СССР (1970-е - начало 1980-х гг.) // Вестник Томского государственного университета. Серия: История. 2018. № 59. С.53-59.

[69] *Пашнина Т.В.* Реализация права на информацию в деятельности библиотек // Право и информация: вопросы теории и практики: Сборник материалов Международной научно-

опиралась, прежде всего, на идеологические критерии, можно говорить о том, что в СССР обеспечение общественной информационной безопасности фактически приравнивалось к формированию однородной политико-идеологической среды. Такая среда создавалась путем ограничения одних категорий информации и распространении других. При этом образ советской страны, созданный в пропагандистских документах партии и правительства, прессе, литературе и кино, довольно существенно отличался от реалий повседневной жизни советских людей, то есть с помощью искаженной или особым образом подававшейся информации формировалась иллюзорная реальность, которую сегодня можно было бы назвать виртуальной. Тем самым системы цензуры и пропаганды дополняли друг друга, опираясь на поддержку всех инфраструктур государства и общества – системы учреждений науки и образования, средств массовой информации, правоохранительных органов[70].

Идеологическая составляющая информационной безопасности в СССР охватывала все сферы жизни и деятельности общества, в том числе распространялась на задачи обеспечения безопасности ВПК, энергетики, транспорта, связи и других технологических систем[71]. Общим для промышленно-технологической и гуманитарной областей, находившихся в орбите государственного информационного контроля, был механизм обеспечения безопасности в форме уровней допуска к секретной информации. Базовым, но не единственным условием допуска к государственной тайне в сфере деятельности спецслужб и других государственных институтов, высшего партийного аппарата, науки и технологий, допуска к архивным спецхранам, идеологически опасным

практической конференции. СПб, 18 марта 2019 г. / Под ред. Н.А. Шевелевой. СПб: Президентская библиотека им. Б.Н. Ельцина, 2020. Вып. 9. С. 173-174.

[70] *Почепцов Г.* Пропаганда: советская и несоветская [Электронный ресурс] URL: https://osvita.mediasapiens.ua/trends/1411978127/propaganda_sovetskaya_i_nesovetskaya/ (Дата обращения: 21.11.2021)

[71] *Миркин В.В.* Средства связи как инструмент политической цензуры в СССР (1970-е – начало 1980-х гг.) // Вестник Томского государственного университета. Серия: История. 2019. № 59. С. 53-58.

(«вредным») иностранным информационным ресурсам являлось членство в КПСС, дополнявшееся системой специальных правил и инструкций по допуску к различным категориям секретной информации. Исключения из этого правила делались для особо значимых деятелей советской науки и техники, так, например, известно, что категорически отказывался вступать в партию выдающийся авиаконструктор А.Н. Туполев[72]. Границы секретности являлись размытыми в архивном деле, несмотря на периодическое обновление правил хранения, учета и использования документов ограниченного доступа; в результате в архивной системе СССР, в том числе в партийных архивах, практиковался дифференцированный подход к данному вопросу, выражавшийся в отказе или, напротив, разрешении доступа к закрытой информации в зависимости от статуса того или иного исследователя и личной позиции администрации конкретного архивного учреждения[73].

С формальной точки зрения эффективность идеологического компонента информационной безопасности в рамках государственно-политической системы СССР была достаточно высокой. Политическая цензура охватывала всю сферу информации, распространявшейся через советскую прессу, телевидение и радио, книги любой тематики и жанров, контролировала кинематограф, театр, тексты эстрадных песен, программы массовых мероприятий. Минимизировалось соприкосновение советских граждан с иностранными информационными источниками; этой цели служило, в частности, ограничение служебных и туристических поездок за рубеж. Обязательным было участие партийных органов по месту работы или учебы в оформлении выездов за границу, включая социалистические страны (что нашло, в частности, отражение в известной песне Владимира Высоцкого). В задачу цензуры входила защита советского общества от вредоносных влияний западной идеологии и культуры и одновременно

[72] *Бодрихин Н.Г.* Туполев. М.: Молодая гвардия, 2011. С.3.
[73] *Павлова Т.Ф.* Доступ к архивным документам спецхранов в начале 1960-х – середине 1980-х гг. // Отечественные архивы. 2014. № 3. С. 13-26.

контроль информационной ситуации в стране. Отдельным, наиболее интенсивно осуществлявшимся направлением борьбы властей за информационную «чистоту» советского общественного пространства являлось преследование диссидентов и правозащитников и ограничение политической и религиозной эмиграции из СССР, сочетавшееся в то же время с максимальным замалчиванием данных явлений[74].

С другой стороны, официальное и личное, а также корпоративное информационное пространство в СССР 1970 – 1980-х гг. существенно отличались друг от друга. В среде советской интеллигенции процветало вольнодумство, пользовались популярностью передачи западных радиостанций и т.п.[75] Данное явление наблюдалось, в том числе и среди «проверенных товарищей», работавших в секретных НИИ, что могло создавать реальные проблемы в сфере информационной безопасности в случае передачи за границу секретных технологий и других данных, составлявших государственную тайну. В целом, в период позднего СССР идеологическое давление системы вызывало обратную реакцию советской молодежи и интеллектуальных кругов общества – происходило отторжение от коммунистической идеологии и идеализация Западного мира. (Эта тенденция, как будет показано далее, не всегда благоприятно сказывалась в 1990-е гг. на обеспечении задач информационной безопасности российского ВПК и других стратегических отраслей).

Формирование теоретических и правовых основ государственной политики России в сфере информационной безопасности во многом связано с феноменом информационного общества, которое к началу 1980-х гг. становится реальным фактором мировой политики и экономики[76]. При этом для российского интеллектуального социума на рубеже 1980-х – 1990-х гг.

---

[74] *Козлов В.А., Мироненко С.В., Эдельман О.В., Завадская Э.Ю.* Крамола. Инакомыслие в СССР при Хрущеве и Брежневе. 1953-1982 гг. М.: Материк, 2005. 432 с.

[75] *Безбородов А.Б., Мейер М.М., Пивовар Е.И.* Материалы по истории диссидентского и правозащитного движения в СССР 50-х – 80-х годов. М., 1995. 151 с.

[76] *Бойченко А.В.* Причины возникновения и особенности информационного общества // Ученые записки ИСГЭ. 2016. Т.14. № 1. С. 87-92.

концепт информационного общества имел собственный смысл, определявшийся, прежде всего, постепенным распадом советской идеологической «матрицы» и начавшейся интеграцией страны в мировое информационное поле, и, лишь во вторую очередь – растущим значением цифровых технологий в системе глобальных коммуникаций и постиндустриальной экономике будущего. Следует отметить, что концепции информационного общества, выдвигавшиеся на Западе, до перестройки подвергались в СССР критике и «разоблачению» как образцы буржуазного мировоззрения. Открытость и свободный обмен информацией, идеями и знаниями, свойственный информационному обществу, находились в очевидном противоречии с советской информационной политикой как представлявшие потенциальную идеологическую опасность и не поддающиеся тотальному контролю.

В 1986 – 1991 гг. происходит размывание идеологической основы и постепенный демонтаж институтов описанной выше системы общественной информационной безопасности СССР. С объявлением на XXVII съезде КПСС политики «гласности» и последовавшей через несколько лет отменой цензуры большинство исследователей перестроечной эпохи связывают начало становления в России информационного общества в социологическом и культурологическом понимании. Тогда же в интеллектуальное пространство СССР приходит наследие американских и европейских теоретиков информационного общества 1950-х – 1960-х гг. и новейшие доктрины западных ученых, значительное место в которых занимает осмысление информационных технологий в настоящем и будущем человечества[77]. Так, в 1986 г. издательством «Прогресс» был выпушен в свет сборник «Новая технократическая волна на Западе», в который вошли труды классиков мировой философской мысли XX в. М. Хайдеггера и К. Ясперса, а также работы Ж. Эллюля, Д. Белла, Т. Стоуньера и других ведущих

[77] *Балашова М.А.* Информационное общество: теоретическая база и российская практика // Известия Иркутской государственной экономической академии. 2013. № 5. С. 5-12.

философов и социологов, посвященные теориям «новой технократической волны»[78]. Одному из разделов книги составители дали название «Информационное общество – компьютерная революция», раскрывающее непосредственную связь новой информационной реальности с развитием цифровых технологий.

Необходимо отметить, что важным аспектом предыстории российской государственной политики информационной безопасности является компьютеризация СССР, обеспечившая технологическую платформу для последующей интеграции Российской Федерации в мировое информационное пространство и для формирования внутренней сетевой среды с соответствующими новыми возможностями и проблемами в сфере информационной безопасности[79].

Однако в 1980-х гг. электронно-вычислительная техника и информатика (русский перевод термина computer science) не ассоциировались с вопросами информационной безопасности; речь могла идти только о секретности каких-либо конкретных разработок для армии или спецслужб, предполагающих применение цифровых технологий. В этот период СССР активно осваивалось производство ЭВМ, включая персональные компьютеры, которые создавались на основе западных образцов (Apple) и отечественных оригинальных разработок. При этом в советской прессе не только велась пропагандистская кампания в пользу компьютерной грамотности, но и публиковались в массовой научно-технической печати инструкции по сборке ПК. С 1 сентября 1985 г. в школьные программы был включен предмет «Основы информатики и вычислительной техники» в целях внедрения новой информационной культуры в образ жизни и трудовую деятельность молодых поколений[80].

---

[78] Новая технократическая волна на Западе / отв. ред. П.С. Гуревич. М.: Прогресс, 1986. 453 с.

[79] *Prokhorov S.P.* Computers in Russia: Science, Education, and Industry IEEE Annals of the History of Computing, vol. 21, №. 3, Jul-Sept, 1999.

[80] *Ершов А.П.* Информатизация: от компьютерной грамотности учащихся к информационной культуре общества // Коммунист, М.: 1988. № 2. С.82-92.

Во второй половине 1980-х гг. происходит обновление институтов государственного регулирования информационно-технологической сферы, в том числе был создан Госкомитет СССР по вычислительной технике и информатике, в распоряжение которого передавался ряд научно-исследовательских и научно-производственных организаций (ВНИИ прикладных автоматизированных систем, Всесоюзное объединение «СоюзЭВМкомплекс» и др.)[81]. Данная программа соответствовала проводившейся в этот период научно-технической политике СССР, направленной на преодоление технологического отставания от Запада. Производство ЭВМ, внедрение цифровых технологий в сферу академических исследований и деятельность научно-производственных центров выдвигается в числе ключевых задач ускорения развития советского машиностроения и других отраслей промышленности[82]. Фундаментальные исследования в области вычислительной техники и информатики вели и координировали четыре академических института: Институт проблем информатики АН СССР (ведавший разработкой персональных ЭВМ), Институт кибернетики имени В.М. Глушкова АН Украинской ССР, Институт микроэлектроники АН СССР и Институт проблем технологии микроэлектроники и особо чистых материалов АН СССР[83].

На фоне разрастания кризиса директивной экономики и сокращения финансирования академической науки процесс развития в СССР компьютерных технологий и цифровизации производства также начинает замедляться. Кроме того, развитие компьютерных средств передачи информации становится в этот период проблемой для идеологического аппарата и цензурных органов СССР, столкнувшихся со своим технологическим отставанием от Запада. В одной из публикаций Т.М. Горяевой приводится текст письма руководства Главлита в ЦК КПСС от

---

[81] Право и информационное общество: Сборник научных трудов / Отв. ред. Бачило И.Л. Москва: ИНИОН РАН, 2002. С.234.

[82] См. Борьба КПСС за ускорение научно-технического прогресса в период зрелого социализма. Л., 1984.

[83] Там же.

16 декабря 1988 г. с просьбой о модернизации материально-технической базы своей спецслужбы, которая не выдерживает конкуренции с западными информационными агентствами, имеющими возможность использовать высокоскоростные компьютеры, факсы и другие современные средства коммуникации[84].

В то же время сборка и обслуживание компьютеров приобретают популярность в теневом и формирующемся легальном частном секторе, а в конце 1980-х – начале 1990-х гг. все больше компьютерной техники ввозится из-за рубежа, складываются основы рынка цифровых технологий. В этой сфере работают многие кооперативы и совместные предприятия переходных и первых рыночных лет. Увлечение программированием, компьютерными играми и другими аспектами цифровой информатизации распространяется среди технической интеллигенции и студенчества[85]. В настоящее время в Интернете представлен ряд публикаций о компьютеризации в позднем СССР, авторы которых, в частности, сообщают, что из рассказов знакомых, которые жили в СССР в 1985–1991 гг., можно сделать вывод, что в среде московской научно-технической интеллигенции компьютеры перестали восприниматься как «что-то сверхъестественное», постепенно становясь обыденным явлением[86].

Событием в отечественной научной мысли тех лет стала публикация в 1989 г. работы А.И. Ракитова, одного из первых отечественных теоретиков информационно-технологического подхода к феномену информационного общества, посвященной особенностям информатизации России[87]. С 1989 г. начал издаваться «Вестник Российского общества информатики и

---

[84] *Горяева Т.М.* Политическая цензура в период стагнации и кризиса власти и идеологии в СССР (1969–1991 гг.) // Политическая цензура в СССР. 1917-1991. М.: РОССПЭН, 2009

[85] [Глезин Е.Д.] Компьютеризация эпохи освободительной Перестройки Горбачева [Электронный ресурс] URL: https://ed-glezin.livejournal.com/1099683.html (Дата обращения: 15.11.2021)

[86] Как в СССР продвигали компьютерную грамотность. Микроша и Агат [Электронный ресурс] URL: https://zxdemos.ru/viewtopic.php?id=10997 (Дата обращения: 15.11.2021)

[87] Теория и практика общественно-научной информации. М.: ИНИОН, 1989. С.31-52.

вычислительной техники» (в настоящее время журнал «Информационное общество»).

Идеология гласности и нового политического мышления периода горбачевской перестройки затрагивали те базовые составляющие информационной безопасности СССР, которые были связаны с цензурными идеологическими ограничениями. Растущая политизация советского общества конца 1980-х – начала 1990-х гг., проявляется и в различных подходах к трансформации общественного информационного пространства. Это явления непосредственно воздействует и на внутреннюю жизнь КПСС и ВЛКСМ, часть состава которых стремится адаптироваться к деятельности в условиях информационной открытости и плюрализма[88]. Данная тенденция проявляется, в частности, в снижении влияния ведущих партийных СМИ, прежде всего, газеты «Правда», главный редактор которой был освистан делегатами XXI съезда ВЛКСМ при попытке разъяснить его участникам смысл известного Открытого письма ЦК КПСС «За консолидацию на принципиальной основе»[89].

Значительная часть партийно-хозяйственной элиты СССР была недовольна и обеспокоена достаточно радикальным реформированием системы государственно-общественных отношений в конце 1980-х гг. – внедрением многопартийности и появлением на страницах газет и журналов, на радио и телевидении лидеров альтернативных политических движений, резко критиковавших компартию, ее идеологию и деятельность. Представители данной социальной группы были ошеломлены тем, что во всех средствах массовой информации, на митингах и собраниях на них обрушивался поток критики и обличений. Стихийные проявления свободы слова в СМИ и во время общественных мероприятий воспринимались

---

[88] *Волгин Е.И.* Проблема модернизации КПСС в преломлении внутрипартийного дискурса (начало 1990-х гг.) // Вестник Московского университета. Серия 12: Политические науки. 2008. № 2. С. 36-45.

[89] РГАСПИ. Ф. 17. Оп. 159. Д. 90 Л. 61.

партийными функционерами как вседозволенность и анархия[90]. Пресса, стремившаяся к объективному изложению событий, в свою очередь подвергавшаяся критике сторонников идеологической цензуры, в том числе вышестоящих партийных органов, в новых условиях, как правило, уже не сдавала свои позиции. Делегата Башкирской областной партийной конференции 25 апреля 1990 г. редактор газеты «Вечерняя Уфа», комментируя недовольство партийных функционеров критическими публикациями в прессе, сказал: «Это и будет так»[91].

Данное явление воспринималось противниками реформ как угроза безопасности страны. Следует отметить, что эта обеспокоенность подтверждалась возникновением в этот период очагов нестабильности – в Нагорном Карабахе, в Средней Азии, Прибалтике, ряде регионов РСФСР где катализатором межэтнических и социальных конфликтов нередко становились различные слухи, провокационные заявления лидеров радикальных групп, излишне резкие высказывания в прессе и т.п.[92] При этом советские журналисты, ученые, работники вузов, учреждений культуры, обладавшие профессиональными навыками работы с информацией и продвигавшие новые подходы к политике и экономике, новую идеологию прошлого, настоящего и будущего страны, быстро завоевывали общественный авторитет. В самых разных слоях советского общества возникает и активно проявляется запрос на объективную и полную информацию о текущем положении в стране, о бюджете КПСС, о западном образе жизни, о забытых или запрещавшихся к упоминанию аспектах отечественной истории и культуры и т.п.

Стимулом для развития общественно-политических дискуссий стали альтернативные выборы в Верховный совет народных депутатов СССР в 1989 г., причем впервые за семь десятилетий в информационном пространстве страны появились агитационные материалы различных партий

[90] РГАСПИ. Ф. 17. Оп. 158. Д.1164. Л.12. 133.
[91] Там же. Оп. 159. Д. 91. Л. 68.
[92] Там же. Д. 90. Л.98; Д. 91. Л. 16.

и движений. В.Ф. Новиков, секретарь Московского областного комитета КПСС сообщал, в частности, о «лихорадке листовочной войны», охватившей филиал Института физики атмосферы АН СССР в период избирательной кампании[93]. Органы власти в этой ситуации стремились максимально сузить возможности для информационного воздействия на советское общество оппозиционных сил, используя различные организационные рычаги[94].

Произошедшая в СССР в 1980-х гг. «революция сознания», которая стала во многом неожиданностью для партийных идеологов, пытавшихся противопоставить процессам трансформации информационного пространства старые административные рычаги воздействия на коллективы предприятий, средства массовой информации, своих соратников по КПСС, проявлявших интерес к проектам либеральных реформ[95]. Структуры КПСС на местах, давно утратившие навык настоящей политической агитации, мыслившие, в основном, шаблонами «застойного» времени, теряли свои позиции, в том числе из-за упрощенного и пассивного восприятия информации[96]. Так, участник одной из региональных конференций КПСС в январе 1989 г., ответственный партийный работник заявлял о деструктивном влиянии со стороны политически незрелой интеллигенции на настроения в обществе[97].

В последующий период на волне либерализации советского общества официальные мероприятия в честь годовщины Октябрьской революции или празднования Первомая порой перетекали в стихийные митинги, на которых звучали речи, оппозиционные коммунистической власти, предавались гласности факты, выставлявшие в отрицательном свете местных партийных деятелей и представителей администрации[98]. Упоминания о росте среди

---

[93] РГАСПИ. Ф. 17. Оп. 158. Д. 572. Л. 23.
[94] *Исаков В.Б.* Председатель Совета Республики. Парламентские дневники. 1990-1991. Екатеринбург, 1997. С.63-65.
[95] РГАСПИ. Ф. 17. Оп. 158. Д. 1164. Л. 32-34.
[96] *Волгин Е.И.* Политическая трансформация КПСС (1990–1991 гг.) // Вестник Московского университета. Серия 12: Политические науки. 2006. № 6. С.26-27.
[97] Там же. Л.150.
[98] РГАСПИ. Ф. 17. Оп. 158. Д. 1164. Лл. 59-60, 77-82.

советских граждан враждебности к идеалам социализма и партии, о нападках на КПСС со стороны «демократов» неоднократно встречаются в материалах партийных организаций Башкирской АССР 1989 – 1990 гг.[99]

В конце 1980-х гг. партийно-политическое руководство СССР, несмотря на провозглашенную им же политику гласности, стремилось сохранить контроль над СМИ и техническими средствами передачи информации – телевидением, радиовещанием и типографским оборудованием, которое должно было оставаться в руках государства либо общественных организаций. В то же время, проявилось и несоответствие данных устремлений реалиям общественной жизни СССР конца 1980-х гг., прежде всего, многократно возросшему политическому влиянию прессы[100]. Де факто к 1990 году в СССР возникла так называемая «новая пресса» – сеть кооперативных газет и журналов, а также несколько негосударственных информационных агентств, включая действующий до настоящего времени «Интерфакс», и независимых телестудий[101]. Значительная часть новых периодических изданий не располагала прочной материально-технической базой. В то же время происходило активное освоение передовых на тот момент технологий распространения информации, так печатные СМИ, не имевшие доступа к государственным типографиям, использовали любую доступную множительную технику, в том числе получавший в эти годы в СССР распространение ксерокс. По свидетельству одного из авторов Закона СССР о печати М.А. Федотова в нескольких регионах страны (в Екатеринбурге, Москве и Московской области, Волгограде) началось внедрение локальных систем кабельного телевидения с собственными программами. Все это происходило еще до появления в СССР законодательства о СМИ и развивалось на основе Закона о кооперации и «на базе индивидуальных политических решений» представителей высшего

[99] РГАСПИ. Ф. 17. Оп. 159. Д. 90. Л. 60.
[100] *Федотов М.А.* Закон СССР о печати как юридическое чудо // Новое литературное обозрение. 2007. № 1 (83). С.463-502.
[101] Там же.

партийного руководства общесоюзного и регионального уровней[102]. Первый секретарь ЦК компартии РСФСР И.К. Полозков в ходе заседания Башкирской областной партийной конференции 26 октября 1990 г. с горечью констатировал, что партия, по существу лишилась главного идеологического оружия – печати, радио и телевидения, и призывал к срочному созданию собственных СМИ на местах, чтобы срочно создавать собственные средства массовой информации, особенно на местах, чтобы противостоять натиску независимой прессы на КПСС, новым трактовкам отечественной истории и критике текущей политики советских властей[103].

Серьезное беспокойство руководящих партийных и советских органов вызывала фактическая утрата контроля над распространявшимися в обществе информационными потоками, включая влияние массовой западной культуры, распространявшейся через открывавшиеся в этот период по всей стране видеосалоны. Например, в Башкирии только в одном Нефтекамске в 1989 г. действовало 22 видеосалона[104]. Министр культуры Башкирской АССР С.Х. Аминев, выступая на Пленуме Башкирского областного комитета КПСС 16 июня 1989 г., отмечал, что в иностранном видео, распространившемся на территории республики, идет пропаганда «освобождения нравственных норм»[105]. Со своей стороны, идеологические структуры КПСС предпринимали попытки усилить свое информационное влияние. Первый секретарь Башкирского обкома КПСС Р.Х. Хабибуллин в дни предвыборной кампании осени 1989 года подчеркивал особую роль средств массовой информации и пропаганды, которые призваны были в ходе предвыборной борьбы обеспечивать равные условия для кандидатов в депутаты, а также всесторонне освещать электоральный процесс[106].

---

[102] *Федотов М.А.* Закон СССР о печати как юридическое чудо // Новое литературное обозрение. 2007. № 1 (83). С. 463-502.
[103] РГАСПИ. Ф. 17. Оп. 158. Д. 93. Л. 62-63.
[104] Там же. Л. 69.
[105] Там же.
[106] РГАСПИ. Ф. 17. Оп. 159. Д. 90. Л. 16.

Региональные парторганизации пытались осуществлять руководство местными СМИ, что в большинстве случаев уже не давало ожидаемого эффекта. Привыкнув к абсолютному доминированию в общественно-политическом пространстве, парткомы не находили в своих рядах людей, которые способны были бы выступать на митингах, вести аргументированную полемику в любой аудитории, противодействуя антисоциалистическим, националистическим и демагогическим призывам[107]. Некоторые попытки со стороны партийных организаций на местах завоевать общественное мнение, используя информационные технологии, были сделаны. В Татарстане, Удмуртии, Чувашии и ряде других регионов России местные партийные структуры начали выпускать свои газеты и журналы, стремясь интегрироваться в новое информационное пространство[108]. Продолжали использоваться и отработанные в предшествующие десятилетия формы пропаганды и агитации среди низового аппарата КПСС – школы партийной учебы, слушателям которых разъяснялась политика реформ и давались инструкции, как отвечать на критику со стороны формирующейся политической оппозиции[109].

Принадлежность к КПСС обеспечивала рядовым коммунистам частичный доступ к определенному, несколько более высокому, чем у беспартийных граждан, уровню информации об общественно-политическом и экономическом положении в стране и решениях ЦК партии. В годы «перестройки» низовой слой компартии также начинает ощущать недостаточность своей информированности о решениях высшего руководства. Например, первый секретарь Гродненского горкома КПСС (Белоруссия) А.И. Альшин, выступая на Пленуме республиканского ЦК в декабре 1989 г. отмечал, что трибуна Съезда народных депутатов стала ареной политических дискуссий и обсуждения партийных вопросов. При этом материалы Пленумов и конференций ЦК КПСС были для рядовых

[107] РГАСПИ. Ф. 17. Оп. 159. Д. 90. Л. 16.
[108] Там же. Л. 134.
[109] Там же. Оп. 158. Д.1099. Л. 92.

коммунистов «покрыты тайной» [110], оставались неясными для них личные политические позиции членов ЦК и Политбюро в условиях возникновения серьезных разногласий в партийной элите СССР[111].

Следует отметить, что начавшееся в 1988–1990 гг. внедрение в систему социалистического хозяйства некоторых элементов рыночной экономики и курс на развитие торгово-экономических связей со странами Запада, оказывали определенное влияние на сферу информационной безопасности в направлении смягчения режима секретности. Так, в 1988 г. Главлит выдвинул предложение о снятии некоторых ограничений, распространявшихся на публикацию информации о советских финансах, внешней политике и внешней политике СССР[112]. В том же году в журнале «Коммунист» вышла в свет статья начальника Управления КГБ СССР В.А. Рубанова, в которой ставился вопрос о формировании новых подходов к сфере секретной информации, в частности, о разделении правовых режимов тайны на государственные и промышленные секреты. Свое предложение автор обосновывал актуальностью задач развития отношений социалистической собственности и повышения самостоятельности советских предприятий[113]. В.А. Рубанов выдвигал также идею перестройки системы режимно-секретной деятельности с переносом приоритетов в сферу развития информационных технологий[114].

В принятый в 1990 г. Закон «О предприятиях в СССР» была включена статья «Коммерческая тайна предприятия»[115], а в тексте документа «Основы гражданского законодательства Союза ССР и союзных республик» 1991 г.

---

[110] РГАСПИ. Ф. 17. Оп. 159. Д. 1170. Л. 45.
[111] Там же.
[112] *Зеленов М.В.* Военная и государственная тайна в РСФСР и СССР. С.155.
[113] *Рубанов В.А.* От культа секретности к информационной культуре // Коммунист. 1988. № 13. С. 24-36.
[114] *Рубанов В.А.* Основные направления перестройки режимно-секретной деятельности // Труды НИИ «Прогноз» КГБ СССР. М., 1988. Вып. 8. № 1101. С. 6 -20.
[115] Закон СССР от 4 июня 1990 № 1529-1 «О предприятиях в СССР» // Ведомости Съезда народных депутатов СССР и Верховного Совета СССР, 1990, № 25, ст. 460.

были отражены вопросы охраны секретов производства[116]. Хотя данные нормы свидетельствовали о том, что теория коммерческого права в его международном понимании того времени еще не вполне утвердилась в российской законотворческой деятельности, они явились важным шагом вперед в становлении в России правовых основ информационной безопасности бизнеса[117].

Некоторая либерализация подходов к информационному обмену СССР с зарубежными странами заметна в Инструкции «О порядке контроля за перевозимыми через государственную границу СССР печатными, аудиовизуальными, другими материалами и документами»., изданной 16 декабря 1988 г. совместно Главным управлением государственного таможенного контроля (ГУ ГТК) при Совмине СССР, КГБ СССР и Главлитом. В частности, данным документом разрешался беспрепятственный ввоз в СССР материалов по изобразительному искусству, театру, балету, кино, музыке[118]. Следует отметить, что к данной категории могли быть отнесены издания, посвященные творческому наследию российского зарубежья, записи западной рок-музыки и другие материалы, ранее закрытые для советских граждан (при условии отсутствия в них информации антисоветского и экстремистского характера). В СССР разрешался свободный ввоз печатных и аудиовизуальных материалов религиозного содержания, при условии, что они были изданы официально и не имели антисоветской или антикоммунистической направленности. Свободно пропускались через границу также предметы религиозного культа или с

---

[116] Основы гражданского законодательства Союза ССР и союзных республик. 31 мая 1991 г. № 2211-1 // Ведомости Съезда народных депутатов СССР и Верховного Совета СССР, 1991, № 26, ст. 733.

[117] См. Основные правовые системы ограничения в доступе к информации в Российской Федерации: первичные системы / Фатьянов А.А. М.: КноРус, 2020. 210 с.

[118] О порядке контроля за перевозимыми через государственную границу СССР печатными, аудиовизуальными, другими материалами и документами: Инструкция ГУ ГТК при Совмине СССР, КГБ СССР, Главного управления по охране государственных тайн в печати при Совмине СССР от 16.12.88 № 11-11/205 ДСП (в ред. Приказа ТК СССР от 30.09.1991) [Электронный ресурс] // «Контур Норматив»: Информационно-правовой портал. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=28853 (Дата обращения: 18.11.2021)

религиозной символикой, но их количество ограничивалось двумя экземплярами каждого изделия. При этом иностранные религиозные и религиозно-пропагандистские издания, направлявшиеся в адрес церковных организаций СССР, провозились беспрепятственно. Для материалов, предназначавшихся к вывозу из СССР, ограничения существовали в отношении текстов и аудиоматериалов различных видов для служебного пользования, рукописей, перфокарт, перфолент, дискет, магнитных дисков, и других носителей информации, пропускавшихся через границу с разрешения соответствующих ведомств. Не требовалось разрешений на ввоз и вывоз из страны каталогов товаров и рекламной продукции[119].

12 июня 1990 г. был принят Закон СССР «О печати и других средствах массовой информации»[120], впервые в советское время вводивший принцип недопустимости цензурных ограничений средств массовой информации. Вместе с тем, в законе отсутствовало определение цензуры, что существенно ограничивало возможности его практического использования. Функцию информационного контроля деятельности СМИ сохраняло созданное при Совмине СССР на базе Главлита Главное управление по охране государственных тайн в печати и других средствах массовой информации (ГУОТ). Год спустя оно было преобразовано в Агентство по защите государственных секретов в СМИ, находившееся в ведении союзного Министерства информации и печати[121]. Тем самым понижался статус данного учреждения системе исполнительной власти и, соответственно, уменьшались и возможности его влияния на деятельность прессы и

---

[119] О порядке контроля за перевозимыми через государственную границу СССР печатными, аудиовизуальными, другими материалами и документами: Инструкция ГУ ГТК при Совмине СССР, КГБ СССР, Главного управления по охране государственных тайн в печати при Совмине СССР от 16.12.88 № 11-11/205 ДСП (в ред. Приказа ТК СССР от 30.09.1991) [Электронный ресурс] // «Контур Норматив»: Информационно-правовой портал. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=28853 (Дата обращения: 18.11.2021)

[120] Закон СССР от 12 июня 1990 г. № 1552-1: «О печати и других средствах массовой информации» // Ведомости СНД и ВС СССР. 1990. № 26, ст. 492.

[121] *Горяева Т.М.* История советской политической цензуры, 1917–1991 гг.: Автореферат дисс. … доктора политических наук. Москва, 2000. 40 с.

книгоиздательскую сферу. Оно было окончательно упразднено в ноябре 1991 г. в числе других общесоюзных ведомств. В РСФСР к этому моменту уже действовала Госинспекция по защите свободы печати и массовой информации[122]. 11 сентября 1991 г. вышел Указ Президента России Б.Н. Ельцина «О мерах по защите свободы печати в РСФСР», которым внедреляся принципиально новый подход власти к информационной сфере[123].

Таким образом, в период конца 1980-х – 1991 гг. проявляются тенденции концептуальных изменений государственной политики СССР в сфере информационной безопасности под влиянием процессов либерализации общественной жизни и внедрения в советскую экономику некоторых рыночных институтов. Накануне распада СССР был сделан ряд шагов в нормативно-правовой сфере, направленных на деидеологизацию информационной политики страны, включая отмену цензурных ограничений.

Во второй половине 1980-х – начале 1990-х гг. в среде научно-технической интеллигенции, в том числе среди специалистов, профессионально работающих в области информационной безопасности (аналитических отделах советских спецслужб и др.), идет осмысление глобальных тенденций развития информационных технологий и роли информации как фактора общественного развития.

---

[122] *Горяева Т.М.* История советской политической цензуры, 1917–1991 гг.: Автореферат дисс. … доктора политических наук. Москва, 2000. 40 с.

[123] Указ Президента Российской Федерации от 11 сентября 1991 г. «О мерах по защите свободы печати в РСФСР» [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/acts/bank/185

1.2. Становление концепций и правовой системы государственной политики информационной безопасности в России в 1990-е гг.

На начальном этапе рыночных реформ государственная политика России в области информационной безопасности развивается под влиянием нескольких основных факторов:

- становления демократической правовой государственности, обусловившего окончательную отмену политической цензуры, а также изменение представлений о правах личности, включая информационную защиту частной жизни;

- трансформации концепций и приоритетов внешней политики Российской Федерации, что оказывало влияние на сферу информационного обмена с иностранными государствами;

- интеграции России в глобальную информационную систему Интернета;

- формирования институтов рыночной экономики – частных предприятий и компаний, банков и др., взаимодействие которых друг с другом и системой государственного регулирования экономики требовало разработки нормативных основ защиты коммерческой тайны и секретов производства.

В течение 1990-х гг. получили дальнейшее развитие подходы к вопросам информационной безопасности, сложившиеся в период позднего СССР. В процессе обновления российского законодательства в постсоветский период изначально устанавливался баланс между основополагающими принципами свободы слова и печати, а также правом доступа граждан к информации, связанной с обеспечением их прав и свобод, экологии, деятельности органов власти и управления, и требованиями информационной безопасности. При этом отказ от идеологического компонента в государственной информационной политике и утверждение свободы печати потребовали четкого определения подходов к защите

государственной тайны и других видов секретной информации в новых условиях.

Основополагающие принципы гармонизации интересов личности, общества и государства постсоветской России в сфере информационной безопасности были обозначены в «Декларации прав и свобод человека и гражданина» (22 ноября 1991 г.)[124] В данном документе утверждалось право каждого человека и гражданина России на неприкосновенность частной жизни, включая тайну переписки и других личных информационных коммуникаций, а также право на осуществление поиска, на получение и свободное распространение информации. «Декларация» оговаривала возможность ограничения реализации данных прав в соответствии с законом и судебными решениями. В том числе указывалось на необходимость защиты тайны, и перечислялись ее виды: семейная, профессиональная, коммерческая и государственная[125].

В течение 1990-х гг. были созданы нормативно-правовые основы государственной политики России в сфере информационной безопасности. Формировалась также система государственных институтов, обеспечивавших реализацию данной отрасли государственной политики в административно-организационном и технологическом плане. (Их становлению и деятельности посвящена вторая глава диссертации). Так, функции обеспечения информационной безопасности в секторе государственного управления обеспечивало Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ), созданное 25 декабря 1991 г.[126], и ряд других структур, о которых будет подробнее сказано далее.

---

[124] Постановление Верховного Совета РСФСР от 22.11.1991 № 1920-I «О Декларации прав и свобод человека и гражданина» // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР от 01.01.1991, N52, стр.1865.

[125] Там же.

[126] *Полонский И.* День ФАПСИ (1991-2003). Слово о правительственной связи [Электронный ресурс] // Военное обозрение. 24 декабря 2015 г. URL: https://topwar.ru/88409-den-fapsi-1991-2003-slovo-o-pravitelstvennoy-svyazi.html (Дата обращения: 19.11.2021)

Права и свободы граждан России в области получения и защиты информации нашли отражение в Конституции Российской Федерации, которая содержала целый ряд позиций, связанных с темой информационной безопасности личности: право на неприкосновенность частной жизни, на сохранение личной и семейной тайны и др. (Ст. 23-24)[127].

Согласно Закону Российской Федерации от 27 декабря 1991 г. «О средствах массовой информации», который, как уже отмечалось выше, окончательно отменил цензуру в России, не допускалось разглашение в СМИ для разглашения государственной тайны и других видов информации, распространение которой ограничивалось законодательно. Соответственно, обязанность государственных учреждений предоставлять информацию по запросам журналистов не распространялась на сведения, входящие в данную категорию. В последующие годы в Закон о СМИ неоднократно вносились поправки, в том числе вводившие дополнительные ограничения (на публикацию порнографии, материалов, пропагандирующих культ насилия и жестокости, использование в видеоматериалах и компьютерных файлах «скрытых вставок», которые могут оказывать воздействие на подсознание людей и создавать угрозу их здоровью и др.). В то же время, большинство осуществленных корректировок законодательства не оказало заметного воздействия на развитие свободы СМИ в России[128].

В первой половине 1990-х гг. осуществляется формирование нормативно-правовой базы государственной тайны, в процессе которого складывается новое федеральное законодательство, регулирующее данную сферу. В то же время был сохранен апробированный временем механизм периодического обновления перечней сведений, составляющих государственную тайну. Впервые в постсоветском законодательстве вопрос об обеспечении информационной безопасности страны был отражен в Законе

---

[127] Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. Москва: Издание ЦИК, 1993.

[128] *Давтян С.Л.* Изменения Закона РФ «О средствах массовой информации» в 1991-2010 гг.: факты как история // Вестник Московского университета. Серия 10. Журналистика. 2011. № 3. С. 13.

Российской Федерации от 5 марта 1992 г. «О безопасности», определявшем понятие безопасности личности, общества и государства, концептуальные и организационные основы их защиты от внешних и внутренних угроз[129].

Информационная безопасность Законом от 5 марта 1992 г. выделялась в самостоятельный вид безопасности наряду с государственной, оборонной, экономической, общественной, экологической и другими видами безопасности, рассмотрение которых входит в сферу компетенции Совета безопасности Российской Федерации[130].

Следует отметить, что в этот период задачи формирования концептуальной и правовой основы государственной политики России в сфере информационной безопасности приобрели особую актуальность в контексте бурного стихийного развития рыночной экономики. В начале 1990-х гг. на волне широкой либерализации общественных отношений, в условиях прекращения «холодной войны» и активного развития культурных и экономических связей с Западом, в России происходит размывание представлений о безопасности, значении государственной тайны и секретов производства. Об этом свидетельствуют, в частности, материалы ряда журналистских расследований тех лет, посвященных коммерческим сделкам, связанным с передачей за границу ценных промышленных технологий и другой информации, значимой для экономики и государственной безопасности страны[131].

Существовавшая в этот период значительная потребность отечественной промышленности в дополнительных финансовых ресурсах вела в ряде случаев к ситуациям, неоднозначным с точки зрения информационной безопасности в экономической сфере. В частности, предприятия российского ВПК, не имевшие в тот период достаточного

---

[129] Федеральный закон от 5 марта 1992 года № 2646-1 «О безопасности» // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ, 1992, № 15, ст. 769.
[130] Там же.
[131] *Турченко С.* В опасности ... безопасность // Советская Россия. 18 марта 1993 г.; Климов В. Продаются секреты. В придачу оружие и бриллианты // Российская газета. 23 ноября 1994 г.

объема государственных заказов, вели поиск иностранных инвесторов, что давало потенциальный доступ иностранным компаниям к российским промышленным секретам и другой стратегически значимой информации. Так, например, в июне 1993 г. состоялась встреча руководства ряда крупных предприятий Челябинской области с делегацией представителей General Motors и ряда других американских корпораций, в ходе которой обсуждались перспективы инвестиционного сотрудничества в таких отраслях как оборонная промышленность, ракетостроение и др.[132]

Подобные тенденции вызывали обеспокоенность значительной части российского общества, включая ведущих специалистов в области безопасности, что нашло отклик в формировании концепций государственной политики информационной безопасности, в том числе в законотворческом процессе. «Информация настолько свободно циркулировала в нашем обществе, что спохватились: слишком свободно!», – вспоминал позднее один из участников Круглого стола, посвященного 10-летию Закона РФ «О государственной тайне», проведенного в Санкт-Петербургском университете в 2003 г.[133]

В целом, развитие государственной политики России в области информационной безопасности в 1990-х гг. происходило в сложных условиях. Становление демократической государственности, институтов гражданского общества, интеграция страны в международное экономическое, социально-культурное пространство, процессы информатизации делового пространства развивались на фоне государственно-политической и экономической нестабильности. Оборотной стороной рыночных преобразований в 1990-е гг. явилось ослабление

---

[132] *Попов И.* Встреча промышленников Челябинска и США // Коммерсант. 26 июня 1993 г. № 119 (342).

[133] Возможна ли безопасность в информационном обществе? Круглый стол, посвященный 10-летию Закона РФ «О государственной тайне» // Санкт-Петербургский университет. 28 ноября 2003 г. № 27 (3652). URL: https://old.journal.spbu.ru/2003/27/3.shtml

институтов государственного управления, рост преступности, фрагментарность новой нормативно-правовой базы[134].

На протяжении всего рассматриваемого периода существовал дискурс между журналистским сообществом, требовавшим абсолютной свободы в получении и публикации информации, и государством, выдвигавшим на первый план вопросы безопасности и стабильности общества, требовавшие в ряде случаев информационных ограничений. Это показывает, в частности, позднейшая дискуссия между Е.Г. Ясиным и А.А. Венедиктовым в эфире радиостанции «Эхо Москвы» о том, как следовало освещать в СМИ события дефолта 1998 года – дозировать информацию, чтобы не вызвать паники, или давать ее в полном объеме[135].

Новым этапом в развитии отечественной системы информационной безопасности стало принятие 21 июля 1993 г. (впервые в отечественной истории) Закона Российской Федерации «О государственной тайне». Данный Закон, вступивший в силу 21 сентября того же года, включал определение государственной тайны как «защищаемых государством сведений в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации»[136]. В Закон были включены рамочные статьи, определявшие базовые параметры деятельности государственных учреждений по формированию «Перечня сведений», которые принадлежали к категории государственной тайны. Устанавливался порядок, согласно которому такие подготовленные правительством «Перечни», утверждались президентом

---

[134] *Швецов А.Н.* Социально-экономические процессы переходного периода. Москва: Гостехиздат, 2015; *Пихоя Р.Г.* История современной России. Десятилетие либеральных реформ. 1991-1999 гг. / Р.Г. Пихоя, С.В. Журавлев, А.К. Соколов. М.: Новый хронограф, 2020.

[135] Свобода слова в 90-е [Электронный ресурс] // Эхо Москвы. 8 мая 2008 г. URL: https://echo.msk.ru/programs/niceninety/512707-echo/ (Дата обращения: 22.11.2021)

[136] Закон РФ от 21 июля 1993 г. № 5485-I «О государственной тайне» // Российская газета. 21 сентября 1993 г. № 183 (799). С. 1.

России[137]. Кроме того, в Законе были определены виды информации, не являющиеся государственной тайной и, соответственно, не подлежавшие засекречиванию.

В последующий период осуществлялась детализация применения государственной тайны в различных областях государственного управления, В августе 1995 г. был издан федеральный закон «Об оперативно-розыскной деятельности», устанавливавший принадлежность к государственной тайне и, соответственно, секретность всего комплекса информации, связанной с подготовкой и проведением оперативно-розыскных мероприятий[138]. Постановлением Правительства РФ в сентябре 1995 г. были утверждены «Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности»[139], согласно которым вводились три уровня секретности, к которым могли относиться сведения, составлявшие государственную тайну, в зависимости от их важности. К разряду сведений особой важности была отнесена информация, поступление которой в публичное пространство может нанести урон Российской Федерации как государству; данные, относящиеся к сфере информационно безопасности государственных учреждений или отраслей экономики России, определялись как совершенно секретные; группу секретных сведения составляла информация, которая имеет отношений к работой предприятий и организаций, связанных с обороной, внешней политикой, разведкой и контрразведкой, оперативно-розыскной работой, инновационными технологиями[140].

На практике четкий порядок разработки и утверждения «Перечней сведений, составляющих государственную тайну», сложился не сразу: в

---

[137] Закон РФ от 21 июля 1993 г. № 5485-I «О государственной тайне» // Российская газета. 21 сентября 1993 г. № 183 (799). С. 1.

[138] Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности // СЗ РФ, 1995, № 33, ст.3349.

[139] Постановление Правительства РФ от 04.09.1995 г. № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» // СЗ РФ, 1995, № 37, ст. 3619.

[140] Там же.

течение двух лет, прошедший после выхода «Закона о государственной тайне», новый перечень не был подготовлен. 27 октября 1995 г. было принято Постановление Государственной Думы РФ, отмечавшее, что возникшая из-за отсутствия «Перечня» ситуация незащищенности сведений, отнесенных к государственной тайне, наносит ущерб безопасности страны[141]. Появление данного документа сыграло положительную роль в дальнейшем формировании государственной политики России в области информационной безопасности. Вопрос был оперативно (в течение месяца) решен[142], и в последующий период определение и утверждение круга сведений, составляющих государственную тайну РФ, осуществлялось в установленном порядке. Министерство обороны РФ формировало отдельные «Перечни сведений, подлежащих засекречиванию в Вооруженных силах Российской Федерации»[143].

Формирование концептуальных подходов к институту государственной тайны продолжалось и в последующие годы. В разработке этого вопроса принял участие Конституционный суд РФ, в своем Постановлении от 20 декабря 1995 г. указавший, что «Перечень сведений, составляющих государственную тайну», должен быть утвержден федеральным законом и опубликован для общественного ознакомления[144]. Кроме того, Конституционный суд в Постановлении которого от 27 марта 1996 г. установил соответствие указанного в Законе «О государственной тайне» порядка защиты государственной тайны нормам Конституции России и

---

[141] Постановление Государственной Думы № 1271-1 ГД от 27.10.1995 г. «О Перечне сведений, отнесенных к государственной тайне» // Собрание законодательства Российской Федерации от 01.01.1995, № 45, с. 429.

[142] Указ Президента РФ 30 ноября 1995 г. № 1230 «Об утверждении перечня сведений, отнесенных к государственной тайне» // Собрание законодательства Российской Федерации, 1995. № 49, ст. 4775.

[143] *Зеленов М.В.* Военная и государственная тайна в РСФСР и СССР. С. 159.

[144] *Смолькова И.В.* Государственная тайна – правовой институт современного российского государства // Материалы международной научно-практической конференции «Обеспечение национальной безопасности России в современном мире». Иркутск, 26–27 мая 2016 г. / Министерство образования и науки РФ; Байкальский государственный университет. Иркутск: Изд-во Байкальского государственного университета, 2016. С. 132

общепризнанным принципам демократической правовой государственности[145].

Была разработана Государственная программа обеспечения защиты государственной тайны в Российской Федерации на 1996–1997 годы», концептуальные и правовые подходы к государственной тайне обсуждались ведущими российскими экспертами в области информационной безопасности[146].

Важное место в становлении государственной политики России в области информационной безопасности занимает Федеральный закон «Об информации, информатизации и защите информации», принятый в феврале 1995 г. Данный правовой акт имел существенное значение в контексте становления в России демократической правовой государственности, поскольку впервые обозначал обязанности исполнительной власти в отношении создания информационных ресурсов и проведения политики информатизации. В частности, государство обязывалось обеспечивать право российских граждан на получение информации в соответствии с действующим законодательством, права на конфиденциальность информации, права субъектов на деятельность в сфере информации и цифровых технологий[147]. В Законе от 20 февраля 1995 г. содержалось также определения информации как правовой категории и целого ряда других, связанных с ней понятий – информатизации, документированной информации, информационных ресурсов, персональных данных и др.[148]

Стимулом для разработки и принятия Закона «Об информации, информатизации и защите информации» явилось подключение Российской

---

[145] Цит. по: Возможна ли безопасность в информационном обществе? Круглый стол, посвященный 10-летию Закона «О государственной тайне» [Электронный ресурс] // Санкт-Петербургский университет. 28 ноября 2003 г. № 27 (3652). URL: https://old.journal.spbu.ru/2003/27/3.shtml (Дата обращения: 22.11.2021)

[146] *Вус М.А., Гусев В.С.* Государственная тайна – правовой институт суверенного государства // Конфидент. 1996. № 1; и др.

[147] Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» // СЗ РФ, 1995, № 8, ст. 609.

[148] Там же.

Федерации как государства к Всемирной сети. В декабре 1993 г. ведущие отечественные интернет-провайдеры подписали договор «О порядке администрирования зоны RU», а 4 апреля 1994 г. Россия зарегистрировала собственный домен RU, заменивший замороженный домен СССР SU[149].

Одним из первых шагов в сфере обеспечения информационной безопасности в системе рыночной экономики стал Закон «О банках и банковской деятельности», принятый в декабре 1990 г. и явившийся (с последующими изменениями и дополнениями) основой для применения правовой категории банковской тайны в постсоветской системе финансового бизнеса[150]. Наряду с вопросами соблюдения условий доступа к банковской тайне самими кредитными организациями, существенное значение в данной отрасли приобрели задачи защиты отраслевых информационно-коммуникационных систем, учитывая то обстоятельство, что банки шли в авангарде освоения цифровых технологий[151].

В период 1993 – 1995 гг. был принят ряд законодательных актов, регулирующих различные области правоотношений, связанных с распространением и использованием информации: «О федеральных органах правительственной связи и информации» (24 декабря 1993 г.), Федеральный закон «Об обязательном экземпляре документов (29 декабря 1994 г.), который затрагивал, в том числе электронные издания, включая программы и базы данных, Федеральный закон «О связи» (16 февраля 1995 г.) и др. Сделан был шаг вперед в развитии института коммерческой тайны, отражение которого в действовавшем в первой половине 1990-х гг. законодательстве не в полной мере отвечало задачам правовой поддержки информационной безопасности промышленности и бизнеса. Включение в Гражданский кодекс РФ статьи 139 «Служебная и коммерческая тайна» получил позитивные оценки специалистов. В то же время высказывались и мнения о

---

[149] 10 лет назад был зарегистрирован домен RU [Электронный ресурс] // РИА «Новости». 7 апреля 2004 г. URL: https://ria.ru/20040407/562920.html (Дата обращения: 22.11.2021)

[150] *Соколова О.* Доступ к банковской тайне // Законность. 2004. № 8. С. 36-37.

[151] *Ершов В.Ф.* Модернизационный этап развития банковской сферы России в контексте процессов глобализации // Наука и бизнес: пути развития. 2019. № 7 (97). С. 171.

необходимости разработки отдельного федерального закона, регулирующего область коммерческой тайны[152].

Развивалась также нормативная база регулирования производства и использования технологий, связанных с защитой информации, как в плане обеспечения интересов производителей цифровой техники и программного обеспечения, так и в связи с задачами информационной безопасности государства и экономики России. В частности, повышенное внимание специалистов привлекают в этот период вопросы информационной безопасности в банковском секторе[153]. В этой связи руководством страны предпринимались меры по модернизации информационно-телекоммуникационных систем, имевших специализированное назначение. 3 апреля 1995 г. Президент России Б.Н. Ельцин подписал указ, который запрещал использование в информационно-телекоммуникационных системах государственных организаций и предприятий шифровальных устройств и других технических средств работы с информацией, без наличия сертификата Федерального агентства правительственной связи и информации (ФАПСИ) при Президенте Российской Федерации[154]. Предприятия, использовавшие оборудование и технологии, не получившие аналогичные сертификаты, не имели права выполнять государственные заказы. Центральному банку России предлагалось принять меры для обеспечения использования сертифицированных средств шифрования и передачи информации при взаимодействии с коммерческими банками. Юридические и физические лица, осуществляющие разработку, производство, реализацию и эксплуатацию средств шифрования информации, а также защищенных носителей информации и средств передачи данных, оказывающие услуги по

---

[152] *Куликов В.* О коммерческой тайне // Хозяйство и право. 1995. С. 114 – 117.

[153] *Герасименко В.Г., Сергеев В.В.* О проблеме информационной безопасности в банках России: потери, прогноз развития и некоторые пути решения // Вопросы защиты информации 1996. № 2. С. 52-56.

[154] Указ Президента РФ от 03.04.1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации // СЗ РФ, 1995. № 15, ст. 1285.

шифрованию информации[155], должны были в обязательном порядке иметь лицензии ФАПСИ. Предполагалось также не допускать ввоза на территорию России шифровальных средств, произведенных за границей без российской лицензии. В структуре ФАПСИ создавался Федеральный центр по защите экономической информации, в задачу которого должна была войти разработка и реализация программ защиты экономической информации российских банков и других предприятий и организаций, значимых для экономического развития страны[156]. Специалистами Госстандарта РФ (Комитет по стандартизации, метрологии и сертификации) был подготовлен и введен в действие с 1 июля 1997 г. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»[157].

Меры по защите отечественных информационно-коммуникационных систем, принимавшиеся руководством России в 1990-е гг., были направлены, в том числе на противодействие правонарушениям, включая деятельность организованной преступности в финансовом секторе и других отраслях экономики. Следует отметить, что вследствие коммерциализации инфраструктуры связи уже в начале 1990-х гг. в данном секторе происходят существенные позитивные изменения: внедрение новейшего оборудования и технологий, расширение спектра услуг для бизнеса и граждан. Развитию отечественной системы телекоммуникаций способствовала конверсия части военных радиочастот, переданных в 1995 г. операторам гражданской сотовой связи[158]. В то же время имели место такие факты как незаконное применение радиоэлектронных средств (РЭС), намеренное создание технических помех государственным системам связи и др. Данная ситуация обусловила, в

---

[155] Указ Президента РФ от 03.04.1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации // СЗ РФ, 1995. № 15, ст. 1285.

[156] Там же.

[157] База данных ГОСТ [Электронный ресурс] // Росстандарт. Центр сертификации. URL: https://rosstandart.msk.ru/gost/001.001.040.001/gost-r-50922-96/

[158] Министры связи РФ с 1990 года. Досье ТАСС [Электронный ресурс] // ТАСС. 18 мая 2018 г. URL: https://tass.ru/info/5214397 (Дата обращения: 20.11.2021).

частности, создание в 1993 г. Службы государственного надзора за связью при Министерстве связи России. Противоправные действия в условиях растущей рыночной конкуренции распространялись на быстро развивавшийся сектор цифровых информационных систем. Сотрудники российских спецслужб все чаще встречались с новыми, неизвестными ранее в России видами преступной деятельности с использованием компьютерной техники и электронных коммуникаций[159].. В этой связи был принят ряд новых правовых актов, направленных на противодействие данному явлению, разрабатывались и нведрялись новые методы оперативно-розыскных мероприятий, в свою очередь опиравшиеся на использование новейших информационных технологий[160]. В Уголовный кодекс РФ, принятый в 1996 году, была включена глава «Преступления в сфере компьютерной информации» (гл. 28). Три статьи, вошедшие в данную главу, касались наказания за правонарушения, связанные с использованием компьютерных технологий: несанкционированного доступа к цифровой информации, охраняемой законом (ст. 272), создания вредоносных программ (ст. 273) и нарушений правил использования и облуживания компьютерных систем (ст.274).

Однако в указанных выше нормативно-правовых документах практически не учитывались информационные риски, связанные с использованием программ и криптографических технологий иностранного производства. Так, Постановление Правительства России от 26 июня 1995 г. вводило обязательную сертификацию технических, криптографических, программных и других средств защиты информации, составляющей государственную тайну, а также средств контроля эффективности защиты

---

[159] *Вехов В.Б.* Некоторые способы совершения преступлений с использованием техники // Современные проблемы правоохранительной деятельности: Межвузовский сборник научный трудов. Волгоград: Высшая школа МВД РФ, 1995. С. 69-74; *Он же.* Компьютерные преступления: Способы совершения и раскрытия. М.: Право и Закон, 1996. С.3.

[160] Там же. С. 137-172.

секретных сведений[161]. Но только в 1999 г. было сделано уточнение, в том, что в системе государственных органов власти и управления и на стратегически значимых объектах должны использоваться криптографические (шифровальные) средства только отечественного производства и технологии, рекомендованные Федеральной службой безопасности России[162]. Не была к этому моменту преодолена и практика использования не сертифицированных программ и устройств, предназначенных для обработки, накопления и передачи информации. Специалисты в области информационной безопасности отмечали, что в ряде государственных учреждений, а также в большинстве кредитных организаций продолжали использоваться системы электронных коммуникаций, созданные на базе иностранных технологий, не прошедших российскую сертификацию по степени информационной безопасности[163].

4 июле 1996 г. вышел Закон РФ «Об участии в международном информационном обмене», направленный на интеграцию Российской Федерации в глобальную информационно-коммуникационную систему и повышение эффективности взаимодействия в сфере информатизации и информационного взаимодействия[164]. Положения закона регулировали процессы физического перемещения материальных носителей информации, не учитывая перспектив развития международных цифровых коммуникаций[165].

---

[161] Постановление Правительства РФ от 26.06.1995 г. № 608 «О сертификации средств защиты информации» // СЗ РФ 1995, № 27, ст. 2579; 1996, № 18, ст. 2142.

[162] Постановление Правительства Российской Федерации от 29 марта 1999 года № 342 «О внесении дополнения в Положение о сертификации средств защиты информации» [Электронный ресурс] // «Норматив Контур»: Информационно-правовой портал. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=8489 (Дата обращения: 18.11.2021)

[163] *Баранов А.П.* Проблемы обеспечения информационной безопасности в информационно-телекоммуникационной системе специального назначения и пути их решения // Информационное общество.1997. Вып. 1. С. 17.

[164] Закон Российской Федерации от 4 июля 1996 г. № 85-ФЗ. Об участии в международном информационном обмене // СЗ РФ, 1996, № 28, ст. 3347.

[165] *Чубукова С.Г.* Развитие концепции правового регулирования международного информационного обмена // Правовая информатика. 2018. № 4. С. 60.

В целом такой подход к информационному обмену, как и к вопросам обеспечения государственной и коммерческой безопасности, был обусловлен незначительной, по сравнению с началом XXI в., степенью охвата Интернетом государственно-административных систем и хозяйственно-экономического пространства. Еще на рубеже 1980-х – 1990-х гг. в российском обществе складывается представление об огромной перспективной роли информации в экономике и модернизационном развитии в целом. «Российская газета» 10 января 1991 г., отмечая, что информационные услуги представляют собой одну из наиболее доходных отраслей бизнеса. писала: «Путь к богатству – приоритетное развитие информационных технологий»[166]. В то же время, взаимосвязь между информатизацией и проблемами безопасности на тот момент в массовом сознании не выглядела актуальной. Глобальный рынок Интернет-услуг находился в стадии становления, шла острая конкурентная борьба ведущих компаний («война браузеров»), завершившаяся в 1998 г. победой Internet Explorer компании Microsoft. Один из ведущих специалистов компании Positive Technologies Д. Скляров, имеющий опыт работы программистом в конце 1990-х гг., отмечает, что уровень распространения Интерната в России этих лет был многократно ниже, чем в наши дни[167]. По словам авторов современной статьи, посвященной истории становления русскоязычного Интернета, хотя Рунет и существовал 20-25 лет назад, но «был практически пустым»[168]. Соответственно, хакерские атаки и другие проблемы, связанные с интегрированностью в глобальные сетевые системы, в то время не имели такой значимости для бизнеса, средств массовой информации и других владельцев информационных ресурсов, как в наши дни. Вопросы

---

[166] Направления прорыва. Из руин – к информационному обществу // Российская газета. 10 января 1991 г.

[167] *Скляров Д.* Как менялась информационная безопасность за последние 20 лет [Электронный ресурс] // Блог компании Positive Technologies Информационная безопасность. 24 апреля 2019 г. URL: https://habr.com/ru/company/pt/blog/449320/ (Дата обращения: 20.11.2021).

[168] «Это было лучшее время»: каким был интернет в России 90-х [Электронный ресурс] // Lenta.ru. 24 октября 2020 г. URL: https://lenta.ru/articles/2020/10/14/beeline_90e/

информационной безопасности бизнеса в 1990-е гг. также были преимущественно связаны с материальной защитой коммерческой и банковской тайны. Утечка данных о контрактах, инновационных разработках, банковских переводах и т.п. зависела от обеспечения физической недоступности бумажных документов и электронных носителей в офисах и сейфах, а также от человеческого фактора (соблюдения секретности персоналом, надежности охраны и т.п.). В то же время был сделан шаг вперед в обеспечении правовой защиты информации, в том числе программного обеспечения и баз данных, с позиций авторского права, что имело немаловажное значение для обеспечения экономических интересов разработчиков[169]. В сентябре 1992 г. был принят Закон РФ «О правовой охране программ для ЭВМ и баз данных», в которой программы приравнивались к авторским литературным произведениям, а базы данных – к сборникам[170]. Общие позиции охраны авторского права определялись на тот момент «Основами гражданского законодательства» 1991 г., а с 1993 г. – Законом «Об авторском праве и смежных правах»[171].

Во второй половине 1990-х гг. государственная политика России в сфере информационной безопасности начинает выходить на новый уровень развития, приобретая черты целостной концепции и ориентируясь на процессы информатизации глобального финансово-экономического, технологического и социального пространства. В 1997 г. была принята новая усовершенствованная редакция Федерального закона «О государственной тайне»[172], в которой, в частности, была представлена новая детализированная

---

[169] *Никифоров И.В.* Правовая охраны программ для ЭВМ и баз данных // Правоведение. 1993. № 4. С. 32-46.

[170] Закон РФ от 23 сентября 1992 г. № 3523-1 «О правовой охране программ для ЭВМ и баз данных» // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ, 1992, № 42, ст. 2325.

[171] Закон РФ от 9 июля 1993г. № 5351-1 «Об авторском праве и смежных правах» // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ, 1993. № 32., ст. 1242.

[172] Федеральный закон от 6 октября 1997 г. № 131-ФЗ «О внесении изменений и дополнений в Закон Российской Федерации «О государственной тайне» [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/acts/bank/11534 (Дата обращения: 18.11.2021).

версия перечня видов информации, представляющих собой государственную тайну. Законом предусматривались следующие группы данных, входящих в категорию гостайны: информация военного характера, информация, относящаяся к экономике, науке и технике, информация в сфере внешней политики и экономики, данные, касающиеся разведки, контрразведки и оперативно-розыскной работы[173].

Осуществленная к началу XXI века модернизация законодательства о государственной тайне обусловила становление данного института как центрального компонента системы информационной безопасности государства и общества[174]. Социальное значение сложившегося в этот период российского законодательства о государственной тайне определялось тем, что наряду с установлением видов информации, не подлежащей введению в общественное пространство, подтверждался свободный доступ к сведениям, имеющим существенное значение для обеспечения гражданских прав, защиты жизни и здоровья россиян (о чрезвычайных происшествиях, о состоянии экологии, здравоохранения, финансов страны и др.)[175]

Важным дополнением к комплексу нормативно-правовых документов, регулирующих сферу информационной безопасности, стал также Указ Президента России Б.Н. Ельцина от 6 марта 1997 г., которым был утвержден перечень сведений, относящихся к информации конфиденциального характера, включая коммерческую тайну, тайну судопроизводства, персональные данные и др.[176]

---

[173] Федеральный закон от 6 октября 1997 г. № 131-ФЗ «О внесении изменений и дополнений в Закон Российской Федерации «О государственной тайне» [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/acts/bank/11534 (Дата обращения: 18.11.2021).

[174] *Аникин П.П., Балыбердин А.Л., Вус М.А.* Государственная тайна и ее защита в Российской Федерации под общ. ред. М.А.Вуса и А.В. Федорова. СПб: Юрид. центр Пресс, 2003. 610 с.

[175] *Соколова О.С.* Институт государственной тайны в российском законодательстве [Электронный ресурс]. URL: https://www.lawmix.ru/comm/3502 (Дата обращения: 19.112021)

[176] Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ, 10 марта 1997 г. № 10, ст. 1127.

17 декабря 1997 г. была утверждена Концепция национальной безопасности Российской Федерации, в которой нашла отражение возросшая роль информации в системе защиты безопасности личности, общества и государства. В частности, разработка моделей и механизмов обеспечения информационной безопасности входит в число основных направлений деятельности государственных и общественных институтов по обеспечению национальной безопасности страны[177].

В 1999 г. была одобрена «Концепция государственной информационной политики Российской Федерации», подготовленная по заданию Комитета Госдумы РФ по информационной политике и связи. Документ был разработан группой квалифицированных специалистов, которую возглавляли Д.С. Черешкин, А.В. Волокитин, Б.В. Кристальный и О.А. Финько. В дни работы над Концепцией представители данной экспертной группы опубликовали ряд научных статей по вопросам развития глобального информационного общества, в которых подчеркивали, что Россия обладает высоким потенциалом как участник процесса мировой экономической и информационно-технологической интеграции. В одной из таких публикаций, в частности, говорилось, что параметры информационного общества, которое формируется в США и ведущих государствах Европейского Союза, должны, с учетом специфики социально-экономического и культурного облика России, стать ориентирами при отборе ключевых направлений и приоритетов в ходе построения информационного общества в России[178].

В декабре 1998 г. Концепция была одобрена Политическим консультативным советом, действубщим при Президенте РФ. Авторы Концепции подчеркивали, что формирование в России информационного общества является залогом социально-экономического развития страны и

---

[177] Указ Президента РФ от 17.12.1997 г. № 1300 «Об утверждении Концепции национальной безопасности Российской Федерации (в ред. от 10.01.2000 г. № 24) // СЗ РФ. 1997, № 52, ст. 5909

[178] *Смолян Г.Л., Черешкин Д.С.* О формировании информационного общества в России // Информационное общество. 1998. № 6. С. 8.

сохранения ее статуса как мировой державы. В документе была сформулирована стратегическая цель развития информационной политики государства в России: построение демократического информационного общества и вхождение страны в глобальное информационное пространство.[179] В качестве первоочередной задачи Концепция выдвигала создание в стране единого цифрового телекоммуникационного пространства через модернизацию и развитие уже существующих систем и технологий. Кроме того, государственная информационная политика решала задачи в сфере создания новых информационных ресурсов и обеспечения их широкой доступности, развития независимых СМИ, подготовки граждан к жизни и профессиональной деятельности в информационном обществе, формирования нормативно-правовой базы информационного общества[180].

Определенное внимание в Концепции было уделено системе информационной безопасности, которая рассматривалась как механизм взаимодействия государственной информационной политики и государственной политики национальной безопасности. Авторы Концепции сформулировали задачи государственной системы информационной безопасности: обеспечение сохранения государственной тайны и других тайн, защита информационных ресурсов и систем связей от атак информационного оружия, информационного терроризма и криминала. Особо подчеркивалась необходимость учитывать фактор глобального сетевого информационного обмена, создающего новые риски и угрозы в сфере личной и общественной информационной безопасности. В связи с этим предлагался комплекс мероприятий, которые позволяли осуществить формирование единых подходов государственных организаций и бизнеса к приобретению и использованию в стратегически значимых областях зарубежной цифровой техники и программного обеспечения[181].

---

[179] Концепция государственной информационной политики / Под общ. ред. О.А. Финько. Москва, 1999. 47 с.
[180] Там же.
[181] Там же.

Таким образом, в первом десятилетии российских реформ разработка и реализация государственной политики в области информационной безопасности осуществлялась в принципиально новых политико-экономических условиях, оказывавших существенное влияние на процессы информатизации общества, характер и механизмы формирования и распространения информационных потоков.

С началом демократических преобразований государство перестает быть монополистом в области создания и контроля информации. Средства массовой информации, частный бизнес, структуры гражданского общества России, являясь владельцами информационных ресурсов, получают возможность формировать собственные системы безопасности. Во второй половине 1990-х гг. существенно ускоряются процессы информатизации экономики и финансов, коммуникационных систем, российского общества в целом. Задачей государственной информационной политики в данных условиях становится создание единого правового пространства, в рамках которого функционируют институты и механизмы обеспечения информационной безопасности всех участников общественных отношений, включая институт государственной тайны.

К концу 1990-х гг. было завершено формирование основных сводов и правил, создававших платформу современной системы информационной безопасности личности, экономики и государства в России, в том числе для обеспечения эффективной деятельности институтов защиты государственной, коммерческой и других видов тайны. Создание законодательной базы государственной политики Российской Федерации в области информационной безопасности выступило существенным фактором дальнейшего развития информационных технологий как важнейшего компонента модернизации российской экономики и общества.

1.3. Формирование стратегии информационной безопасности Российской Федерации в начале XXI в.

В 2000-х гг. государственная политика Российской Федерации в области информационной безопасности развивалась в контексте нового стратегического курса социально-экономической модернизации страны, провозглашенного Президентом В.В. Путиным, включая совершенствование государственного управления, причем одним из ключевых компонентов осуществлявшихся преобразований явилось создание информационно открытой системы электронного администрирования. Другим базовым направлением развития России в 2000 – 2010-е гг. стало утверждение международных позиций России как мировой державы. Оба стратегических направления российской государственной политики потребовали, как будет показано далее, разработки и внедрения новых программно-целевых установок в вопросах обеспечения информационной безопасности.

Новый этап формирования российской государственной политики информационной безопасности определялся также растущим влиянием цифровизации на все стороны жизни общества, превращением информационных технологий в самостоятельный механизм взаимодействия государства и общественных институтов[182]. Реализация курса социально-экономической модернизации начиналась в условиях, когда в информационно-технологическом пространстве России и повседневной жизни россиян все более заметным становилось влияние цифровых технологий и, прежде всего, Интернета, стремительно увеличивалось количество зарегистрированных сайтов, информационных порталов, пользователей Рунета. После принятия в 2000 г. Хартии глобального информационного общества Россия показывала сверхвысокие темпы роста

[182] *Варламова Л.Н.* Государственная власть и общество: Пути взаимодействия через новые информационные технологии // Государственная власть и общество России в XX веке: Материалы межвузовской научной конференции, 15 мая 2004 г. / Российский государственный гуманитарный университет, Историко-архивный институт, Кафедра истории государственных учреждений и общественных организаций; сост.: Г.В. Кожевникова, Л.Д. Шаповалова. М., 2004. С. 182-185.

отрасли информационно-коммуникационных технологий – 30% в год, объемы трафика в российском интернете за период 2000 – 2008 гг. возросли в 183 раза[183]. В 2000-е гг. начинается бурное развитие российских социальных сетей – Live Journal, «Одноклассники», LinkedIn, Facebook, «ВКонтакте» и др.[184]. В этот же период на новый уровень выходят мировые телекоммуникационные технологии, что находит свое выражение в появлении смартфонов, среди которых в России лидером стала выпушенная в 2006 г. Nokia № 73. В 2007 г. состоялась презентация первого сенсорного аккумулятора iPhone 2G, который официально не был представлен на отечественном рынке, но россияне приобретали его за рубежом[185].

Активное включение граждан и деловых структур России 2000-х гг. в мировое цифровое пространство способствовало становлению в стране информационного общества, стимулировало развитие новых социальных институтов, образования, международных интеллектуальных связей. С другой стороны, возникали более серьезные риски и технологические проблемы в сфере информационной безопасности, как в частной жизни и бизнесе, так и на государственном уровне[186]. Соответственно, стратегия государственной информационной политики Российской Федерации в первом десятилетии XXI в. была дополнена концептуальными документами, отражающими взаимосвязь процессов информатизации и создания

---

[183] Заседание Совета по развитию информационного общества. 12 февраля 2009 г. Стенографический отчет [Электронный ресурс] // Президент России. Официальный сайт. URL: http://www.kremlin.ru/events/president/transcripts/3161 (Дата обращения: 21.11.2021)

[184] *Соколова С.* История соцсетей, рассказанная пионером Рунета [Электронный ресурс] // Архив RB.ru. 23 апреля 2014 г. URL: https://rb.ru/article/istoriya-sotssetey-rasskazannaya-pionerom-runeta/7323287.html (Дата обращения: 20.11.2021)

[185] Смартфоны и России и в мире: как они менялись [Электронный ресурс] // Роскачество. 2 апреля 2021 г. URL: https://rskrf.ru/news/smartfony-v-rossii-i-mire-kak-oni-menyalis/(Дата обращения: 20.11.2021)

[186] *Овчинников С.А., Гришин С.Е.* Угрозы личности, обществу и государству при внедрении информационных технологий // Информационная безопасность регионов. 2011. № 2 (9). № 2. С. 26.

информационного общества с задачами обеспечения информационной безопасности[187].

Существенными факторами развития российской государственной политики информационной безопасности в начале XXI в. явились тенденции, сложившиеся во второй половине 1990-х гг., прежде всего, информатизация отечественного делового пространства, общий рост числа пользователей Интернет и самоидентификация значительной части из них как сообщества, обладающего общими компетенциями, интересами и социальными запросами, связанными, прежде всего, с возможностями расширения свободных сетевых коммуникаций. Об этом говорит, в частности, появление ряда общественных организаций, таких, как Региональный общественный центр Интернет-технологий (РОЦИТ), основанный в 1996 г. в целях популяризации Интернета и формирования дружественной цифровой среды и активно действующий в настоящее время[188].

Важным компонентом институционализации отечественного Интернет-сообщества стало также развитие сетевого информационного бизнеса и сетевой журналистики[189]. В 1997 г. группой сетевых изданий Рунета был создан Международный союз интернет-деятелей «ЕЖЕ» (ЕЖЕ-движение) – саморегулируемую организацию, объединяющую представителей элиты интернет-бизнеса и ведущих IT-специалистов, которые взаимодействуют между собой и пространством русскоязычного Интернета, в целях популяризации и поддержки сетевых технологий и сетевой культуры в России. В то же время, участники ЕЖЕ-движения рассматривают его как подобие профессиональной гильдии, одной из основных задач которой

---

[187] Власть в обществе и информационная политика / Снетков В.Н., Пономаренко А.И., кол.авт. СПб: Изд-во Санкт-Петербургского государственного технологического института (технического университета), 2001. 244 с.

[188] О нас [Электронный ресурс] // Сайт РОЦИТ URL: https://rocit.ru/about (Дата обращения 20.11.2021).

[189] *Хаитина Н.* Интернет для журналистов, или Журналисты для Интернета. Русскоязычная пресса в Интернете // Мир Интернет 1998. № 4.

является защита их деловых и профессиональных интересов[190]. Подобные организации формировали новые модели социального поведения и общественной активности, так, авторы «Манифеста ЕЖЕ» подчеркивали, что движение не имеет официальных лидеров и иерархии, не поддерживает практику каких-либо заявлений от имени ЕЖЕ. В то же время его участники всегда находят возможность «постоять за интересы индустрии и ее работников»[191].

В 1998 г. был основан Институт развития информационного общества (ИРИО), который представляет собой научно-аналитический и консалтинговый центр. В настоящее время ИРИО осуществляет поддержку и продвижение технологий, которые способствуют развитию экономики, культуры и общественных институтов, работая под лозунгом: «Развитие информационного общества для нас не тренд, а деятельная гражданская позиция». В число основных задач ИРИО вошли также вопросы сетевой информационной безопасности, а именно противодействие распространению в телекоммуникационных сетях «асоциального контента»[192].

Интеллектуальная и деловая элита российского Интернета в силу специфики свой деятельности изначально проявляла интерес, как к вопросам пространственного и технологического расширения цифрового пространства, так и к теме информационной безопасности. С 2001 г. в Москве ежегодно проводится Национальный форум информационной безопасности (Инфофорум), начинавшийся как специализированное мероприятие, но в последующие годы утвердившийся в статусе крупнейшей площадки диалога IT-бизнеса, государства и экспертного сообщества[193]. Инициатива проведения форума исходила от Совета безопасности России и Комитета

---

[190] Манифест Международного союза интернет-деятелей ЕЖЕ / Малюков А., под ред. А Панесенкова и Д. Леонова. Москва, 2003.
[191] Там же.
[192] Институт развития информационного общества [Электронный ресурс] // Сайт ИРИО. URL: http://ирио.рф/ (Дата обращения: 20.11.2021).
[193] *Петров С.Т.* Национальный форум информационной безопасности «Инфофорум – 2015» // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2015. № 12(155). С. 157.

Государственной Думы РФ по безопасности в целях привлечения внимания российской общественности к проблематике информационной безопасности. Интерес российского информационного бизнеса, научных организаций, журналистов к данному мероприятию постоянно возрастал. О поддержке Инфофорума со стороны делового сообщества говорит тот факт, что его партнерами выступают такие отечественные и иностранные компании, как Ростехнологии, КРОК, ВСС, Microsoft, IBM, Huawei и др. Предметом обсуждения на Инфофоруме являются наиболее актуальные вопросы технологического, организационного, правового обеспечения безопасности российского и международного информационного пространства, проблемы развития рынка информационных технологий и услуг, безопасность банковской деятельности и т.п.[194]

Активность лидеров интернет-бизнеса в сфере ИБ нашла выражение в создании в 2003 г. Национальной коалиции против спама, в число учредителей которой вошли Mail.ru, Microsoft Russia, Лаборатория Касперского и ряд других компаний и фирм. С 2006 г. действует Российская ассоциация электронных коммуникаций (РАЭК), видящая свою миссию в поддержке процесса развития цивилизованного рынка электронных коммуникаций, в реализации проектов в профильном образовании и науке, в развитии нормативно-правовых механизмов защиты интересов участников цифрового рынка[195].

С 2004 г. в Москве проводится международная специализированная выставка по информационной безопасности Infosecurity Russia, организатором которой является британская выставочная компания Reed Exhibitions в сотрудничестве с российским Выставочным объединением «Рестэк». Первая выставка в серии Infosecurity состоялась в Лондоне в 1996 г. В Москве на этой площадке ежегодно собиралось до 5000 специалистов в

---

[194] *Петров С.Т.* Национальный форум информационной безопасности «Инфофорум – 2015» // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2015. № 12(155). С. 160-161.

[195] Об Ассоциации [Электронный ресурс] // Сайт РАЭК. URL: https://raec.ru/about/ (Дата обращения: 20.11.2021).

области IT, представителей интернет-бизнеса, крупных технологических компаний из российских регионов и стран ближнего зарубежья. С 2005 г. одновременно с Infosecurity Russia проводится международная выставка-конференция Storage Expo, объединяющая специалистов по системам хранения данных, а с 2007 г. специализированная выставка-конференция Documation, посвященная достижениям в области электронного документооборота.

Соответственно, в рассматриваемый период приобретают первостепенное значение такие аспекты государственной политики информационной безопасности, как взаимодействие с цифровыми структурами гражданского общества, в том числе с отечественным интернет-бизнесом в процессе реализации государственных информационных программ и проектов, обеспечение информационной безопасности государственного сегмента электронных коммуникаций, поддержка отечественных инновационных разработок в сфере защиты информации.

9 сентября 2000 г. Президентом Российской Федерации В.В. Путиным была утверждена первая в отечественной истории «Доктрина информационной безопасности Российской Федерации», в которой информационная безопасность определялась как защищенность национальных интересов России информационной сфере, которое обеспечивается на основе «совокупности сбалансированных интересов личности, общества и государства»[196].

Доктрина опиралась, прежде всего, на представления о приоритетности конституционных гарантий прав граждан на свободное получение и использование информации для разрешенной законом коммерческой, творческой, образовательной и иной деятельности и в интересах личностного развития; не менее существенное значение придавалось в Доктрине обеспечению прав на сохранение конфиденциальности в целях обеспечения

[196] Доктрина информационной безопасности Российской Федерации от 09.09.2000 № Пр-1895 (утратила силу) [Электронный ресурс] // Гарант.ру: информационно-правовой портал. URL: https://base.garant.ru/182535/ (Дата обращения: 12.05.2019).

личной безопасности[197]. Данный подход коррелировал с приоритетами развития России в XXI в., которые были сформулированы В.В. Путиным в его первом президентском Послании Федеральному собранию 8 июля 2000 г., включая создание эффективного демократического государства, инструменты которого обеспечивают «свободу личности, свободу предпринимательства, свободу развития институтов гражданского общества»[198].

С 2002 г. начинается реализация проекта цифровизации государственного управления Российской Федерации. Первым этапом в решении данной стратегической задачи явилась Федеральная целевая программа (ФЦП) «Электронная Россия», рассчитанная на 2002–2010 гг. Программа включала задачи по технологическому и организационному обеспечению взаимодействия общества и государственно-административного аппарата на основе информационных, в том числе сетевых технологий, предусматривала меры в области дальнейшего внедрения цифровых коммуникаций в повседневную жизнь россиян, совершенствования системы подготовки IT-специалистов и повышения компьютерной грамотности населения[199].

Уже на начальном этапе выполнения Программы обозначилась тенденция расширения взаимодействия государственных учреждений, общественных организаций и IT-предпринимательства в развитии информационных технологий, что сыграло важную роль и в плане обеспечения информационной безопасности, поскольку впоследствии негосударственные экспертные структуры выступали поставщиками идей и

---

[197] *Чеботарева А.А.* Информационная политика России в обеспечении информационной безопасности личности: история и современность // История государства и права. 2015. № 24.

[198] Государство Россия. Путь к эффективному государству (О положении в стране и основных направлениях внутренней и внешней политики государства): Послание Президента России Федеральному Собранию РФ. 8 июля 2000 г. // Президент России. Официальный сайт. URL: https://www.kremlin.ru/acts/bank/22401 (Дата обращения: 20.11.2021).

[199] ФЦП «Электронная Россия 2002-2010». Утверждена Распоряжением Правительства РФ от 28.01.2002 // СЗ РФ. 2002. № 5, ст. 531.

технологий зашиты информации в системах государственных и общественных (деловых) коммуникаций. На Интернет-конференции «Электронная Россия: проблемы и перспективы», состоявшейся 26 июня 2002 г., первый заместитель министра по связи и информатизации России А.В. Коротков, комментируя свое участие в работе некоммерческой организации «Партнерство для развития информационного общества России» (ПРИОР) подчеркнул, что считает за честь принять участие в объединении такого рода, которое отвечает его потребностям как государственного чиновника, стремящегося довести свою позицию до участников общественного диалога по вопросам развития информационного общества[200].

Следует отметить, что ПРИОР, основанное 30 ноября 2001 г. сыграло важную роль в развитии нового «партнерского»[201], этапа формирования в России информационного общества, который ознаменовался проявлением широкой общественной инициативы в области информатизации и становление механизмов совместного участия государства и общественных институтов в создании в стране современной информационной среды[202]. ПРИОР представляло собой ассоциацию более 50 организаций из различных регионов России, а также частных лиц, объединивших свои интеллектуальные, информационные, технологические и иные ресурсы в целях содействия полноправному вхождению России в глобальное информационное общество и строительству отечественной экономики знаний. В ПРИОР были представлены органы государственного управления,

---

[200] Электронная Россия: проблемы и перспективы: Интернет-конференция Первого заместителя Министра РФ по связи и информатизации А.В. Короткова. 26 июня 2002 г. URL // Информационно-правовой портал «Гарант.ру».: https://www.garant.ru/interview/10161/ (Дата обращения: 21.11.2021)

[201] *Ершова Т.В., Чугунов А.В.* Партнерство для развития информационного общества в России и его региональный сегмент на Северо-Западе России [Электронный ресурс] URL: http://www.ifahcom.ru/files/ershova_PRIOR.pdf (Дата обращения: 21.11.2021)

[202] *Кравченко В.И.* Власть и коммуникация: проблемы взаимодействия в информационном обществе. Санкт-Петербург: СПбГУЭФ, 2003. 270 с.

научно-исследовательские центры, коммерческие организации, инвестиционные группы и др.[203]

Несмотря на ряд проблем и трудностей, возникших на начальном этапе реализации ФЦП «Электронная Россия», ее основные параметры были успешно выполнены, при этом решались и задачи в области технологического обеспечения информационной безопасности. Так, органы государственной власти получили возможность использования волоконно-оптических линий связи для подключения к защищенной системе межведомственного электронного документооборота (МЭДО)[204]. Создание единого портала государственных услуг (www.gosuslugi.ru) способствовало повышению уровня информационной открытости сферы государственного управления, что сыграло важную роль в 2010-х гг. в процессе реализации концепции Открытого правительства[205]. При этом в сетевое пространство поступало все большее количество персональных данных граждан, что, в свою очередь, требовало усиления правовых и технологических гарантий их защиты от утечки в Интернет. Кроме того, различными министерствами и ведомствами федерального и регионального уровня в процессе цифровизации их деятельности создавались собственные системы защиты персональных данных, имеющие различную степень защищенности. В связи с этой проблемой в российском экспертном сообществе в течение ряда лет велись дискуссии о путях создания единой национальной инфраструктуры доверия (НИД), которая включала в себя систему удостоверяющих центров (УЦ), расположенных в едином домене цифрового доверия. Тем самым

---

[203] *Ершова Т.В.* Партнерство для развития информационного общества в России и поддержка «электронного» развития в регионах // Информационное общество. 2002. Вып.1. С. 25-26.

[204] *Кравчук Н.Ю., Юрков Д.В.* Государственные информационные ресурсы РФ на современном этапе: проблемы и перспективы развития // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2017. № Т.4. № 2. С. 119.

[205] *Юсупов Р.Г., Чинаев Т.В* Утверждение принципа информационной открытости государственных и муниципальных учреждений // Государственное управление в России: историко-правовые аспекты: Монография / Коллектив авторов; под научной редакцией Р.Г. Юсупова. Москва: ИНФРА-М, 2018.

должно было обеспечиваться безопасное единое пространство применения электронной подписи и других средств электронного документооборота[206]. В этой связи в 2010 г. было положено начало функционированию Единой системы идентификации и аутентификации (ЕСИА), которая постоянно развивается и совершенствуется в течение последующего десятилетия. С 2011 г. началось распространение ЕСИА на региональные системы государственных услуг, было обеспечено ее взаимодействие с web-приложениями электронного правительства[207]. Ежегодно осуществляется сертификация портала государственных услуг, в ходе которой анализируется его технологическое соответствие требованиям информационной безопасности. В арсенал информационной защиты портала госуслуг входят межсетевые экраны, антивирусные программы, средства предотвращения вторжений и другие технологии. Программное обеспечение портала госуслуг также сертифицируется Федеральной службой по техническому и экспортному контролю (ФСТЭК) по требованиям информационной безопасности[208].

В 2000-е гг. была модернизирована правовая база деятельности российских государственных структур, бизнеса и общественных организаций в информационном пространстве, в том числе приняты новые федеральные законы – «О техническом регулировании» (от 27 декабря 2002 № 184-ФЗ), «О связи» (от 7 июля 2003 № 126-ФЗ) и др.

---

[206] *Овчинников С.А., Ковалева Е.В.* Вопросы защиты информации при переходе на оказание государственных услуг в электронном виде // Вестник Саратовского государственного университета. 2012. № 5(44). С. 205.

[207] Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» [Электронный ресурс] // Информационно-правовой портал Гарант.ру. URL: https://www.garant.ru/products/ipo/prime/doc/12092469/ (Дата обращения: 21.11.2021)

[208] Защита персональных данных при предоставлении госуслуг. [Электронный ресурс] // Управление МВД России. 30 Октября 2016 г. https://40.xn--b1aew.xn--p1ai/news/item/8822881 (Дата обращения: 21.11.2021)

Федеральный закон «О коммерческой тайне» (9 июля 2004 г. № 98-ФЗ) имел существенное значение для защиты прав отечественного бизнеса и граждан, поскольку развивал и детализировал существующие нормы законодательства относительно коммерческой тайны, усиливая возможности борьбы с правонарушениями в данной сфере. К моменту его принятия в России было расследовано только одно уголовное дело по факту незаконного получения и использования конфиденциальной коммерческой информации[209]. Между тем, число преступных посягательств на коммерческую тайну было весьма велико. В частности, широкое распространение получили хищения денежных средств со счетов организаций и частных лиц, совершавшиеся при помощи поддельных банковских карт, чеков и аккредитивов. Данные преступления предварялись выявлением данных о номерах счетов и т.п. информации, составлявшей банковскую и коммерческую тайну[210].

Развитие законодательства о коммерческой тайне способствовало также формированию правовой и деловой культуры отечественного бизнеса. Российское предпринимательское сообщество, уделяя значительное внимание техническим средствам защиты коммерческой тайны, было недостаточно знакомо с правовыми нормами организации защиты конфиденциальной коммерческой информации на предприятии[211]. Примечательно, что именно в этот период элита отечественного бизнеса формирует свою корпоративную позицию в отношении информации и информационной безопасности. Так, 16 ноября 2004 г. на XIV съезде Российского союза промышленников и предпринимателей (РСПП) были приняты Социальная хартия российского бизнеса и Хартия корпоративной и деловой этики. В первом из этих документов, отражавшем гражданскую позицию делового сообщества и его готовность участвовать в процессе

---

[209] *Топорков А.А., Сербин И.С.* Коммерческая тайна и условия ее защиты по российскому законодательству // Lex Russica. 2006. Т.65. № 1. С.78.
[210] Там же. С. 78-79.
[211] Там же. С. 90.

устойчивого общественного развития страны, декларировалось стремление бизнеса к тому, чтобы его деятельность была открытой и прозрачной[212]. Хартия корпоративной и деловой этики включала добровольные обязательства лидеров предпринимательского сообщества России «избегать участия в распространении напрямую либо через третьих лиц заведомо ложной и непроверенной информации»[213].

Во второй половине 2000-х гг. вопросы информатизации России и дальнейшего становления институтов информационного общества являются предметом целенаправленного внимания российских законодателей и органов исполнительной власти[214]. При этом тема информационной безопасности государства и общества включается в число приоритетов государственной информационной политики. Наглядным свидетельством этой тенденции являются принятые в 2006 г. новые Федеральные законы «Об информации, информационных технологиях и о защите информации» и «О персональных данных», учитывающие уровень информатизации и развития сетевых технологий в России начала XXI в. В 2006 г был также утвержден Национальный стандарт РФ «Защита информации. Основные термины и определения», содержавший определения базовых понятий, связанных с информационной безопасностью[215]. В Стандарте были даны определения защищаемой информации – данных, которые являются предметом собственности и должны охраняться в соответствии с требованиями законодательства, либо в соответствии с требованиями, которые устанавливаются собственником. Под зашитой информации, согласно Стандарту, подразумевается деятельность, которая нацелена на

---

[212] Социальная хартия российского бизнеса. Принята XIV съездом РСПП 16 ноября 2004 г. URL: https://www.cproton.uu.ru/www.74rif.ru/rspp.html (Дата обращения: 20.11.2021).

[213] Хартия корпоративной и деловой этики. Принята XIV съездом РСПП 16 ноября 2004 г. URL: https://www.cproton.uu.ru/www.74rif.ru/rspp.html (Дата обращения: 20.11.2021).

[214] См. Государственная политика Российской Федерации в области развития информационного общества / А.В. Коротков, Б.В. Кристальный, И.Н. Курносов; под науч. ред. А.В. Короткова. Москва: Трейн, 2007.469 с.

[215] Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации Основные термины и определения» [Электронный ресурс] // Гарант.ру: информационно-правовой портал. URL: https://base.garant.ru/193664/ (дата обращения: 12.05.2019).

предотвращение утечки, несанкционированного доступа, разглашения и нежелательных преднамеренных и непреднамеренных воздействий на защищаемую информацию. В качестве самостоятельного направления защиты информации выделялось противодействие иностранной разведывательной деятельности[216].

25 июля 2007 г. на заседании Совета безопасности РФ, состоялось обсуждение проекта текста «Стратегии развития информационного общества». Президент России В.В. Путин в своем вступительном слове отметил, что в стране целенаправленно проводится политика информатизации экономики и общества в целом, а также системы государственного управления, активно идет распространение Интернета и сферы телекоммуникаций. В.В. Путин подчеркнул, что «Стратегия развития информационного общества» должна стать отправной точкой для комплекса конкретных долгосрочных программ и проектов, обеспечивающих развитие информационных технологий и повышение конкурентоспособности России в данной сфере[217]. Вместе с тем было уделено внимание задачам обеспечения национальной информационной безопасности, которые в условиях интеграции страны в глобальное информационное пространство приобретали дополнительную актуальность. Президент В.В. Путин, в частности, сказал: «Особое внимание прошу уделить вопросам информатизации безопасности в самом широком смысле этого слова. Ведь глобализация открывает для нас не только новые возможности, но и создает определенные риски, и мы должны быть готовыми адекватно парировать такие потенциальные угрозы, как, например, кибертерроризм»[218].

---

[216] Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации Основные термины и определения» [Электронный ресурс] // Гарант.ру: информационно-правовой портал. URL: https://base.garant.ru/193664/ (дата обращения: 12.05.2019).

[217] *Путин В.В.* Вступительное слово на заседании Совета безопасности по вопросу развития информационного общества в России. Москва, Кремль, 25 июля 2007 года [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.special.kremlin.ru/events/president/transcripts/24432 (Дата обращения: 20.11.2021).

[218] Там же.

Создание системы правовых, организационных и научно-технологических условий для обеспечения государственной безопасности России в сфере информации выступает в качестве одной из задач стратегического развития страны в XXI в. В частности, данное направление государственной политики было отражено в «Стратегии развития информационного общества в Российской Федерации», утвержденной 7 февраля 2008 г.[219] В Стратегии была отражена роль информационных и телекоммуникационных технологий как инструмента обеспечения безопасности государства и укрепления обороноспособности страны. Создание в России единого информационного пространства рассматривалось в качестве одного из условий обеспечения национальной безопасности. Одним из направлений реализации Стратегии являлось противодействие применению информационных и телекоммуникационных технологий в целях, угрожающих национальным интересам России. В том числе Стратегия предполагала решение задач в сфере обеспечения безопасности в процессе функционирования информационно-коммуникационных систем и инфраструктуры, включая стратегические объекты, технологические структуры повышенной опасности, информационные системы компаний и др.[220] Предусматривалось формирование единой технологической системы защиты, органов государственного управления и спецслужб от угроз деструктивного применения информационно-телекоммуникационных технологий. В Стратегии были поставлены также задачи обеспечения конфиденциальности частной жизни россиян, защиты личной и семейной тайны, противодействия пропаганде идей терроризма, экстремизма, насилия[221].

В данном контексте в 2008 – 2015 гг. развивались механизмы защиты безопасности российских информационных ресурсов в глобальных

[219] Стратегия развития информационного общества в Российской Федерации от 7 февраля 2008 г. № Пр-212. URL: https://digital.gov.ru/uploaded/files/strategiya_razvitiya_inf_obschestva_1.pdf (Дата обращения: 20.11.2021).
[220] Там же.
[221] Там же.

цифровых коммуникациях. В частности, был утвержден определенный порядок выхода во Всемирную сеть информационных систем и компьютеров, используемых для хранения и передачи данных, составляющих государственную, либо служебную тайну только в случае необходимости и при обязательной защите информации специальными, в том числе криптографическими средствами, прошедшими сертификацию ФСБ РФ и ФСТЭК[222].

В начале 2009 г. была проведена работа по формированию межведомственных рабочих групп по реализации «Стратегии развития информационного общества» в России, в том числе были созданы «Межведомственная группа по использованию информационно-коммуникационных технологий по обеспечению безопасности жизнедеятельности населения» под руководством главы МЧС С.К. Шойгу и «Межведомственная группа по вопросам противодействия использованию потенциала информационно-коммуникационных технологий для нанесения ущерба национальным интересам России» под руководством директора ФСБ России А.В. Бортникова[223].

12 февраля 2009 г. состоялось первое заседание Совета по развитию информационного общества, в ходе которого обсуждалась необходимость оперативного преодоления существенного на тот момент разрыва в уровне информации Россией и ведущих стран мира. Президент России в ходе заседания поставил перед руководителями министерств и ведомств задачу принять решительные меры по ускорению темпов создания электронного

---

[222] Указ Президента РФ от 17.03.2008 № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»

[223] Перечень межведомственных рабочих групп по основным направлениям реализации Стратегии информационного общества в Российской Федерации // Информационное общество. 2009. № 4-5. С. 24-31.

правительства и цифровизации социального сектора[224]. Предметом обсуждения в данном контексте стал вопрос обеспечения баланса между открытостью и безопасностью цифровых коммуникаций. Так, И.Ю. Юргенс, председатель правления Института современного развития (ИНСОР), высказался в пользу большей межведомственной открытости в целях активизации внутренних электронных коммуникаций и предлагал «пойти на определённый риск сотрудничества с иностранцами» в целях стимулирования деятельности в России международного бизнеса в сфере высоких технологий. И.Ю. Юргенсом был также поставлен вопрос о проблеме защиты персональных данных, возникающих при использовании международных платежных систем и стратегической задаче преодоления монополии США в сфере суперкомпьютеров, в частности, при использовании кредитных карт, данные о которых поступают в американские электронные базы данных, причем решение данной сложной проблемы находится «на стыке МИДа, спецслужб, гражданского общества»[225].

Следует отметить, что тема информационной безопасности в финансовой сфере на фоне успешного продвижения российского банковского сектора в систему глобальных электронных коммуникаций, утверждения в деятельности российских банков мировых технологических и деловых стандартов, находилась в центре внимания отечественного бизнеса, в том числе на региональном уровне. Так, в 2009 г. по предложению Главного управления безопасности и защиты информации Банка России в Республике Башкортостан была проведена конференция, посвященная проблемам обеспечения информационной безопасности банков. Организатором мероприятия, участниками которого стали более 170 специалистов в области информационной безопасности и руководящих работников банков, выступил Национальный Банк Республики Башкортостан

[224] Стенографический отчет о заседании Совета по развитию информационного общества. 12 февраля 2009 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/events/president/transcripts/3161 (Дата обращения: 21.11.2021)
[225] Там же.

под руководством Р.Х. Марданова. Проведение конференции вызвало большой интерес в российских банковских кругах и органах финансового регулирования, показав востребованность подобных встреч[226].

На II конференции «Информационная безопасность банков» в центре внимания собравшихся были такие вопросы как внедрение в кредитных организациях Стандарта информационной безопасности Банка России и совершенствование механизмов защиты базы персональных данных в соответствии с международными стандартами и положениями Федерального закона «О персональных данных» в редакции от 27 декабря 2009 г.[227] Необходимо отметить, что обеспечение защиты персональной информации было в этот период одной из центральных проблем в работе отечественных кредитных организаций, большинство которых не было готово с технологической и кадровой точки зрения к деятельности в соответствии с новыми нормативными требованиями. В связи с этим обстоятельством Государственная Дума РФ по настоянию банковского сообщества дважды (в декабре 2009 и в декабре 2010 г) принимала решение об отсрочке приведения в соответствие со стандартами информационных систем персональных данных (ИСПД). Контрольная дата в итоге была перенесена на 1 июля 2011 г.[228]

В течение последующих лет в живописном уголке Башкирии, на озере Банное, известном также как Якты-Куль («Светлое озеро»), ежегодно проводится Уральский форум информационной безопасности. Форум является ключевым отраслевым мероприятием в области безопасности, его главным организатором выступает Банк России при поддержке и участии таких структур как Совет Федерации Государственной Думы РФ,

---

[226] История Уральского форума // Уральский форум «Информационная безопасность финансовой сферы» [Электронный ресурс] URL: https://ib-bank.ru/uf2020/

[227] Безопасность банков выходит на первый план [Электронный ресурс] // Информационный портал «UFA1.ru». 17 февраля 2010 г. URL: https://ufa1.ru/text/business/2010/02/17/54643361/

[228] См.: Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // СЗ РФ, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, 4196; № 49, ст. 6409; № 52, ст. 6974; 2011, № 23, ст. 3263.

Правительство РФ, Министерство цифрового развития, связи и массовых коммуникации (Минцифры) России, ФСБ, Роскомнадзор и других заинтересованных ведомств. Уральский форум в течение 2010-х гг. выступал как площадка диалога между органами исполнительной власти и специалистами в области IT, воздействуя на процесс развития государственной политики информационной безопасности в финансовом секторе.

Одним из наиболее представительных стал московский «Инфофорум – 2009», участники которого обсуждали, в частности, актуальные вопросы противодействия киберпреступности, информационному терроризму и другим сетевым угрозам, проблему информационных войн и др. С докладами на форуме выступали министр Минкомсвязи И.О. Щеголев и его заместитель А.А. Солдатов, заместитель начальника Генштаба Вооруженных сил России А.Г. Бурутин, начальник Бюро специальных технических мероприятий МВД РФ Б.Н. Мирошников и другие представители властных структур, деятельность которых непосредственно связна с реализацией государственной политики информационной безопасности, защитой государственной и служенной тайны[229]. Одним из главных предметов дискуссий стала проблема авторизации пользователей Интернета, в подходе к которой со стороны правоохранительных ведомств и сетевого сообщества выявились довольно существенные различия. Так, представители правоохранительных структур рассматривали анонимность в сети как серьезное препятствие для борьбы с киберпреступностью; при этом персональные пользователи и коммерческие предприятия выдвигали на первый план свои права на конфиденциальность, защиту частных и коммерческих данных[230]. В этой связи возрастала актуальность утверждения

[229] Инфофорум-2009. [Электронный ресурс] // CNews: Интернет издание о высоких технологиях. 5 февраля 2009 г. URL: https://www.cnews.ru/articles/infoforum_2009_anonimnost_pugaet_chinovnikov/2 (Дата обращения: 22.11.2021)
[230] Там же.

правовых норм защиты персональных данных и совершенствования цифровых технологий в данной сфере.

В конце сентября – начале октября 2009 г. в Москве в Экспоцентре на Красной Пресне успешно прошла очередная выставка Infosecurity Russia, на церемонии открытия которой звучали слова о необходимости дальнейшей координации усилий государственных институтов и бизнеса в сфере информационной безопасности, которая в начале XXI в. стала одним из главных вызовов глобальному сообществу. На выставке были представлены достижения ведущих компаний России, Великобритании, США, Китая, разрабатывающих технологии защиты информации – Agilent Technologies, Eset, Huawei Symantec Technologies Co., Kaspersky Lab, Microsoft и др.[231] Большой интерес IT-специалистов и представителей бизнеса вызвала научно-практическая конференция, многочисленные технические семинары и круглые столы, проводившиеся под эгидой выставки. Их тематика отражала спектр ключевых проблем в развитии отрасли информационной безопасности в глобальном формате: «Интернет как поле конкурентных битв», «Человеческий фактор и информационная безопасность (антропогенные угрозы ИБ)» и др.[232] В работе конференции приняли участие представители Совета безопасности России, руководящие работники и специалисты Банка России, МВД РФ, Минкомсвязи РФ, и других министерств и ведомств.

В 2010-е гг. продолжалась реализация стратегического курса руководства России на инновационное развитие экономики и социальной инфраструктуры страны, частью которого стала дальнейшая информатизация системы государственного управления[233].

---

[231] В Москве прошла выставка Infosecurity Russia 2009 [Электронный ресурс] // Газета InfoSecurity. 1 октября 2009 г. URL: https://www.infosecurity.ru/_gazeta/content/091002/n_091001a.shtml (Дата обращения: 21.11.2021).

[232] Там же.

[233] *Алферова Е.В., Бачило И.Л.* Информационные технологии: инновации в государственном управлении. М.: ИНИОН РАН, 2016.

Положения «Стратегии развития информационного общества в Российской Федерации» составили основу для разработки и реализации Госпрограммы «Информационное общество», которая явилась уже в новых социально-экономических и технологических условиях продолжением ФЦП «Электронная Россия». Госпрограмма «Информационное общество» осуществлялась в два этапа в течение периода 2010 – 2020 гг.[234] В процессе ее реализации велась работа в области модернизации системы правового регулирования деятельности органов государственного управления в условиях информационного общества. Так, важным компонентом модернизации правовой базы цифрового администрирования стало принятие Федерального закона «Об электронной подписи» (от 06.04.2011 № 63-ФЗ)[235]. На втором этапе реализации госпрограммы «Информационное общество», (с 2014 г.) в нее были интегрированы целевые подпрограммы, в том числе подпрограмма «Безопасность в информационном обществе», направленная на решение задач в области надзора и контроля за соблюдением законности в информационном пространстве, выявления информационно-технологических угроз национальным интересам России, противодействия информационному экстремизму и терроризму, развития грид-технологий (специальных программ, позволяющих объединять ресурсы различных типов – базы данных, компьютеры, деловые сети и др.). Исполнителями подпрограммы являлись Роскомнадзор, Минкомсвязь, ФСБ России и Роспечать[236].

К началу второго десятилетия XXI в. был подготовлен новый Федеральный закон «О безопасности», принятый 28 декабря 2010 г. и в последующий период, ставший концептуальной основой для развития различных отраслей государственного управления и технологий, связанных с

---

[234] Государственная программа «Информационное общество (2011-2020 г.). Распоряжение Правительства РФ от 20.10.2010 г. № 1815-р // СЗ РФ. 2010. № 46. Ст. 6026; Государственная программа Информационное общество (2011-2020 г.). Постановление Правительства РФ № 313 от 15.04.2014 // СЗ РФ. 2014. № 18. Ч. II. Ст. 2159.

[235] *Талапина Э.В.* Государственное управление в информационном обществе (правовой аспект): монография. Москва: Юриспруденция, 2015. 214 с.

[236] *Кравчук Н.Ю., Юрков Д.В.* Государственные информационные ресурсы Российской Федерации. С.120.

задачами защиты информационной безопасности, в том числе в рамках международного диалога по вопросам развития информационных коммуникаций. В этот период вопросы обеспечения международной информационной безопасности приобретают характер самостоятельного направления государственной политики России, что нашло свое выражение в утвержденных 24 июля 2013 г. «Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». В данном документе отмечалось, что информационные и коммуникационные технологии могут быть применены в военно-политических, а также в террористических в целях вопреки нормам международного права, могут выступать в качестве механизма вмешательства во внутренние дела суверенных стран, использоваться для совершения киберпреступлений и других деструктивных действий, что является основной угрозой в сфере международной информационной безопасности.[237]

Информационные технологии начала XXI в. создали принципиально новые условия для социализации, личностного развития, профессиональной деятельности пользователей Интернета, выступали важнейшим стимулом экономического роста, внедрения новых постиндустриальных технологий и т.п. Вместе с тем, по оценкам большинства ведущих специалистов, переход глобальной информатизации на новый уровень технологического и институционального развития оказывал противоречивое воздействие на человечество, выдвигая на первый план вопросы информационной безопасности. Успешное продвижение России по пути информатизации неизбежно актуализировало и вопросы защиты общества от возникающих в

[237] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года [Электронный ресурс]. // Институт проблем информационной безопасности. Официальный сайт. URL: https://www.iisi.msu.ru/Docs/article43/

этой связи проблем[238]. В то же время стремительное развитие цифровых технологий и рост их общедоступности многократно повышал уровень угроз и рисков, существующих в киберпространстве. Эти риски были связаны с хакерскими атаками на бизнес и государственные организации, с доступом детей и подростков к деструктивным сайтам, продвигающим культ жестокости, терроризма, порнографии, самоубийств и т.п. Масштабы данных явлений в Глобальной сети, в том числе в Рунете, ставили перед обществом и государственными институтами целый спектр моральных и юридических проблем.

В XXI в., участвуя в противодействии угрозам международной информационной безопасности в рамках программ ООН, на основе двусторонних соглашений и договоров о сотрудничества в системах содружеств СНГ, ШОС, БРИКС, АТЭС и других объединений, Россия уделяет постоянное внимание вопросам регулирования внутреннего сетевого пространства, диалогу с сообществом пользователей Интернета и цифровым бизнесом[239].

При этом во второй половине 2010-х гг. в условиях сложной геополитической обстановки обостряется информационное противостояние в мировых СМИ и Интернете, фактически поставившее Россию в ситуацию информационной войны. На фоне развития политико-пропагандистской составляющей международной напряженности приобрели особую актуальность и вопросы защиты в международном пространстве информационной безопасности государства и бизнеса России, поскольку снизился уровень доверия к международным интернет-компаниям, поставщикам программного обеспечения, сетевым сервисам, созданным в странах НАТО. Одной из серьезных потенциальных угроз является создание

---

[238] *Прончев Г.Б., Лонцов В.В., Монахов Д.Н., Монахова Г.А.* Проблемы безопасности информационного общества современной России. МГУ им. М.В. Ломоносова, социологический факультет. М.: Экон-Информ, 2014. 215 с.

[239] *Рыдченко К.Д.* «Моральный кодекс» пользователя Интернет и государственная цензура киберпространства: некоторые вопросы законодательного регулирования // Мониторинг правоприменения. 2012. № 3. С. 40-44.

ложных цифровых аватаров учреждений и персоналий, которые могут использоваться в ходе информационных войн[240].

В этой связи российским руководством осуществлялись меры по укреплению системы информационной безопасности страны. Так, во второй половине 2010-х гг. были предприняты дополнительные меры по защите персональных данных россиян: с 1 сентября 2016 г. провайдеры почтовых и социальных сетей и другие цифровые сервисы обязаны хранить исключительно на серверах, созданных на территории России[241].

В 2016 – 2021 гг. российским руководством были модернизированы концептуальные подходы к задачам информационной безопасности и развитию информационного общества, зафиксированные в нормативно-правовых документах[242]. В том числе новая Доктрина информационной безопасности (2016 г.) отражала изменившуюся международную ситуацию и стремление России к созданию системы стабильных и неконфликтных отношений в информационном пространстве[243].

Повышенное внимание в этот период уделяется противодействию внешним угрозам информационной безопасности государства и общества России. 18 июня 2019 г. в Уфе состоялась 10-я Международная встреча высоких представителей, курирующих вопросы безопасности. Директор Службы внешней разведки РФ С.Е. Нарышкин в своем выступлении на данном мероприятии особо подчеркнул растущее значение фактора

---

[240] *Федорченко С.Н.* Феномен искусственного интеллекта. Журнал политических исследований. 2020. Т. 4. № 2. С. 51.

[241] Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях».

[242] Указ Президента РФ от 5 декабря 2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ Российской Федерации. 2016. № 50. Ст. 7074; Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901; Федеральный закон от 26 июля .2017 № 187-ФЗ. «О безопасности критической информационной инфраструктуры Российской Федерации» и др.

[243] С учетом новых реалий: В.В. Путин утвердил Доктрину информбезопасности России [Электронный ресурс] // РИА Новости. 6 декабря 2016 г. URL: https://ria.ru/20161206/1482970311.html (Дата обращения: 2211.2021).

информационной глобализации и интеграции на характер современных «гибридных угроз», отметив, в частности, что «речь идет о создании универсального алгоритма проведения тайных акций влияния в непрерывном режиме и в глобальных масштабах» с использованием сетевых коммуникаций[244]. С.Е. Нарышкин говорил также о превращении киберпространства в «самостоятельную операционную среду» с собственной виртуальной экономикой, криптовалютами и криминальным «подпольем», что содержит потенциал серьезных угроз национальной безопасности. При этом особую тревогу российских спецслужб вызывает стремление США и других стран НАТО использовать киберпространство как поле «гибридной» войны[245].

2 июля 2021 г. Президентом России В.В. Путиным была утверждена новая версия Стратегии национальной безопасности Российской Федерации, в тексте которой информационная безопасность впервые стала рассматриваться как один стратегических приоритетов государственной политики. Основанием для данного подхода явился рост практики деструктивного использования информационно-коммуникативных технологий в глобальном международном поле, в том числе для вмешательства во внутренние дела независимых государств, подрыва их национального суверенитета и экономики. В Стратегии отмечалось также увеличение интенсивности кибератак на информационные ресурсы России, активизация иностранных спецслужб в российском информационном пространстве, в том числе в целях поиска средств для выведения из строя объектов критической информационной инфраструктуры России (КИИ). Кроме того, возрастают масштабы внедрения в российский сегмент

---

[244] *Нарышкин С.Е.* Об обеспечении национальной безопасности и устойчивого социально-экономического развития государств в условиях роста «гибридных» угроз: Выступление на 10-й международной встрече высоких представителей, курирующих вопросы безопасности, на тему «», Уфа, 18 июня 2019 г. [Электронный ресурс] // МИД России. Официальный сайт. 28 июня 2019 г. URL: https://www.mid.ru/foreign_policy/international_safety/regprla/-/asset_publisher/YCxLFJnKuD1W/content/id/3704728 (Дата обращения: 23.11.2021)

[245] Там же.

Интернета различного рода дезинформации и асоциального контента (призывы к терроризму, массовым беспорядкам и т.д.), создающего угрозу социальной стабильности и правопорядку в стране, причем массированному воздействию такого рода подвергается российская молодежь[246].

В связи с этим в Стратегии поставлена цель укрепления суверенитета России в глобальном информационном пространстве путем формирования безопасной среды информационного обмена, обеспечения высокого уровня защищенности и устойчивости информационно-технологической инфраструктуры страны, эффективного выявления и предупреждения угроз национальной информационной безопасности, в том числе пресечения действий преступных сообществ, террористических и экстремистских организаций, иностранных спецслужб и разведок. В Стратегии ставятся также задачи укрепления механизмов защиты государственной и служебной тайны, персональных данных и другой информации ограниченного пользования. Ключевое направление обеспечения национальной информационной безопасности авторы Стратегии видят в преодолении критической зависимости России от импорта высоких технологий через внедрение передовых отечественных разработок и развитие на территории страны высокотехнологичного производства цифровой техники и программного обеспечения, общей цифровизации российской экономики[247].

Необходимо отметить, что меры по обеспечению информационной безопасности в Российской Федерации в 2010-е - 2022 гг., включая запрет экстремистской пропаганды и соответствующий контроль за сетевым контентом, осуществлялись в рамках демократических правовых норм, без введения какой-либо политической цензуры пользовательского Рунета[248].

---

[246] Владимир Путин включил информбезопасность в число приоритетов Стратегии национальной безопасности России [Электронный ресурс]. // CNews: Интернет издание о высоких технологиях. 5 июля 2021 г. URL: https://safe.cnews.ru/news/top/2021-07-05_putin_vklyuchil_informbezopasnost

[247] Там же.

[248] *Федорченко С.Н.* Сетевая легитимация политических режимов: теория и технологии. М.: Московский государственный областной университет. 2018. С.75.

Важную роль в ограждении российского общества от информационных рисков играет социальная ответственность отечественных блогеров и представителей СМИ[249].

Таким образом, формирование концептуальных и правовых основ государственной политики России в области информационной безопасности в течение периода 1990-х – 2010-х гг. развивалась в общем русле российских реформ, пройдя через ряд этапов. В течение первой половины 1990-х гг. в России осуществляется строительства новой модели взаимодействия государства и общества в информационной сфере и создание основ правового регулирования вопросов национальной безопасности в соответствии с принципами демократической государственности и потребностями рыночной экономики

Во второй половине 1990-х –2000-е гг. под влиянием процессов глобальной информатизации, распространения цифровых технологий в государственном управлении, коммуникационных системах, частной жизни граждан России, проводится дальнейшая модернизация нормативно-правовых и организационных основ государственной политики в области информационной безопасности при активном участии российского IT-сообщества.

В 2010-е гг. существенно возрастает роль геополитического фактора в определении стратегических приоритетов информационной безопасности России, создаются механизмы защиты государственных институтов и всего российского общества от внешних информационных угроз.

Значительный комплекс мероприятий, направленных на решение задач в области информационной безопасности личности, общества и государства был осуществлен в 2000 – 2010-х гг. министерствами и ведомствами России, научно-экспертными центрами и общественными организациями, что будет показано в следующих главах диссертации.

---

[249] Там же.

ГЛАВА II. ИНСТИТУЦИОНАЛИЗАЦИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ

2.1. Государственные и коммерческие институты информационной безопасности России в 1990-е гг.

В течение 1990-х гг. институционализация системы информационной безопасности России происходила в рамках процесса общей трансформации правового пространства страны, органов законодательной и исполнительной власти, хозяйственно-экономической сферы, а также в условиях становления нового общественного сознания.

Как отмечают многие авторы, изучающие тему информационной безопасности Российской Федерации, в начальный период демократических реформ данная отрасль государственного управления не воспринималась руководством страны как приоритетная[250]. Это было обусловлено спецификой перехода к рынку, когда в центре внимания правительства России находились, прежде всего, вопросы экономики, а бюджетные расходы на оборону и работу спецслужб сокращались. На фоне сближения России с Западом много говорилось об окончании «холодной войны», а международный терроризм и киберпреступность на тот момент еще не проявили себя как глобальная угроза. Соответственно, тема информационной безопасности выглядела неактуальной, особенно в глазах либеральной общественности и СМИ. В России начала 1990-х гг. возник общественный запрос на создание принципиально новой системы национальной безопасности, включая ее информационную составляющую, которая не ассоциировалась бы с КГБ и политической цензурой эпохи СССР. В соответствии с данным подходом функции обеспечения национальной безопасности России были распределены между несколькими ведомствами, и образован коллегиальный орган, определяющий государственную политику в

[250] *Меньшиков П.В.* Эволюция государственной информационной политики в России // Международные коммуникации. 2017. № 4. С. 3; *Медовкина Л.Ю.* Политика Президента Российской Федерации Б.Н. Ельцина в области информационной безопасности // Научные ведомости Белгородского государственного университета. Серия: История. Политология. 2019. Т. 46. № 1. С. 178 и др.

данной сфере в целом, включая вопросы информационной безопасности государства, бизнеса и граждан. Первый шаг в построении новой системы государственной безопасности был предпринят еще в период существования СССР, когда в рамках изменений Конституции СССР в соответствии с Законом от 26 декабря 1990 г. был учрежден Совет Безопасности СССР, ставший прообразом аналогичной структуры в реформируемой России. В Законе «О Президенте РСФСР» от 24 апреля 1991 г. упоминался Совет безопасности, главой которой является президент, а порядок деятельности определяется законодательством республики[251]. В мае того же года статус Совета Безопасности в качестве конституционного органа был закреплен в Конституции РСФСР.

Осенью 1990 г. был учрежден независимый от союзного ведомства «Государственный комитет РСФСР по общественной безопасности и взаимодействию с Министерством обороны СССР и КГБ СССР», который в январе 1991 г. был преобразован в Госкомитет РСФСР по обороне и безопасности (КГБ РСФСР)[252]. В рамках реформирования системы государственной безопасности постсоветской России были основаны новые ведомства и подразделения в действующих организациях, функцией которых было обеспечение информационной безопасности в различных отраслях государственного управления, обороны, экономической и социальной инфраструктуры. В течение 1991 года были образованы: Агентство федеральной безопасности (на базе КГБ РСФСР), Служба внешней разведки, Государственное управление охраны; имевшие в рамках своих компетенций функции, связанные с вопросами информационной безопасности, а также орган, который непосредственно действовал в информационной сфере, –

---

[251] Закон РСФСР 24 апреля 1991 года № 1098-1 «О Президенте РСФСР» // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1991. № 17. С. 512.

[252] Постановление Совета министров РСФСР от 31 января 1991 г. № 66 «О преобразовании Государственного комитета РСФСР по общественной безопасности и взаимодействию с Министерством обороны СССР и КГБ СССР в Государственный комитет РСФСР по обороне и безопасности» [Электронный ресурс] URL: https://docs.cntd.ru/document/901604496 (Дата обращения: 18.01.2022)

Федеральное агентство правительственной связи и информации (ФАПСИ). В течение некоторого времени существовало объединенное Министерство безопасности и внутренних дел (МБВД) РСФСР, в 1992 г. разделенное на два самостоятельных ведомства – МВД и Министерство безопасности РФ, в структуре которого до декабря 1993 г. действовал ряд спецслужб, включая ФАПСИ[253]. В 1995 – 1996 гг. реформа отечественных органов безопасности была в целом завершена. Ее результатом явилось создание в России комплекса специальных ведомств, действующих под контролем Совета безопасности при Президенте РФ – Федеральной службы безопасности (ФСБ), Федеральной службы охраны (ФСО), ФАПСИ и Службы внешней разведки (СВР)[254].

В начале 1990-х гг. руководство России уделяет большое внимание внедрению в системе реформируемых спецслужб новых концептуальных подходов и направлений деятельности, соответствующих требованиям демократической государственности и рыночной экономики. 18 июля 1991 г. (на шестой день после своего избрания на пост президента РСФСР) Б.Н. Ельцин провел совещание с руководством республиканского Комитета по обороне и безопасности, в ходе которого, в частности, подчеркнул, что Комитет должен быть превращен в «важный элемент демократического государства»[255]. На встрече была также озвучена идея нового органа – Совета безопасности при Президенте России, определяющего на коллегиальной основе, в том числе с участием представителей специальных органов госбезопасности, стратегию политического курса страны[256]. Такая организация руководства государственной политикой в области безопасности была типологически наиболее близка к модели Совета безопасности США,

---

[253] *Есипов В.А.* Реформы органов госбезопасности в России и государствах бывшего СССР в 1990-е годы и мировая система их организации // Образование и наука в России и за рубежом. 2019. №2 (Vol. 50). С.444-446.
[254]. Там же.
[255] Архив Президента РФ. Ф. 6. Оп. 1. Д. 113. Л. 4.
[256] Там же. С. 25.

что соответствовало курсу постсоветской России на внедрение западных форм государственно-общественного устройства.

По мере развития в России рыночных отношений формируются представления о ценности коммерческой тайны и, соответственно, о необходимости обеспечения защиты экономической информации, что находит отражение в развитии государственной политики информационной безопасности. Предложенная Б.Н. Ельциным концепция развития органов государственной безопасности РСФСР, включала (помимо традиционной разведки и контрразведки) выполнение ими функции по обеспечению прав и свобод граждан и содействие проведению экономических реформ. «Новое время требует совершенно иначе оценить роль органов безопасности в экономике», – говорится в проекте текста выступления российского лидера перед сотрудниками Комитета безопасности РСФСР. Примечательно, что рядом имеется приписка рукой Б.Н. Ельцина: «Находить новые формы внедрения в совмест[ные] коммер[ческие] орг[анизации] для зашиты экон[омических] секретов»[257].

26 декабря 1991 г. состоялась встреча Президента РСФСР Б.Н. Ельцина с руководством Министерства безопасности и внутренних дел (МБВД) РСФСР и Агентства федеральной безопасности (АФБ) РСФСР, в которой приняли участие 50 человек, включая лиц, ответственных за сбор и зашиту информации: начальник Главного управления контрразведки МБВД генерал-майор Ю.Е. Булыгин и его заместители, начальник Главного управления контрразведки АФБ генерал-майор Ю.В. Чичелов, начальник Информационно-аналитического центра МБВД В.А. Рубакин и др. Среди подготовительных документов данного мероприятия сохранилась справка «Основные направления деятельности органов государственной безопасности МБВД РСФСР», которая показывает роль и место информационной работы в функционировании системы госбезопасности России в период ее реформирования. Так, контрразведывательная

[257] Архив Президента РФ. Ф. 6. Оп. 1. Д. 113. Л. 9.

деятельность органов МБВД была направлена на борьбу с иностранным шпионажем и государственной изменой во всех ее формах, соответственно и с передачей иностранным разведслужбам информации, имеющей значение для национальной безопасности страны. В справке было дано определение разведывательной деятельности МБВД как работы, проводящейся в целях «добывания приоритетной информации политического, экономического, научно-технического, военного и оперативного характера»[258]. В перечень функций органов безопасности МБВД входило также обеспечение структур власти и управления РСФСР информацией, необходимой для решения задач как непосредственно в сфере безопасности страны, так и связанной с проведением экономических реформ, строительством оборонного комплекса, научно-техническим развитием, реализацией ключевых направлений внутренней и внешней политики[259].

В Законе РСФСР от 5 марта 1992 г. «О безопасности» и в Указе Президента России Б.Н. Ельцина от 3 июня 1992 г. были прописаны функции, полномочия и принципы формирования Совета безопасности РСФСР, включая рассмотрение и подготовку решений Президента России по вопросам государственной информационной безопасности[260].

Архивные документы о работе Совета безопасности РФ в течение 1990-х гг. показывают, что на заседаниях Совета в этот период обсуждались преимущественно вопросы обеспечения правопорядка и экономической безопасности страны, в том числе задачи борьбы с организованной преступностью, коррупцией, вывозом капиталов[261]. Тема информационной безопасности поднималась в основном в контексте преодоления кризисных явлений в экономике. Так, 19 января 1994 г., выступая на заседании Совета

---

[258] Архив Президента РФ. Ф. 6. Оп. 1. Д. 113. Л. 34.
[259] Там же. Л.34-35.
[260] Положение о Совете Безопасности Российской Федерации: утверждено Указом Президента Российской Федерации от 3 июня 1992 г. № 547 // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации,1992, № 24, ст. 1323.
[261] Архив Президента РФ. Ф. 6. Оп. 1. Д. 111. Л. 34-40.

безопасности, Б.Н. Ельцин призвал учитывать хозяйственное значение военно-научных разработок в области новых энергий, материалов, технологий и в связи с этим пересмотреть законы «О безопасности», «Об обороне», «О государственной тайне» и др. «Прежде чем засекретить ту или иную разработку, уважаемые военные, обратите внимание, а как она может быть применима в народном хозяйстве», – подчеркнул он[262].

Целый ряд изменений был в 1990-е гг. предпринят в системе государственного регулирования систем связи. Реформы в данном секторе были направлены, с одной стороны, на развитие новых технологий и инфраструктуры связи, создание механизмов государственного контроля, обеспечивавшие технологическую стандартизацию и добросовестную конкуренцию на быстро развивавшемся рынке телекоммуникаций, с другой – на решение вопросов в области информационной безопасности. Особое внимание уделялось обеспечению информационной защиты правительственной связи. До 1991 г. данная задача входила в зону ответственности специализированных подразделений КГБ СССР, которые обеспечивали функционирование систем правительственной связи, шифрование и дешифрование данных, а также радиоэлектронную разведку. После упразднения КГБ СССР эти структуры были включены в состав Комитета правительственной связи при Президенте РСФСР, объединившего ресурсы бывшего 8-го (шифрование и дешифрование) и 16-го (электронная разведка и радиоперехват) Главных управлений КГБ СССР и Государственного информационно-вычислительного центра при Государственной комиссии по чрезвычайным ситуациям[263]. Подразделение по обслуживанию и защите безопасности президентской связи с 1992 г. действовало в структуре Главного управления охраны РФ.

---

[262] Архив Президента РФ. Ф. 6. Оп. 1. Д. 111. Л. 45.

[263] *Полонский И.* День ФАПСИ (1991-2003). Слово о правительственной связи [Электронный ресурс] // Военное обозрение. 24 декабря 2015 г. URL: https://topwar.ru/88409-den-fapsi-1991-2003-slovo-o-pravitelstvennoy-svyazi.html (Дата обращения: 20.01.2022)

24 декабря 1991 г. Комитет правительственной связи был преобразован в Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ), о деятельности которого в области сертификации и лицензирования технических средств накопления и передачи информации уже упоминалось выше. Руководителем Комитета правительственной связи РФ, а затем ФАПСИ был назначен заместитель начальника Управления войск правительственной связи КГБ СССР генерал-лейтенант А.В. Старовойтов. В субъектах Россиикой Федерации была создана система Региональных информационно-аналитических центров (РИАЦ) ФАПСИ.

Создание ФАПСИ имело важнейшее значение для реализации государственной политики информационной безопасности в постсоветской России, поскольку позволило сохранить инфраструктурную, технологическую и кадровую основу для дальнейшего развития данного сектора системы национальной безопасности, выросшего «в мощную специальную службу, которая на протяжении 1990-х годов постоянно развивалась и совершенствовалась, оставаясь едва ли не самой засекреченной из российских силовых структур»[264].

Специалистами Главного управления информационных ресурсов ФАПСИ (ГУИР ФАПСИ) осуществлялись задачи в области безопасного информационного и информационно-технологического обеспечения деятельности органов государственной власти и управления России, включая Совет безопасности РФ и ФСБ[265]. По лицензиям ФАПСИ действовало более 150 организаций и предприятий: НИИ, инновационные фирмы, специализированные научно-технические центры («Атлас», «Программные системы и технологии» и др.) вели разработку и установку защищенных телекоммуникационных сетей и цифровой межрегиональной связи (RSNET),

---

[264] *Полонский И.* День ФАПСИ (1991-2003). Слово о правительственной связи [Электронный ресурс] // Военное обозрение. 24 декабря 2015 г. URL: https://topwar.ru/88409-den-fapsi-1991-2003-slovo-o-pravitelstvennoy-svyazi.html (Дата обращения: 20.01.2022)

[265] Там же.

защищенных систем информационного обмена для МВД («Занавес») и Федеральной налоговой полиции (ИСИНПОЛ), сертифицированных средств защиты банковских систем – российских интеллектуальных карт (РИК), цифровой подписи, сетевых шифраторов и др.[266] Одним из ведущих предприятий по созданию средств информационной безопасности, работавших под эгидой ФАПСИ, является основанное в 1994 г. ЗАО «МО ПНИЭИ» (Московское отделение Пензенского научно-исследовательского электротехнического института)[267].

Научно-технологическая деятельность ФАПСИ была направлена на противодействие киберпреступности, резко возросшей в конце 1990-х гг. Так, через несанкционированный доступ к программам регистратора ценных бумаг «Крона Плюс» (Тверь) было похищено 5 млн. акций «Газпрома». В 1998 г. в Сибирском регионе злоумышленниками, изготовившими дубликаты незащищенных пластиковых карт, был нанесен серьезный ущерб платежной системе «Золотая корона». Прибор электронного шпионажа, установленный под видом устройства для защиты информации, был обнаружен группой ФАПСИ в кабинете одного из губернаторов[268] и т.п.

В данном контексте задачей ФАПСИ являлось утверждение высоких технологических стандартов на российском рынке специальной аппаратуры и программных средств защиты информации, соответствующих мировым стандартам. В государственных учреждениях и коммерческих структурах нередко использовались недостаточно эффективные системы информационной безопасности. Так, об одном из средств криптографической защиты, популярном в этот период у российских потребителей, говорилось, что специалисты ФАПСИ способны дешифровать его всего за 20 минут,

---

[266] *Горбачев В.С.* Для информационной безопасности в субъектах Федерации [Электронный ресурс] // Бизнес и безопасность в России. 2003. № 1. URL: https://fapsi2004.chat.ru/uvs/doc/ip_gorb.htm (Дата обращения: 18.01.2022)

[267] О компании [Электронный ресурс] // Сайт ЗАО «МО ПНИЭИ». URL: https://security.ru/default.php (Дата обращения: 18.01.2022)

[268] ФАПСИ и обеспечение региональной информационной безопасности [Электронный ресурс] URL: https://www.vrsystems.ru/stati/fapsi_i_obespechenie_regionalnoi_informacionnoi_bezopasnosti.htm (Дата обращения: 18.01.2022)

используя «бытовой персональный компьютер класса Pentium»[269]. Соответственно, осуществлявшееся ФАПСИ лицензирование фирм-производителей средств информационной безопасности становилось гарантией высокого качества их работы и способствовало в целом дальнейшему развитию отечественных цифровых технологий.

Одним из вновь созданных институтов информационной безопасности в России 1990-х гг. явилась Государственная техническая комиссия (Гостехкомиссия) России, учрежденная президентским указом от 5 января 1992 г. с целью «обеспечения национальной безопасности народов и территорий Российской Федерации в части приоритетов и защиты информации в области обороны, политики, экономики, науки, экологии, ресурсов и противодействия иностранным техническим разведкам»[270]. В пределах своей компетенции она выполняла руководящие функции по отношению к органам защиты информации, составляющей государственную и служебную тайну во всех сферах государственного управления, экономики, общественной жизни. Решения Гостехкомиссии являлись обязательными для всех учреждений и организаций России независимо от форм собственности. На Гостехкомиссию возлагалась задача проведения единой технической политики и координации деятельности по защите информации, имеющей значение с точки зрения национальной безопасности страны, от утечек, незаконного доступа, уничтожения, либо искажения в деструктивных целях.

Гостехкомиссия создавалась на базе Государственной технической комиссии СССР по противодействию иностранным разведкам и унаследовала ее основные штаты и организационные структуры. Возглавлявший Гостехкомиссию СССР с 1989 г. генерал армии Ю.А. Яшин был назначен исполняющим обязанности председателя Гостехкомиссии РФ.

---

[269] ФАПСИ и обеспечение региональной информационной безопасности [Электронный ресурс] URL: https://www.vrsystems.ru/stati/fapsi_i_obespechenie_regionalnoi_informacionnoi_bezopasnosti.htm (Дата обращения: 18.01.2022)

[270] Указ Президента РФ от 5 января 1992 г. № 9. «О создании Государственной технической комиссии при Президенте Российской Федерации» Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1992, № 3, ст. 109.

Его задачей стало преобразование узкоспециализированной военной структуры в орган безопасности общегосударственного значения. В течение месяца командой Юрия Яшина был подготовлен проект «Положения» о Государственной технической комиссии, в котором определялись ее главные задачи: защита информации в политической, экономической, научно-технической, военной и других сферах деятельности государства[271]. В число направлений работы Гостехкомиссии, по замыслу Ю.А. Яшина, входило обеспечение информационной безопасности ключевых компонентов оборонного комплекса: стратегических сил сдерживания, систем боевого управления, приоритетных вооружений, а также программ сокращения вооружений. Кроме того, Гостехкомиссия должна была осуществлять защиту всех видов государственной информации, в том числе коммерческой, на внутренних и внешних рынках и в банковских системах. Были подготовлены также проекты государственно-правовых и нормативных актов, регулирующих различные аспекты защиты информации в государственном секторе, бизнесе, частной жизни граждан, определен персональный состав Комиссии[272]. В согласовании материалов о деятельности Гостехкомиссии участвовали: Министерство безопасности РФ, МИД России, Министерство науки, высшей школы и технической политики РФ, министерства связи, юстиции, экономики и финансов, Вооруженные силы СНГ, Федеральное агентство правительственной связи и информации, Служба внешней разведки РФ и ряд других структур[273]. В том числе в группу экспертов по вопросу создания и деятельности Гостехкомиссии входил А.И. Ракитов, который, как уже отмечалось выше, явился одним из пионеров отечественной философии информатизации, а с 1991 г. занимал должность советника Президента России по вопросам научно-технологической политики и информации. Труд ученого «Философия компьютерной

[271] Архив Президента РФ. Ф. 6. Оп. 1. Д. 111. Л. 1.
[272]. Там же. Л. 2.
[273] Там же. Л. 4-5.

революции», вышедший в свет в 1991 г., стал одной из классических работ в области теории информационного общества в России[274].

11 февраля 1992 г. Ю.А. Яшин направил Б.Н. Ельцину служебную записку, в которой, в частности, отмечалось, что деятельность Гостехкомиссии опирается на принцип коллективного принятия решений по важнейшим вопросам защиты информации и новую модель управления государственной системой зашиты информации в Российской Федерации. Новизна подхода к регулированию и контролю государственных и коммерческих организаций в сфере информационной безопасности предполагала внедрение механизмов лицензирования и сертификации деятельности в области защиты информации[275].

Ю.А. Яшин предлагал сформировать аппарат Комиссии в составе до 235 человек, из них 155 военнослужащих. В аппарат и органы Комиссии предлагалось включать офицеров и представителей руководящего состава МВД, а также гражданских специалистов. Общая численность специальных центров и головной научной организации (6 управление ЦНИИ МО) должна была составить до 900 человек. Для обеспечения работы Гостехкомиссии создавались структуры по защите информации в органах власти и управления, в государственных учреждениях, на предприятиях. Ю.А. Яшин выдвинул также предложение о передаче Гостхкомиссии функции координации и контроля реализации продукции российского ВПК на мировом рынке, подчеркивая, что данная задача должна оставаться монополией государства[276]. Распоряжением Президента России от 18 января 1993 г. генерал Ю.А. Яшин был назначен председателем Государственной технической комиссии в статусе министра Российской Федерации, что обозначало и новый статус самой Гостехкомиссии[277]. Однако в последующие

---

[274] *Ракитов А.И.* Философия компьютерной революции. М.: Политиздат, 1991. 287 с.
[275] Архив Президента РФ. Ф. 6. Оп. 1. Д. 111. Л.1.
[276] Там же. Л. 2.
[277] Распоряжение Президента РФ В.В. Путина от 18.01.1993 г. № 41-рп «О председателе Государственной технической комиссии при Президенте Российской Федерации»

несколько лет формирование нормативной базы деятельности технологической защиты национальной информационной безопасности не осуществлялось. «Положению о Государственной технической комиссии при Президенте Российской Федерации» было утверждено только в 1999 г. Согласно данному документу, предельный штат Гостехкомиссии насчитывал 163 единицы, без учета персонала по охране и обслуживанию зданий, из которых до 136 человек могли составлять прикомандированные военнослужащие. При Гостехкомиссии России создавались инженерно-технические воинские формирования, в состав которых включалась головная научная организация, занимавшаяся вопросами защиты информации от технических разведок и утечек, а также соответствующие региональные структуры, которые образовывались на базе специальных центров Минобороны РФ, но исключались из состава Вооруженных сил и переходили в подчинение Гостехкомиссии[278].

Функции Гостехкомиссии в целом соответствовали предложениям, выдвигавшимся в начальный период ее организации. «Положение о Государственной технической комиссии» 1999 года подтвердило ее задачи в области межотраслевой координация и регулированию сферы обеспечения криптографической зашиты данных, представляющих собой государственную или служебную тайну, а также ответственность за осуществление единой научно-технической политики по разработке и использованию информационных технологических систем и устройств. Устанавливалось также, что в пределах своих полномочий Гостехкомиссия России выступает в качестве государственного заказчика по осуществлению научных исследований общесистемного характера в области технической

[Электронный ресурс]. URL: https://pravo.gov.ru/proxy/ips/?docbody=&nd=102021066 (Дата обращения: 15.01.2022)

[278] Указ Президента РФ В.В. Путина от 19 февраля 1999 г. № 212 «Вопросы Государственной технической комиссии при Президенте Российской Федерации» [Электронный ресурс]. URL: https://pravo.gov.ru/proxy/ips/?doc_itself=&collection=1&nd=201146 (Дата обращения: 15.01.2022)

защиты информации, по разработке и производству соответствующих технических средств и средств контроля их эффективности[279].

С марта 1994 г. руководитель Гостехкомиссии одновременно занимает пост председателя Межведомственной комиссии по охране государственной тайны Российской Федерации, создание которой было предусмотрено Законом «О государственной тайне» 1993 г., Комиссия представляла собой коллегиальную структуру, куда входили представители структур исполнительной власти, деятельность которых была непосредственно связана с задачами обеспечения информационной безопасности (ФСБ, МВД, ФАПСИ и др.), а также ведомств, наиболее значимых в контексте национальной безопасности (Администрации Президента РФ, МИД, ВПК, Минатома и др.). Фактически состав Комиссии совпадал с перечнем учреждений и организаций, руководители которых имеют полномочия по отнесению сведений к государственной тайне[280].

Согласно «Положению о Межведомственной комиссии», вышедшему в 1996 г., ее задачей являлась координация работы органов государственной власти и управления в области зашиты государственной тайны. В отличие от Гостехкомиссии она действовала не в технологической, а в нормативно-правовой и административной сфере: формировала перечни должностных лиц и учреждений, наделяемых полномочиями по отношению к государственной тайне, а также перечни сведений, относящихся к государственной тайне, рассматривала и представляла Президенту и Правительству РФ предложения в области правового регулирования и организационного обеспечения защиты государственной тайны[281].

---

[279] Указ Президента РФ В.В. Путина от 19 февраля 1999 г. № 212 «Вопросы Государственной технической комиссии при Президенте Российской Федерации» [Электронный ресурс]. URL: https://pravo.gov.ru/proxy/ips/?doc_itself=&collection=1&nd=201146 (Дата обращения: 15.01.2022)

[280] *Верютин В.Н.* Межведомственная комиссия по защите государственной тайны: структура и компетенция // Вестник Воронежского института МВД России. 2010. № 2. С. 23

[281] Там же.

Одновременно со строительством в реформируемой России обновленной системы федеральных и региональных органов информационной безопасности, в 1990-е годы происходило становление соответствующих отделов, департаментов и специальных служб в органах государственной власти и управления, министерствах и ведомствах – Государственной Думе РФ, Министерстве обороны, МВД, Министерстве иностранных дел, Банке России и др.

Процесс институционализации сферы информационной безопасности активно развивался в секторе крупного и среднего промышленного бизнеса и банковском деле, и других отраслях формирующейся рыночной экономики. Функции технологической защиты деловой переписки, различной коммерческой информации, инновационных разработок в наиболее крупных структурах выполняли специализированные группы, занимавшиеся компьютеризацией внутреннего и внешнего документооборота компаний. Задачи в сфере информационной безопасности решали сотрудники вычислительных центров, действовавших на ведущих предприятиях машиностроения, ВПК, энергетики[282].

По мере цифровизации бизнеса и государственного управления России в отечественном профессиональном сообществе IT-специалистов в самостоятельный вид деятельности вырастают системное администрирование и администрирование баз данных, которые также становятся институтами информационной безопасности[283].

Растущий спрос на новые технологии и организационные модели в сфере информационной безопасности явился стимулом для создания и успешной деятельности специализированных подразделений и коллективов

---

[282] *Абакумов Е.М., Кожевников Н.О. Петунин С.А.* В век высоких технологий: к юбилею отделения информационных технологий и информационной безопасности ФГУП «ВНИИА» / Под ред. Ю.Н. Бармакова. Всероссийский научно-исследовательский институт автоматики им. Н. Л. Духова. Москва: Кодекс, 2016. 204 с.

[283] *Зиндер Е.З.* Администратор базы данных - кто он? // Системы управления базами ланных. 1995. № 2; *Вьюкова Н.И., Галатенко В.А.* Информационная безопасность систем управления базами данных // Системы управления базами данных. 1996. № 1.

НИИ и независимых научно-технологических центров, осуществлявших подобные разработки на коммерческой основе. Примечательно, что целый ряд подобных фирм и компаний, созданных в 1990-е гг. продолжает действовать и в настоящее время. Так, в 1991 г. был основан Центр финансовых технологий – группа компаний, занимающихся разработкой программного обеспечения, IT-консалтингом и другими услугами в цифровой сфере для финансово-банковского сектора, в том числе вопросами защиты финансовой информации. Также с 1991 г. начинается история АО «Инфосистемы Джет», которая в 2020 г. вошла в пятерку компаний – лидеров российского рынка IT-услуг, включая сервисы по обеспечению информационной безопасности. С 1994 г. на отечественном рынке информационных технологий действует российский системный интегратор и разработчик IT-решений АО «АМТ-ГРУП», предоставляющий также услуги в области информационной безопасности сложных инфраструктурных и отраслевых систем и т.п.[284]

Следует отметить, что работа в области информационной безопасности в государственных структурах и в бизнесе изначально имела ряд отличий, особенно до начала внедрения модели «открытого правительства» и систем электронного администрирования. В 1990-е гг. приоритетным направлением обеспечения информационной безопасности в госсекторе была защита государственной и служебной тайны, что обеспечивалось применением криптографии и технологий противодействия незаконным проникновениям в базы данных. При этом для бизнеса вопрос информационной открытости и доступности для клиентов и партнеров был не менее значимым, чем конфиденциальность и защита коммерческой тайны. Соответственно, и технологические задачи по обеспечению информационной безопасности имели определенные различия. Так, один из ведущих российских специалистов в области технологий информационной безопасности В.А.

[284] *Пуха А.* Сервисная модель безопасности. 21 сентября 2015 г. [Электронный ресурс] URL: https://www.tadviser.ru/a/276297 (Дата обращения: 15.01.2022)

Галатенко выстраивал следующую последовательность аспектов информационной безопасности в бизнесе по мере значимости: «доступность (возможность за разумное время получить требуемую информационную услугу); целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения)» и лишь в последнюю очередь – «конфиденциальность (защита от несанкционированного прочтения)»[285].

Услуги в области защиты информации в постсоветской России начали оказывать частные предприятия охранно-детективного и юридического профиля. Кроме того, были основаны фонды безопасности, создававшиеся, главным образом, по инициативе бывших сотрудников спецслужб и правоохранительных ведомств. Так, например, в 1994 г. был образован Международный общественный фонд «Правопорядок-Центр», действующий и в настоящее время в России и ряде стран СНГ в целях укрепления законности, безопасности и общественного порядка, защиты собственности, законных прав и интересов граждан, государственных и общественных организаций и бизнеса. Под эгидой Фонда работает сеть организаций и предприятий, ряд которых занимается разработкой систем защиты и анализа информации[286].

Одним из ключевых компонентов общественной эволюции России в постсоветский период стали высокие темпы и масштабы развития СМИ, играющих огромную роль в формировании информационного пространства, в том числе в качестве института информационной безопасности. Данная функция СМИ определяется их деятельностью в области распространения значимых для государства и общества актуальных сведений в области

---

[285] *Галатенко В.А.* Информационная безопасность – основы [Электронный ресурс] // Системы управления базами данных. 1996. № 1. URL: https://www.osp.ru/dbms/1996/01/13031466 (Дата обращения: 15.01.2022)

[286] Профессиональное содействие в комплексном обеспечении безопасности законного предпринимательства и личности [Электронный ресурс] // Информационный портал «Общественные фонды и правозащитные организации». URL: https://publicfund.info/fondy-i-obedineniya/fondy-bezopasnosti/professional-noe-sodeistvie-v-kompleksnom-obespechenii-bezopasnosti-zakonnogo-predprinimatel-stva-i-lichnosti.html (Дата обращения: 15.01.2022)

политики, экономики, культуры, экологии, здравоохранения и др.[287] При этом острая конкуренция на рынке информационных услуг обусловила внимание телеканалов, редакций печатных и появляющихся электронных периодических изданий к созданию собственных структур защиты информации.

К институтам информационной безопасности могут быть также отнесены научно-аналитические и консалтинговые центры, занимавшиеся разработкой правовых и социальных аспектов защиты информации в бизнесе и частной жизни, а также проблематикой национальной и международной информационной безопасности – Центр международной безопасности ИМЭМО РАН, Институт развития информационного общества и др.

Таким образом, в течение 1990-х гг. в России в рамках строительства демократической государственности было осуществлено преобразование органов безопасности страны. Частью этого процесса явился поиск оптимальной институциональной системы государственной информационной безопасности, происходивший одновременно с формированием правовой базы государственной информационной политики.

В течение первого десятилетия реформ в России активно формировались институты экономической информационной безопасности, связанные со становлением в стране рыночных отношений – внутренние подразделения безопасности фирм и компаний и структуры IT-сервиса в области информационного администрирования и защиты данных.

На новый качественный и количественный уровень развития по сравнению с советским периодом вышли в 1990-е гг. отечественные СМИ, являющиеся одним из важнейших факторов формирования в России открытого информационного пространства. Одновременно в условиях интеграции России в глобальное информационное общество складываются

---

[287] *Прохоров Е.П.* Средства массовой информации и информационная безопасность // Информационное общество. 1997. Вып. 4-6. С.36-42; *Россошанский А.В.* Средства массовой информации как институт системы информационной безопасности // Известия Саратовского университета. Серия: Социология. Политология. 2008. Вып.1. С. 121.

научные гуманитарные и технологические центры, участвующие в формировании интеллектуальной базы государственной политики информационной безопасности.

2.2. Новые тенденции в деятельности министерств и ведомств информационного профиля в 2000-е гг.

Политика социально-экономической модернизации России, реализация которой началась в 2000-е гг., включала ряд программ и мероприятий, направленных на создание эффективной системы исполнительной власти, соответствующей параметрам демократического рыночного государства, международным стандартам управленческих и информационных технологий[288]. Частью этого процесса стало обновление комплекса институтов государственной информационной политики, проводившееся в контексте административной реформы и, в то же время – как часть мероприятий по реализации «Доктрины информационной безопасности России – 2000» и последующих версий[289].

Как будет показано далее, модернизация институциональной базы информационной политики Российской Федерации, а также связанное с процессами информатизации организационное, технологическое и кадровое развитие системы отечественных спецслужб, оказало существенное влияние на сферу информационной безопасности России 2000 – 2010-х гг. Процесс обновления концепций деятельности и инфраструктуры органов власти и управления информационного профиля начинается на рубеже XX–XXI в. В 1999 г. сотрудники Аппарата Совета Безопасности Российской Федерации

---

[288] *Юсупов Р.Г., Хайбуллин А.Р.* Функции и роль системы государственного управления в контексте социально-экономической модернизации страны // Государственное управление в России: историко-правовые аспекты: Монография / Коллектив авторов; под научной редакцией доктора исторических наук Р.Г. Юсупова. Москва: ИНФРА-М, 2018. С. 17-24.

[289] *Стрельцов А.А.* Обеспечение информационной безопасности России. Теоретические и методологические основы / под ред. В.А. Садовничего, В.П. Шерстюка. М., 2002; *Алексеева Е.В.* Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере // Ленинградский юридический журнал. 2016. № 4(46). С. 97-103.

Г.В. Емельянов и А.А. Стрельцов опубликовали статью, посвященную вопросам обеспечения безопасности информационного общества, в которой, в частности, отмечалось, что глобальная информатизация создает новые типы рисков и угроз, как для государства и бизнеса, так и для конкретного человека. Среди этих рисков – накопление персональных данных граждан в государственных цифровых базах данных в процессе формирования электронных систем управления, а также рост зависимости пользователей компьютерной техники и Интернета от IT-специалистов, тех кто разрабатывает информационные технологии, определяет алгоритмы поиска информации, оказывает услуги в области информационной безопасности. Авторы подчеркивали, что «непрерывное усложнение информационных систем и сетей связи критически важных инфраструктур обеспечения жизни общества» создает угрозы безопасности, возникающие по технологическим причинам, либо вследствие злонамеренных противоправных действий[290]. В этой связи возрастала ответственность государства в сфере обеспечения информационной безопасности, что требовало, в частности, дальнейшего совершенствования системы институтов государственного управления информационного профиля[291].

В начале XXI в. масштабное расширение российского рынка услуг в области мобильной и сетевой связи от центра к регионам и его глубокая интеграция в глобальное пространство электронных коммуникаций актуализировали задачи дальнейшего совершенствования технологий и организационно-инфраструктурных аспектов системы информационной безопасности государства, бизнеса и граждан[292]. В течение 2000-х гг. был предпринят ряд изменений в структуре федеральных и региональных органов

---

[290] *Емельянов Г.В., Стрельцов А.А.* Проблемы обеспечения безопасности информационного общества // Информационное общество. 1999. № 2. С.15-16.

[291] *Уфимцев Ю.С., Ерофеев Е.А.* Информационная безопасность России. М., 2003.

[292] *Проценко Е.А.* Информационная безопасность субъектов Российской Федерации как составная часть национальной безопасности России // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2006. С. 111.

связи и информации, а также специальных служб, ответственных за обеспечение информационной безопасности по линии государственной, служебной и коммерческой тайны. Так, в апреле 2001 г. в соответствии с «Положением о государственном надзоре за связью и информатизацией в Российской Федерации» Служба государственного надзора за связью (Госвязьнадзор), действовавшая в структуре Министерства связи РФ с 1993 г., была преобразована в Департамент по надзору за связью и информатизацией того же министерства[293].

Одновременно в ведении Минсвязи создавались 77 управлений по надзору за связью и информатизацией в субъектах Российской Федерации. В задачу Департамента входил контроль деятельности систем и средств связи юридических лиц всех форм собственности и ведомственной принадлежности, физических лиц, оказывающих услуги в области связи, а также радиоэлектронных приборов, высокочастотных устройств, производственно-технологических сетей. Вне его ведения находились специальные сети правительственной связи, ведомств обороны, государственной безопасности и правопорядка. Годом ранее газета «Коммерсантъ» опубликовала статью, посвященную предстоящей реформе государственного надзора за связью, в которой Госсвязьнадзор именовался «коммуникационной милицией» и разъяснялось, что без разрешения его инспекторов не может начать работу ни один объект связи: «Они проверяют все: имеет ли оборудование оператора сертификаты, на тех ли частотах работает передатчик, доходят ли телеграммы в срок до адресата и т.д.»[294]. Положительную оценку эксперт «Коммерсанта» дал отмене существовавшей в 1990-е гг. системы оплаты операторами работ Госвязьнадзора по тестированию средств связи и оформлению разрешений на эксплуатацию

---

[293] Постановление Правительства РФ от 28.04.2000 N 380 (ред. от 26.04.2004) «О реорганизации системы государственного надзора за связью и информатизацией в Российской Федерации» [Электронный ресурс]. URL: https://legalacts.ru/doc/postanovlenie-pravitelstva-rf-ot-28042000-n-380/ (Дата обращения: 15.01.2022)

[294] *Чеберко И.* «Госсвязьнадзор» заживет по новым правилам // Коммерсантъ. 5 мая 2000 г. С. 4.

базовых станций по договорным ценам. (В ноябре 1999 г. Министерство антимонопольной политики вынесло в связи с этой ситуацией предписание Минсвязи о приведении «Положения» о Госсвязьнадзоре в соответствие с действующим законодательством)[295].

Указом Президента России В.В. Путина от 11 августа 2003 г. были уточнены полномочия Федеральной службы безопасности Российской Федерации (ФСБ России), на которую возлагается ряд ответственных функций в области защиты государственной тайны, включая задачи противодействия иностранным техническим разведкам, развития инженерно-технических и криптографических средств информационной безопасности, систем спецсвязи на территории России и за рубежом.[296]

Новый этап институционализации государственной политики информационной безопасности России начинается в 2004 г., когда в рамках мероприятий по модернизации государственного управления страны в целом была создана трехзвенная система федеральной исполнительной власти, включающая федеральные министерства, службы и агентства[297]. С этого момента функции государственного надзора в области информатизации и связи вновь переходят к ведомству федерального уровня – Службе Россвязьнадзор, которая в 2008 г. была преобразована в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Служба РКН или Роскомнадзор). В том же году было создано Министерство связи и массовых коммуникаций России, с 2018 г. – Министерство цифрового развития, связи и массовых коммуникаций РФ (Минцифры), в ведение которого вошел Роскомнадзор.

---

[295] *Чеберко И.* «Госсвязьнадзор» заживет по новым правилам // Коммерсантъ. 5 мая 2000 г. С. 4.

[296] Указ Президента РФ В.В. Путина от 11 августа 2003 № 960 «Вопросы Федеральной службы безопасности Российской Федерации» (в ред. 21.06.2021). [Электронный ресурс] URL: https://legalacts.ru/doc/ukaz-prezidenta-rf-ot-11082003-n-960/ (Дата обращения: 15.01.2022)

[297] Указ Президента РФ В.В. Путина от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти» [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/acts/bank/20611 (Дата обращения: 18.01.2022)

Постановлением Правительства России от 16 марта 2009 г. № 228. Роскомнадзору был передан ряд федеральных государственных унитарных предприятий: Главный радиочастотный центр (Москва), Радиочастотные центры федеральных округов – Центрального (Москва), Приволжского (Нижний Новгород) Сибирского (Новосибирск), Южного (Ростов-на-Дону), Северо-Западного (Санкт-Петербург), Уральского (Екатеринбург) и Дальневосточного (Хабаровск), а также Научно-технический центр «Информрегистр» (Москва)[298]. К 2011 г. Служба осуществляла надзор за системами и средствами связи 385 юридических лиц[299]. В 2013 г. была проведена реорганизация сети территориальных органов Роскомнадзора и сделан значительный шаг вперед в развитии системы межведомственного электронного взаимодействия (СМЭВ) Службы РКН с другими органами исполнительной власти страны. В течение 2013 г. сервисами СМЭВ воспользовались 20 министерств и ведомств, которым Роскомнадзор предоставил информацию по 4,8 тыс. запросов[300]. С 1 декабря 2013 г. Служба полностью перешла на работу с гражданами и юридическими лицами через Единый портал государственных и муниципальных услуг, в том числе начала осуществляться в электронном формате процедура выдачи разрешений на использование радиочастот[301].

После вхождения Крыма в состав Российской Федерации уже в первых числах апреля 2014 г. было создано Управление Роскомнадзора по Республике Крым и г. Севастополю, а также образован филиал радиочастотной службы по Крымскому федеральному округу и началась

---

[298] Подведомственные предприятия // Электронный архив Роскомнадзора. URL: https://web.archive.org/web/20141007202701/http://rkn.gov.ru/p426/ (Дата обращения: 24.01.2022)

[299] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс]. URL: https://www.tadviser.ru/index.php (Дата обращения: 24.01.2022)

[300] Резервы эффективности Роскомнадзора - в автоматизации, электронном межведомственном взаимодействии и оказании государственных услуг в электронном виде // Электронный архив Роскомнадзора. Новости. 24 декабря 2013 г. URL: https://web.archive.org/web/20141007001035/http://rkn.gov.ru/news/rsoc/news23317.htm (Дата обращения: 25.01.2022)

[301] Там же.

модернизация его имеющейся материально-технологической базы в соответствии со стандартами российской Автоматизированной системы радиоконтроля (АСРК-РФ). На заседании Координационного совета предприятий радиочастотной службы при Роскомнадзоре 29 апреля 2014 г. был отмечен высокий профессиональный уровень крымских специалистов в области радиоконтроля, кадры которых были сохранены при формировании российской инфраструктуры Роскомнадзора в Крыму[302].

В современную структуру Роскомнадзора входят десять центральных управлений по основным направлениям деятельности и 75 территориальных органов в федеральных округах и субъектах Российской Федерации. Кроме того, Роскомнадзор располагает цифровой инфраструктурой – официальным сайтом, страницами в наиболее популярных социальных сетях (ВКонтакте, Facebook, Twitter и др.)[303]. С июня 2018 г. важной функцией Роскомнадзора является ведение Единого реестра доменных имен, в базу данных которого входят сайты, содержащие информацию, запрещенную к распространению в Российской Федерации[304].

Важным этапом в формировании современной системы институтов государственной информационной безопасности стало учреждение в августе 2004 г. Федеральной службы по техническому и экспортному контролю (ФСТЭК), к которой перешли полномочия и подчиненная инфраструктура Гостехкомиссии[305]. В январе 2005 г. в журнале «Системы безопасности»

---

[302] Система радиоконтроля в Крыму будет модернизирована // Электронный архив Роскомнадзора. Новости. 29 апреля 2014 г. URL: https://web.archive.org/web/20140713042021/http://rkn.gov.ru/news/rsoc/news25133.htm(Дата обращения: 25.01.2022)

[303] *Унукович А.С.* Деятельность Роскомнадзора по обеспечению безопасности пользователей сети Интернет // Молодой ученый. 2019. № 22 (260). С.371.

[304] Постановление Правительства РФ от 26 октября 2012 года № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено (в ред. постановления Правительства РФ от 5 июня 2018 года № 651) // СЗ РФ. 2012. № 44, ст. 6044.

[305] Указ Президента РФ В.В. Путина от 16.08.2004 № 1085 (ред. от 30.11.2006) «Вопросы Федеральной службы по техническому и экспортному контролю» // СЗ РФ, 2004, № 4, ст. 3541.

было опубликовано большое интервью руководителя ФСТЭК С.И. Григорова, в котором освещались полномочия и задачи преобразованной Службы, а также разъяснялись вопросы взаимодействия ФСТЭК с другими министерствами и ведомствами. С.И. Григоров, в частности, отметил, что Служба руководствуется практикой принятия своих основных решений совместно с заинтересованными органами власти, руководители которых, в соответствии с перечнем, утвержденным Президентом России, участвуют в заседания коллегии ФСТЭК. При этом глава ФСТЭК подчеркнул, что работа Службы осуществляется на основе принципа коллегиальности в сочетании с персональной ответственностью каждого ведомства за свой участок защиты информации, полностью исключив возможность монополизма в принятии решений в вопросах национальной безопасности.[306] Кроме того, ФСТЭК продолжила практику работы на основе двусторонних соглашений с другими государственными учреждениями и ведомствами по вопросам, представляющим совместный интерес, и о совместном проведении работ в области обеспечения информационной безопасности[307].

ФСТЭК представляет собой федеральный орган власти, который контролирует сферу обеспечения информационной безопасности в базовых компонентах информационной и телекоммуникационной инфраструктуры, в том числе в плане технического противодействия иностранным разведкам на российской территории. Служба выступает специальным уполномоченным органом по экспортному контролю программного обеспечения, носителей информации, электроники, технических средств связи и других товаров, связанных со сферой хранения и передачи информации. Данное направление работы Службы было связано также с необходимостью усиления мер противодействия распространению оружия массового уничтожения (ОМУ) в

[306] Гостехкомиссия России стала ФСТЭК России. Что изменила реформа? [Интервью с С.И. Григоровым] // Системы безопасности. 2005. № 1. URL: https://secuteck.ru/articles2/oficial/gostehkom_stala_fstek (Дата обращения: 26.01.2022)
[307] Там же.

связи с возросшими глобальными угрозами со стороны международного терроризма. Президент России В.В. Путин, выступая 3 декабря 2003 г. на заседании Совета Безопасности, посвященного этой проблеме, в частности, отметил значение экспортного контроля в российской системе по нераспространению ОМУ, а также необходимость более четкой координации действий органов власти в данной сфере[308]. В 2005 г. были одобрены «Основы государственной политики РФ в области нераспространения ОМУ и средств его доставки», а в 2007 г. – внесены необходимые дополнения в Закон 1999 г. «Об экспортном контроле». Соответственно, структуры ФСТЭК во второй половине 2000-х гг. усилили контроль экспорта в Россию техники и технологий двойного назначения, компоненты которых могли быть использованы для создания ОМУ, взаимодействуя в этом вопросе с межведомственной Комиссией по экспортному контролю[309].

ФСТЭК и ее территориальные структуры (управления в федеральных округах), являясь органами государственной безопасности, ведут работу в области защиты государственной тайны и других видов информации ограниченного доступа. Функцией ФСТЭК является лицензирование и сертификация, а также разработка и производство технических средств защиты информации некриптографическими методами (область шифрования находится в компетенции ФСБ). В ведении ФСТЭК находится Государственный научно-исследовательский испытательный институт проблем технической защиты информации – головная организация по данному направлению научных исследований.

В связи с принятием Федерального закона от 27 декабря 2002 г. «О техническом регулировании» и ряда подзаконных нормативных актов,

---

[308] Вступительное слово Президента России В.В. Путина на заседании Совета Безопасности по вопросу об обеспечении национальной безопасности в сфере нераспространения оружия массового уничтожения и средств его доставки. Москва, 3 декабря 2003 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/events/president/transcripts/22237 (Дата обращения: 26.01.2022)

[309] Забалуев, Ю. Политика России в сфере нераспространения ОМУ и средств его доставки // Научно-аналитический журнал Обозреватель - Observer. 2008. № 2(217). С. 19-23.

включая «Программу разработки технических регламентов на 2005–2006 годы» (утверждена распоряжением Правительства РФ от 6 ноября 2004 г.) на ФСТЭК была возложена организация разработки и непосредственное участие в создании технических регламентов «О безопасности информационных технологий» и «О требованиях к средствам обеспечения безопасности информационных технологий». Разработку нормативной документации в области защиты информации ФСТЭК продолжает на протяжении всего периода своей деятельности. Документы ФСТЭК регламентируют такие вопросы как классификация программного обеспечения и технических средств защиты информации; применение тех или иных схем защиты информации данных исходя из уровня и характера угроз; параметры оценки деятельности организаций и персонала в сфере информационной безопасности; порядок лицензирования деятельности в соответствующих отраслях и сертификации программного обеспечения[310]. «Деятельность ФСТЭК РФ показывает ее готовность успевать за требованиями времени и предлагать рынку новые инструменты защиты информации», – пишет эксперт компании «СёрчИнформ», одной из ведущих российских разработчиков средств ИБ, резидента Инновационного центра «Сколково»[311].

В XXI в. работа министерств и ведомств информационного профиля осуществлялась в качественно новых условиях компьютеризации деловой и общественной жизни России, когда задачи информационной безопасности выдвигаются в число первоочередных задач в области обеспечения национальной безопасности государства[312]. При этом уровень интеграции госструктур, бизнеса, общественных организаций и СМИ в пространство цифровых коммуникаций в Москве, Санкт-Петербурге и других крупных

---

[310] Требования ФСТЭК по защите информации [Электронный ресурс] // Сайт компании «СёрчИнформ». URL: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/razrabotka-trebovanij-po-ib/trebovaniya-fstek-po-zaschite-informatsii/ (Дата обращения: 26.01.2022)

[311] Там же.

[312] *Ноговицын А.А.* Информационная безопасность в системе национальной безопасности Российской Федерации // Безопасность России – 2010: экспертно-аналитическое обозрение. М.: Триумфальная арка, 2009. С. 46-63.

городах существенно опережал многие российские регионы. Соответственно, требовался дифференцированный подход к решению организационных, технологических и кадровых задач в области информационной безопасности. Существенно различалась степень внедрения информационных технологий по отраслям экономики и управления, а также нередко и внутри того или иного ведомства.

В 2000-е гг. расширяется использование цифровых технологий в деятельности правоохранительных органов России. В частности, с 2001 г., развертываются цифровые комплексы радиосвязи МВД РФ. Цифровизация работы структур МВД, в свою очередь, обусловила необходимость повышения уровня информационной безопасности оперативной работы, служебной переписки и внутреннего делопроизводства органов внутренних дел. Существовали специфические риски, связанные с необходимостью оградить информационные базы правоохранительных органов от доступа преступных элементов[313].

25 января 2011 г. Указом Президента России в структуре МВД РФ был создан Департамент информационных технологий, связи и защиты информации (ДИТСиЗИ). Новое подразделение центрального аппарата МВД выполняло задачи по организации и нормативному регулированию работы структур ведомства в области развития информационных и телекоммуникационных систем, радиоэлектронной и цифровой связи. В сферу ответственности ДИТСиЗИ входили такие аспекты деятельности органов внутренних дел РФ как противодействие иностранным техническим разведкам, техническая и криптографическая защита информации, использование электронной подписи и др.[314]

---

[313] *Кемпф В.А.* Особенности субъективных угроз информационной безопасности информационных систем в деятельности органов внутренних дел Российской Федерации // Полицейская деятельность. 2019. № 5. С. 47-52.

[314] Положение о Департаменте информационных технологий, связи и защиты информации МВД России. Утверждено приказом МВД России от 15 июня 2021 г. № 444 (в ред. приказа МВД России от 22 октября 2021 г. № 770) [Электронный ресурс] // МВД России. Официальный сайт. URL: https://мвд.рф/mvd/structure1/Departamenti/Departament_informacionnih_tehnologij_sv/Polozhenie (Дата обращения: 26.01.2022)

В 2014-2015 г. была введена в действие единая система информационно-аналитического обеспечения деятельности (ИСОД) МВД России. За два с половиной года число ее пользователей превысило 570000. По данным на 2017 г. Единый информационно-аналитический центр МВД обрабатывал более 12000 обращений, услугами ИСОД пользовались 425000 граждан и организаций[315]. Система предусматривала несколько уровней доступа, каждый из которых обладал соответствующим классом информационной защиты. Главный конструктор ИСОД А.Ю. Нечаев, выделяя в качестве одного из ключеаых направлений дальнейшего развития системы обеспечение ее информационной безопасности, подчеркивал, что существует «глобальная задача создания единой информационно-коммуникационной среды, в рамках которой обеспечивается защита информации на всех этапах ее прохождения, обработки и хранения»[316].

В контексте решения задач информационной безопасности России большое значение имело взаимодействие Совета безопасности, органов исполнительной власти и других государственных институтов информационной безопасности, которое обеспечивалось как нормативно-правовыми актами, определявшими их функции и полномочия, так и на основе межведомственных документов. 28 апреля 2014 г. заместителем руководителей Роскомнадзора А. Приезжевой, заместителем председателя ЦИК России С. Вавиловым и заместителем руководителя Федеральной службы судебных приставов Т. Игнатьевой было подписано «Соглашение о сотрудничестве при реализации своих полномочий в сфере защиты прав субъектов персональных данных». Инициатива соглашения исходила от Роскомнадзора как органа, ответственного за данное направление информационной безопасности. Глава Службы РКН А. Жаров, выступая на церемонии подписания Соглашения, выразил убеждение, что к нему

[315] Тематический сборник «Информационные технологии, связь и защита информации МВД России»-2017. С.5 [Электронный ресурс] // МВД России. Официальный сайт. URL: https://мвд.рф/mvd/structure1/Departamenti/Departament_informacionnih_tehnologij_sv/informacionnie-tehnologii-sbornik (Дата обращения: 26.01.2022)

[316] Там же.

присоединятся и другие ведомства, поскольку «только общими усилиями можно добиться реальных результатов, сформировать эффективную систему защиты персональных данных в Российской Федерации»[317].

Примером сотрудничества органов власти в сфере информационной безопасности является работа Межведомственной комиссии по защите государственной тайны, которая объединяет представителей ФСБ России, Министерства обороны РФ, Службы внешней разведки и ФСТЭК России[318].

Свой вклад в развитие информационного общества и реализацию политики информационной безопасности России в 2000-е гг. внесли созданная в 2002 г. «Межведомственная комиссия по программам, содержащим мероприятия по разработке и использованию информационно-коммуникационных технологий», Государственная комиссия по информатизации (ГКИ), осуществлявшая, в частности, проект «КиберПочт@», и Совет по проблемам информатизации регионов при ГКИ.

Существенным фактором институционального развития и повышения качества системы обеспечения государственной информационной безопасности России явился Федеральный закон № ФЗ-187. «О безопасности критической информационной инфраструктуры Российской Федерации», принятый 26 июля 2017 г. Актуальность мер в сфере защиты от «экспоненциального роста целенаправленных атак на КИИ России»[319], нашедших отражение в данном правовом акте и в принятых на его основе

---

[317] Подписано Соглашение о сотрудничестве органов государственной власти при реализации своих полномочий в сфере защиты прав субъектов персональных данных // Электронный архив Роскомнадзора. Новости. 28 апреля 2014 г. URL: https://web.archive.org/web/20141007023431/http://rkn.gov.ru/news/rsoc/news25114.htm (Дата обращения: 26.01.2022)

[318] *См.: Пурис А.В.* Межведомственная комиссия по защите государственной тайны: структура и компетенция // Государство, право, общество: проблемы взаимодействия: Сборник статей II Международной научно-практической конференции, Пенза, 29 апреля 2015 года / Пензенский государственный университет, Общество «Знание» России; под редакцией Н.Г. Карнишиной. Пенза: Автономная некоммерческая научно-образовательная организация «Приволжский Дом знаний», 2015. С. 76-79.

[319] *Горелик В.Ю., Безус М.Ю.* О безопасности критической информационной инфраструктуры Российской Федерации // StudNet. 2020. Т. 3. № 9. С. 1438.

нормативных документах[320], способствовала активизации деятельности ФСТЭК и других органов информационной безопасности, экспертного сообщества, участников рынка информационных технологий и услуг[321]. Законом 2017 г. было дано определение объектов и субъектов критической информационной инфраструктуры[322], и указаны три регулятора в сфере обеспечения безопасности КИИ – ФСТЭК, ФСБ России и Минсвязь. В последующий период руководство и специалисты данных ведомств уделяли значительное внимание взаимодействию в данной сфере и разъяснению правовых норм и методики безопасности КИИ в ходе расширенных заседаний коллегий ФСТЭК и Минсвязи, специализированных семинаров, научных конференций. Так, например, заместитель начальника управления ФСТЭК России Елена Торбенко в сентябре 2020 г. приняла участие в XXV Международной научно-практической конференции «Комплексная

---

[320] Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. (Утверждены приказом ФСТЭК России от 25 декабря 2017 г. №239). СПб.: Стаун-кантри, 2017. 34 с.; Постановление Правительства России от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [Электронный ресурс] URL: https://static.government.ru/media/files/uPA03V4BfqknJWNExcfX3gSlDZi4zuas.pdf (Дата обращения: 26.01.2022)

[321] *Сторожик В.С.* Нормативно-правовое и методическое обеспечение реализации государственной политики в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации // Региональная информатика и информационная безопасность: Сборник трудов, Санкт-Петербург, 23–25 октября 2019 г. СПб.: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2019. С. 17-18.

[322] Объекты критической информационной безопасности (КИИ) – это информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, принадлежащие субъекту КИИ. Под субъектами КИИ понимаются:1. государственные органы, государственные учреждения, российские юридические лица и индивидуальные предприниматели, действующие в сфере здравоохранения, науки, транспорта, связи, финансовом и банковском секторах, энергетике, ТЭК, атомной энергетике, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, которые являются собственниками, арендаторами или распоряжаются на иных законных основаниях объектами КИИ; 2. государственные органы, государственные учреждения, российские юридические лица и индивидуальные предприниматели, которые обеспечивают взаимодействие информационных систем и сетей, принадлежащих субъектам КИИ (прим. авт.)

защита информации», где выступила с докладом о правовом регулировании обеспечения безопасности КИИ. Она подчеркнула, в частности, важность взаимодействия федеральных органов информационной безопасности с отраслевыми регуляторами КИИ, которые более глубоко знают специфику того или иного сектора экономики и бизнеса. «Кто лучше этих регуляторов знает специфику тех систем, которые есть в этих сферах? Никто… У автоматизированных систем управления в сфере здравоохранения очень мало общего с автоматизированными системами в транспорте. В системах управления сетью связи очень мало общего с банковскими системами. Специфика реализации, специфика последствий, которые будут от нарушения функционирования, в том числе специфика проведения атак на эти системы тоже будет разная. Поэтому мы бы хотели, чтобы отраслевые регуляторы помогали», – подчеркнула Е. Торбенко[323].

В 2021 г. вступили в силу нормативные требования, которые, с одной стороны усиливали ответственность руководителей субъектов КИИ, которые были обязаны создать силы обеспечения безопасности КИИ (группу сотрудников, отвечающих за сферу защиты информации); с другой стороны, возрастал и уровень федерального контроля – начинались посещения представителями ФСТЭК объектов КИИ. Как подчеркнул в интервью журналу «Информационная безопасность» заместитель начальника управления ФСТЭК России Алексей Кубарев, «всем нам надо быть крайне внимательными и помогать друг другу»[324].

В 2008 – 2010 гг. в ряде российских организаций в порядке эксперимента начали создавать ведомственные системы обнаружения и предупреждения компьютерных атак (СОПКА), опираясь на модель

---

[323] ФСТЭК рассказал о проблемах реализации законодательства в области обеспечения безопасности КИИ [Электронный ресурс] // BIS Journal − Информационная безопасность банков. 17 сентября 2020 г. URL: https://ib-bank.ru/bisjournal/news/14212 (Дата обращения: 28.01.2022)

[324] Ответы на актуальные вопросы о безопасности объектов КИИ [Электронный ресурс] // Сайт журнала «Информационная безопасность». 12 января 2021 г. URL: https://www.itsec.ru/articles/otvety-na-aktualnye-voprosy-o-bezopasnosti-obektov-kii (Дата обращения: 28.01.2022)

противодействия хакерским атакам, разработанную Агентством национальной безопасности США. Однако последующие события, в том числе успешные хакерские атаки на американские госструктуры, показали, что в данном вопросе необходима межведомственная централизация[325]. В 2014 г. Президентом России В.В. Путиным была утверждена «Концепция ГосСОПКА», в течение двух последующих лет апробировался пилотный проект в Министерстве экономического развития РФ. В 2017 – 2018 гг. ФСБ России занималось созданием технологического ядра системы, после чего был сформирован Национальный координационный центр по компьютерным инцидентам (НКЦКИ), к которому подключались субъекты КИИ[326]. Законом 2017 г. «О безопасности КИИ РФ» и приказе ФСТЭК от 25 декабря 2017 г. предусмотрена модель взаимодействия с ГосСОПКА субъектов критической информационной инфраструктуры. ФСТЭК рекомендует организациям и предприятиям КИИ применять технологии, разработанные ГосСОПКА, либо иные модели информационной безопасности, если они являются эффективными для данной информационной системы или сети. Но в случае компьютерной атаки, с которой не могут справиться собственные силы обеспечения безопасности КИИ, обращение к ГосСОПКА становится обязательным. По вопросам взаимодействия КИИ и ГосСОПКА проводятся научные конференции и обучающие вебинары[327].

Таким образом, в 2000-е - начале 2010-х гг. в Российской Федерации была осуществлена модернизация органов государственного управления информационного профиля: создана система институтов информационной безопасности, включающая федеральные министерства и департаменты федеральных министерств, федеральные специализированные службы и их

---

[325] *Кузнецов Д.* ГосСОПКА: что такое, зачем нужна и как устроена [Электронный ресурс] URL: https://www.anti-malware.ru/analytics/Technology_Analysis/gossopka-what-is-it-how-it-works (Дата обращения: 28.01.2022)

[326] Там же.

[327] См.: *Куц С.* Взаимодействие КИИ и ГосСОПКА: Вебинар. [Электронный ресурс] URL: https://www.ussc.ru/upload/files (Дата обращения: 28.01.2022)

региональные управленческие структуры, а также находящиеся в их ведении НИИ и научно-производственные структуры.

2.3. Информационная безопасность и российское общество в условиях распространения цифровых технологий начала XXI в. (социальные сети, зашита корпоративных и частных данных)

По мере распространения в России XXI в. компьютерных технологий, современных телекоммуникаций и цифровых сетей возрастают общественные риски в сфере информационной безопасности, связанные с вопросами технологической защиты коммерческой тайны и личной конфиденциальности, распространением через Интернет социально деструктивной и запрещенной законом информации, проблемами достоверности данных СМИ и социальных сетей[328]. Информационные риски, проявились в самых разных областях экономики, общественной и частной жизни (фейки в Интернете, хакерские атаки из-за рубежа на российский бизнес и СМИ[329]). Дополнительные угрозы государственной и общественной информационной безопасности России возникли в 2010-е гг. связи с обострением геополитической обстановки[330].

В то же время растет и степень вовлеченности российского общества в обеспечение информационной безопасности бизнеса, личности, отдельных категорий граждан, прежде всего детей и молодежи, а также страны в целом[331]. Данная тенденция проявляется в расширении рынка технических средств, программного обеспечения и сервисов защиты информации, на использование которых россияне готовы были расходовать личные и

---

[328] *Куракин А.Л.* Реальные проблемы искусственного мира (об информационной безопасности) // Полигнозис. 2000. № 1. С. 12-15; *Овчинников С.А., Гришин С.Е.* Угрозы личности, обществу и государству при внедрении информационных технологий // Информационная безопасность регионов. 2011. № 2 (9). № 2. С. 26-31.

[329] См.: Хакеры уничтожили сайт «Московского комсомольца» // Коммерсант. 4 декабря 2009 г. № 227. С.6.

[330] Интервью Секретаря Совета Безопасности Российской Федерации Н.П. Патрушева // Российская газета. Федеральный выпуск. 23 декабря 2015 г. № 6861.

[331] *Хохлов Ю.Е.* Об информационном обществе, информационном праве и информационной безопасности // Информационное общество. 2001. № 4. С. 1.

корпоративные средства, исходя из своих деловых интересов, защиты прав интеллектуальной собственности, безопасности семьи и т.п. Соответственно, все участники этого рынка – торговые фирмы и производители электроники и технологических компонентов систем связи, IT-компании, потребители материальной и цифровой продукции, обеспечивающей различные аспекты ИБ – воздействовали на процесс осознания российским обществом проблем информационной безопасности и утверждения различных моделей и форм ее решения.

Информатизация повседневной жизни, государственного управления и сферы услуг, массовый переход на цифровые формы создания и тиражирования всех видов документации ведет, с одной стороны, к росту компьютерной грамотности населения. С другой стороны, в России начала 2000-х гг. появляется многочисленное сообщество пользователей Интернета, нуждающихся в помощи профессионалов для обеспечения защиты своих компьютеров от вирусов, установки фильтров для определенных видов сайтов в семьях с детьми и т.п. В 2000-е гг. среди российских пользователей Интернета высокими темпами повышается спрос на такие услуги как «лечение» зараженных вирусами информационных систем организаций и персональных компьютеров, подключение почтовых серверов, имеющих дополнительные уровни защиты, и др.

В XXI в. вопросы информационной безопасности становятся неотъемлемой частью интеллектуального пространства России, что находит свое выражение в различного рода конференциях и форумах, телепередачах, выходе в свет большого количества публицистической, научной, учебной литературы, посвященной теме информационной безопасности, поиску наиболее эффективных моделей взаимодействия государства и общества в решении проблем информационной безопасности[332].

---

[332]. *Евтюшкин А.В.* Сотрудничество государства, бизнеса, гражданского общества и научно-образовательного сообщества в подготовке и реализации национальной стратегии перехода России к информационному обществу / А.В. Евтюшкин, Т.В. Ершова, А.В. Коротков, Ю.Е. Хохлов // Информационное общество. 2002. Вып. 1. С. 47-51.

В том числе 2000-е гг. характеризуются появлением новых корпоративных и общественных структур, деятельность которых связана с поддержкой информатизации, включая компоненты информационной безопасности, а также стартом крупных государственно-общественных мероприятий по тематике информационной безопасности, ряд которых регулярно проводится до настоящего времени.

В 2000 году две российских интернет-компании «Релком. Деловая сеть» и «Демос-Интернет» основали «Фонд развития Интернет» в целях поддержки проектов, связанных с развитием Интернета, глобальных информационных сетей и сетевых технологий, научной деятельности в данной сфере, распространения компьютерной грамотности среди широких слоев населения России. В последующий период Фонд стал участником большинства крупных проектов и мероприятий, связанных с вхождением России в глобальное информационное общество. В 2016 г. Фонд вошел в Международный исследовательский консорциум информационной безопасности,(МИКИБ)[333].

В 2010-е гг. на платформе Инфофорума началась реализация Всероссийской акции «Информационная безопасность для всех» и других общественных инициатив. Инфофорум интегрирован в такие международные проекты, как Евразийский форум информационного взаимодействия «Инфофорум-Евразия» и др.

С конца 2000-х гг. возрастает активность общественных организаций и деятелей цифрового рынка в сфере поддержки различных проектов по обеспечению безопасности в Интернете, в том числе уделяется внимание проблемам информационной безопасности детей и подростков. По инициативе группы общественных организаций и Интернет-компаний 2009 г. был объявлен Годом безопасного Интернета в России. В рамках данного проекта Фондом «Дружественный Рунет» была организована горячая линия

[333] О Фонде [Электронный ресурс] // Сайт Фонда развития Интернет URL: https://www.fid.su/about-us/purpose (Дата обращения: 17.02.2022)

по противодействию детской порнографии в сети и открыта телефонная линия психологической помощи «Дети Онлайн» для детей и подростков, столкнувшихся с проблемами при пользовании Интернетом или мобильной телефонной связью. Также начал действовать цифровой Центр безопасного Интернета в России, выполнявший справочно-информационные функции, а также оказывавший правовую и психологическую помощь пользователям Интернета[334].

В 2011 г. при поддержке Минкомсвязи РФ, МВД России и Комитета Государственной Думы РФ по вопросам семьи, женщин и детей было основано некоммерческое партнерство «Лига безопасного интернета», действующая в целях «искоренения опасного контента путем самоорганизации профессионального сообщества, участников интернет-рынка и рядовых пользователей»[335]. Деятельность Лиги направлена, в первую очередь, на защиту детей и молодежи от влияния социально опасных сайтов и сетевых сообществ. Организация проводит мониторинг нарушений информационного законодательства, анализирует информационные потоки, выявляя фейки, кибербуллинг и другие деструктивные явления в Интернете, готовит рейтинги безопасности поисковых систем, ведет просветительскую работу с педагогами и родительскими организациями российских регионов в рамках акции «Месяц безопасного Интернета» и др.[336]

Следует отметить, что в 2010-е гг. заметно возрастает интерес научных центров, гуманитарных организаций, деловых структур субъектов Российской Федерации к участию в мероприятиях и проектах в области информационной безопасности, что связано с общим расширением информатизации на местах[337].

---

[334] *Хохлова Н.И.* Обеспечение детской безопасности в Интернете: российский опыт и зарубежные инициативы // Пространство и Время. 2012. № 1(7). С. 87-92.

[335] О Лиге // Сайт Лиги безопасного Интернета [Электронный ресурс] URL: https://ligainternet.ru/liga/about.php (Дата обращения: 28.01.2022)

[336] Там же.

[337] *Жданчиков П.А.* Итоги и перспективы региональной информатизации // Региональная экономика: теория и практика. 2018. Т. 16. № 11. С. 2015-2033.

С 2010 г. в России проводится ежегодный Международный Форум безопасного Интернета (ФБИ) – крупное мероприятие, проходящее при поддержке Минсвязи РФ, РИА «Новости», МИА «Россия сегодня» и Российской Ассоциации электронных коммуникаций (РАЭК). Его участниками являются представители органов власти и управления, научного сообщества, ведущих компаний – деятелей рынка информационных технологий и услуг (Mail.ru Group, Лаборатория Касперского и др.). С 2012 г. организатором Форума выступает Лига безопасного Интернета. Тогда же впервые был проведен Детский форум безопасного Интернета.

В процессе становления в России информационного общества в рамках различных сообществ и социально-профессиональных групп формируются определенные различия в видении проблемы информационной безопасности, в представлениях об этике профессиональной деятельности, связанной с созданием и распространением информации. Так, для журналистов, блогеров, студенческой молодежи и других категорий лиц, непосредственно вовлеченных в формирование информационного пространства России и расширение его международного поля, безусловным приоритетом является возможность свободного получения, создания и использования информации. экстремиДля специалистов, профессиональная деятельность которых осуществляется в структурах, обеспечивающих национальную безопасность и правопорядок (спецслужбы, армия, органы исполнительной власти, связанные со сферой ИБ) приоритетными являются вопросы обеспечения защиты государственной и служебной тайны.

При этом для большинства представителей вышеназванных социальных страт в рассматриваемый период существуют и дополнительные факторы, воздействующие на восприятие ими проблем информационной безопасности и работу с информацией. «Ответственность журналистов перед общественностью имеет верховенство над любой другой ответственностью, в частности, над ответственностью перед работодателями и государственной властью. Миссия по информированию обязательно включает в себя

ограничения, которые спонтанно налагают на себя сами журналисты», – говорится в принятой в 1971 г т.н. «Мюнхенской хартии» свободной прессы[338]. При этом формально независимые СМИ могут испытывать существенное давление финансовых, политических, идеологических факторов, определяющих выбор транслируемых в информационное пространство фактов и их трактовку[339]. В своей профессиональной деятельности журналисты непосредственно сталкиваются с вопросами о достоверности источников полученной и опубликованной ими информации, воздействующей на огромную читательскую (зрительскую аудиторию). Отстаивая свое право на получение информации, представители СМИ могут осознанно или невольно вступать в противоречие с установленными законом ограничениями доступа к тем или иным данным. При этом деятели СМИ, литераторы, ученые заинтересованы не только в продвижении созданных ими текстов и визуальных образов, но и в защите своего авторского права, случаи ущемления которого могут быть связаны с некорректным тиражированием произведений в Интернете, взломами частной переписки и т.п.

В рассматриваемый период наблюдалась динамика информационной политики отечественного бизнеса. «Почти все организации ждут от информационных систем, в первую очередь, полезной функциональности, – отмечал представитель АО «Инфосистемы Джет» В.А. Галатенко в 1996 г. – Компьютерные системы покупаются не ради защиты данных, а, наоборот, защита данных строится ради экономически выгодного использования компьютерных систем»[340]. Он же отмечал, что в России интерес к вопросам информационной безопасности проявляют преимущественно банковские

---

[338] Хартия обязанностей и прав журналистов [Электронный ресурс] // Сайт профсоюза журналистов и работников СМИ. URL: https://profjur.org/hartija-objazannostej-i-prav-zhurnalistov/ (Дата обращения: 16.02.2022)

[339] *Ахмадиев Ф.В.* Свобода слова и ответственность журналиста // Вестник Башкирского университета. 2011. Т. 16. № 2. С. 529-530.

[340] *Галатенко В.А.* Информационная безопасность – основы [Электронный ресурс] // Системы управления базами данных. 1996. № 1. URL: https://www.osp.ru/dbms/1996/01/13031466 (Дата обращения: 15.01.2022)

круги[341]. В XXI в. отношение российского бизнеса к вопросам информационной безопасности изменилось в сторону большей ответственности. Российские компании и фирмы в самых различных сегментах рынка, в том числе представляющие услуги в сфере информации и связи, электронной коммерции и др., в 2000 – 2010-е гг. повышают уровень защиты собственной экономической информации и данных своих клиентов; лидеры цифрового рынка следуют принципам самоконтроля в области соблюдения информационного законодательства. При этом частный бизнес неизменно стремится к оптимизации расходов на ИБ, к привлечению рекламодателей и других внешних партнеров, что увеличивает информационные риски как для самого бизнеса, так и для получателей товаров и услуг. В 2017 – 2021 гг. в связи с усилением контроля информационной инфраструктуры со стороны ФСТЭК в российском деловом сообществе развертывается дискуссия относительно практики применения новых нормативных документов и взаимодействия с государственными институтами в сфере информационной безопасности и значимости ИБ для современного российского бизнеса. В условиях пандемии COVID-19 произошел существенный рост рынка электронной коммерции и услуг, в том числе спрос на обеспечение информационной безопасности к весне 2020 г. по сравнению с аналогичным периодом 2019 г. увеличился вдвое. Представляют интерес экспертные оценки отношения современного отечественного бизнеса к затратам на информационную безопасность. В беседе с корреспондентом газеты «Коммерсант» директор по развитию бизнеса в России компании Positive Technologies Максим Филиппов высказал мнение, что интерес компаний к ИБ – это кратковременное явление: «в приоритете у бизнеса обеспечить функциональность и работоспособность бизнес-процессов, а

[341] *Галатенко В.А.* Информационная безопасность – основы [Электронный ресурс] // Системы управления базами данных. 1996. № 1. URL: https://www.osp.ru/dbms/1996/01/13031466 (Дата обращения: 15.01.2022)

вопросы ИБ отошли на второй план»[342]. Директор департамента проектирования компании «Газинформсервис» Александр Калита, со своей стороны, подчеркивает, что в 2021 году высокий уровень информационной безопасности является конкурентным преимуществом для бизнеса[343]. Хотя многие представители IT-бизнеса и критиковали установленные нормы государственного контроля в области ИБ как осложняющие деятельность предприятий, они, в то же время, были заинтересованы в дальнейшем развитии технологий и услуг ИБ и, соответственно, во внедрении требований законодательства в российскую экономику и бизнес. Так, например, Компания «СёрчИнформ» на своем сайте призывает пользователей «не пренебрегать рекомендациями и требованиями ФСТЭК по защите информации», подчеркивая, что происходящая из-за беспечности утечка персональных данных и других сведений «может в итоге привести к значительным убыткам»[344].

В данном контексте в России XXI в. складывается широкое дискуссионное пространство о социальной ответственности СМИ и делового мира в плане обеспечения информационной безопасности общества. В период конца 1980-х – начала 1990-х гг. российское журналистское сообщество приняло ряд концептуальных документов, отражавших общественную позицию ведущих СМИ: Кодекс профессиональной этики советского журналиста (1989), Московскую Хартию журналистов (1994) и Кодекс профессиональной этики российского журналиста (1994), положения которого являются актуальными для профессиональной журналистики России в настоящее время. В Кодексе 1994 г. в частности, зафиксирована моральная обязанность журналиста распространять и комментировать только

---

[342] *Степанова Ю.* Кибербезопасность ощутила зарегулированность [Электронный ресурс] // Коммерсант. 3 апреля 2020 г. URL: https://www.kommersant.ru/doc/4311090 (Дата обращения: 17.02.2022)

[343] Интервью с экспертами [Электронный ресурс] // Электронное издание Anti-Malware.ru. URL: https://www.anti-malware.ru/interviews (Дата обращения: 17.02.2022)

[344] О компании [Электронный ресурс] // Сайт компании «СёрчИнформ» URL: https://searchinform.ru/company/ (Дата обращения: 16.02.2022)

достоверную информацию, а также прилагать все усилия к тому, чтобы неточность информации, распространение ложных сведений, либо, напротив, сокрытие общественно значимой информации, не нанесло какого-либо ущерба обществу или конкретному лицу. Клевета, злонамеренные искажения фактов, получение платы за подобные действия трактуются как профессиональные преступления. При этом в Кодексе подчеркивается, что журналист признает за организациями и гражданами не предоставлять информацию, за исключением случаев, оговоренных законом, а также не раскрывает источники информации, полученной конфиденциально[345].

Вопрос о роли СМИ в контексте информационной безопасности как таковой в вышеперечисленных документах российского журналистского сообщества не ставился. Однако в XXI в. эта тема все чаще оказывается в центре корпоративных и более широких общественных дискуссий, в том числе в формате СНГ. Вопросы социальной ответственности СМИ обсуждаются на Международном фестивале журналистов «Вся Россия», проводимом ежегодно с 1997 г., медиа-форумах и конференциях различного формата. В ноябре 2020 г. состоялся российско-белорусский экспертно-медийный форум «Информационная безопасность Союзного государства: современные вызовы и новые технологии», в котором приняли участие представители центральных и региональных СМИ двух стран. Ведущие деятели российских СМИ неизменно подчеркивают, что роль журналистики в контексте проблемы информационной безопасности определяется не только рамками действующего законодательства, но и этическими нормами, охватывающими и взаимодействие журналиста с его аудиторией, и внутрикорпоративные установки, политику конкретного издания или телеканала[346].

---

[345] Кодекс профессиональной этики российского журналиста Союза журналистов России. Принят Конгрессом журналистов России 23 июня 1994 г. [Электронный ресурс] // Официальный сайт Союза журналистов России. URL: https://www.ruj.ru (Дата обращения: 16.02.2022)

[346] *Тулупов В.В.* Региональная журналистика: сегодня и завтра // Вопросы теории и практики журналистики. 2013. № 2. С. 78-92; *Шайхутдинова Л.С.* Социальная

В 2010-х гг. отмечается сближение социальных функций (миссий) профессиональных журналистов и активных участников сетевых коммуникаций – блогеров, модераторов, лидеров сообществ, которые в связи с этим должны действовать «не забывая об информационной безопасности, которая в современном мире становится все более актуальной»[347].

Таким образом, в XXI в. практически все страты российского общества в большей или меньше степени становятся акторами информационного пространства. Соответственно растет заинтересованность общества в целом и каждого человека в обеспечении информационной безопасности, включая как доступ необходимой, социально и экономически значимой информации, так и защиту данных, требующих ограничения доступа. В этой связи наблюдается встречное движение государства, которое формирует нормативно-правовую базу и инфраструктуру информационной безопасности, и общественных институтов (бизнеса, ведущих СМИ, научных и гуманитарных организаций, ответственных пользователей Интернета), берущих на себя часть ответственности за создание в России безопасной информационной среды.

Важным компонентом этого процесса является развитие науки и образования в сфере информационных технологий, создающих фундамент для дальнейшего формирования в России постиндустриального информационного общества, для эффективного обмена знаниями между профессиональными поколениями IT-специалистов и повышения компьютерной грамотности населения страны, в том числе в сфере информационной безопасности.

ответственность средств массовой информации в современных условиях // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2016. № 12 (74): в 3-х ч. Ч. 3. С. 206-208;

[347] Информационная безопасность и свобода слова: точки взаимодействия // Медиа Тренды. 30 мая 2019. № 4 (67). С.1.

2.4. Система подготовки специалистов в области информационной безопасности России

Процесс формирования корпуса квалифицированных специалистов, обеспечивающих реализацию государственной политики информационной безопасности, а также интересы граждан и бизнеса в данной сфере, в 1991 – начале 2000-х гг. носил противоречивый характер, что было во многом обусловлено и общей спецификой развития профессионального образования в этот период[348].

С одной стороны, существовавшая, как уже упоминалось выше, в период позднего СССР увлеченность научно-технической интеллигенции и студенчества компьютерными технологиями способствовала появлению довольно многочисленной прослойки лиц, профессионально работавших в сфере IT, в том числе проявлявших интерес к вопросам информационной безопасности. Один из представителей российского IT-сообщества, который окончил институт в 1991 г. и работал программистом в торговавшей компьютерами фирме «Ниеншанц», вспоминал: «Нам казалось очень важным обеспечивать пессимистичную блокировку – если кто-то вошел в документ, то никто другой войти не мог бы»[349]. IT-специалисты, которым удалось в первые годы реформ трудоустроиться в частном секторе, имели относительно хорошие заработки. «Лично для меня это было очень оптимистичное время, – пишет тот же мемуарист. – Я купил видик (Электроника ВМ-12)… А в 95-м году купил свой первый автомобиль – Таврия»[350]. При этом образование в сфере информационных технологий, как

---

[348] *Жуков В.И.* Российское образование: истоки, традиции, проблемы. М., 2001; *Горбунов А.П.* Российская высшая школа в условиях рыночных реформ 1990-х гг. // Новый исторический вестник. 2006. № 1(14). С. 181-207.

[349] IT в «лихие 90е» – из воспоминаний бумера [Электронный ресурс] URL: https://habr.com/ru/post/541160/ (Дата обращения: 25.01.2022).

[350] Там же.

и большинство отраслей инженерного образования в конце 1980-х – начале 1990-х гг. не было престижным[351].

Во второй половине 1990-х – 2000-е гг. вследствие интеграции России в глобальное информационное общество, становления и быстрого расширения российского рынка информационных услуг, а также связанного с ним рынка электроники, компьютерной техники и программного обеспечения, увеличился спрос на специалистов в области информационных технологий, в том числе обладающих компетенциями в сфере информационной безопасности. Соответственно, возросли и предложения со стороны высшей и средней специальной школы в области подготовки IT-специалистов[352]. Помимо ведущих отечественных технических вузов, военных академий и училищ, образовательных учреждений правоохранительных ведомств и органов безопасности, традиционно осуществляющих подготовку кадров специалистов высокого класса в области электроники, радиотехники, связи, новые специальности информационного профиля начали открываться во многих государственных и коммерческих вузах.

С другой стороны, в процессе преобразования отечественной системы государственной безопасности, осуществлявшегося в первой половине 1990-х гг., происходило сокращение кадров спецслужб, переход многих квалифицированных специалистов в области информатики и связи в частный бизнес, другие сферы деятельности[353]. Эта тенденция негативно проявилась в ходе антитеррористических операций 1990-х гг. на Северном Кавказе, в особенности в период первой Чеченской кампании, показавшей недостаточно высокий технический уровень защищенности оперативной связи российских

---

[351] «Потерянные ребята» из IT: история программиста из 90-х. [Электронный ресурс] URL: https://techrocks.ru/2020/10/12/programmer-from-90s-it-history/ (Дата обращения: 25.01.2022).

[352] *Prokhorov S.P.* Computers in Russia: Science, Education, and Industry // IEEE Annals of the History of Computing. 1999. Jul-Sept. Vol. 21. № 3.

[353] *Есипов В.А.* Реформы органов госбезопасности в России и государствах бывшего СССР в 1990-е годы и мировая система их организации. С. 448.

военных и сил МВД[354]. Данное обстоятельство, по мнению историков российских спецслужб, стало одной из причин решения Президента России В.В. Путина об упразднении ФАПСИ[355].

В 2003-2004 гг. была преобразована система специализированных вузов, находившихся в предшествующий период в ведении ФАПСИ. Среди них были Академия ФАПСИ (бывшее Орловское высшее военное командное училище связи им. М.И. Калинина, в 1992–2000 гг. Военный институт правительственной связи – ВИПС), Воронежское военно-техническое училище (основано в 1998 г.), Академия криптографии и другие военно-учебные центры, перешедшие главным образом в систему Федеральной службы охраны. На базе бывшей Академии ФАПСИ была образована Академия Службы специальной связи и информации при ФСО или Академия спецсвязи, с 2004 г. – Академия ФСО РФ. В 2008 г. Воронежское военно-техническое училище ФСО стало филиалом Академии. Вуз осуществляет подготовку квалифицированных специалистов в области установки и функционирования многоканальных телекоммуникационных систем, радиовещания и ряда других технологических видов связи, а также информационной безопасности телекоммуникационных систем и правовому обеспечению национальной безопасности. Как отмечает историк российских спецслужб И. Полонский, переход в систему Федеральной службы охраны образовательных учреждений стал «особым событием» в истории Службы, позволившим ФСО внести значительный вклад в формирование кадровой и научно-теоретической базы государственной политики национальной, в том числе информационной безопасности России в XXI в.[356]

В течение периода 2000 – 2010-х гг. институциональная и методическая база подготовки кадров для системы информационной безопасности России

---

[354] *Полонский И.* День ФАПСИ (1991-2003). Слово о правительственной связи // Военное обозрение. 24 декабря 2015 г. URL: https://topwar.ru/88409-den-fapsi-1991-2003-slovo-o-pravitelstvennoy-svyazi.html (Дата обращения: 25.01.2022)

[355] Там же.

[356] Там же.

выходит на новый уровень развития[357]. В ряде российских вузов, в том числе в регионах, научно-методические разработки в области подготовки специалистов в области информационной безопасности активно велись уже в 1990-е гг.[358] Начавшаяся в 2000-е гг. в Российской Федерации модернизация образовательной системы предполагала обновление спектра специальностей и образовательных направлений высшей и средней профессиональной школы в соответствии с потребностями государства и общества, в том числе учитывалось развитие информатизации во всех сферах жизни и переход на новый качественный уровень информационных технологий. Приказом Министра образования России от 2 марта 2000 г. № 686) был утвержден (с последующими уточнениями новый «Перечень направлений подготовки и специальностей высшего профессионального образования», в котором подготовка специалистов в области информационной безопасности выделялась в самостоятельный раздел. В группу специальностей высшего образования по направлению «Информационная безопасность были включены криптография и компьютерная безопасность с квалификациями выпускника – «математик»), специальности, ориентированные на обеспечение безопасности объектов – «организация и методология защиты информации» и «комплексная защита объектов информации» (квалификация выпускника – «специалист по защите информации»), и на управление технологическими системами – «комплексное обеспечение информационной безопасности автоматизированных систем» и «информационная безопасность телекоммуникационных систем» (квалификация выпускника – «специалист по защите информации»)[359]. Таким образом, происходило

---

[357] *Galushkin A.A.* Education in the field of national information security in the Russian Federation and abroad // Journal of Computer Science. 2015. Vol. 11. No 10. P. 988-994. DOI 10.3844/jcssp.2015.988.994

[358] *Ильюшенко В.Н.* Информационная безопасность общества: Учебное пособие / Томский государственный университет систем управления и радиоэлектроники. Томск, 1998. 64 с.

[359] Приказ Министерства образования РФ от 8 ноября 2000 г. № 3200 «О частичном изменении приказа Минобразования России от 02.03.2000 № 686 «Об утверждении государственных образовательных стандартов высшего профессионального образования» [Электронный ресурс] URL: https://base.garant.ru/5347960/ (Дата обращения 15.02.2022)

формирование двух основных групп профессионалов в сфере информационной безопасности: специалистов по комплексному обеспечению информационной безопасности и непосредственно по цифровым и коммуникационным технологиям.[360] Оба направления образовательной деятельности развивались на базе ведущих технологических вузов страны.

Сфера подготовки кадров для систем информационной безопасности в России, как и во всем мире, развивается в условиях цифровой революции XXI в., перманентных быстрых изменений в сфере технологий и моделей информационных коммуникаций. Соответственно, перед учебными заведениями, действующими в данном секторе, стоят задачи обновления образовательных программ и формирования у студентов навыков самостоятельного профессионального роста[361]. Возникает также необходимость расширения спектра специальностей в области информационной безопасности. 12 сентября 2013 г. Министерство образования и науки РФ утвердило Перечень направлений подготовки высшего образования с укрупненной группой специальностей по направлению 10.00.00 – Информационная безопасность. В состав Учебно-методического объединения (УМО) вузов по образованию в области информационной безопасности к 2016 году входило более 60 вузов, главным образом технологического профиля[362]. Сложился круг новых востребованных

---

[360] *Астахова Л.В.* Развитие управленческой компетенции будущего специалиста по защите информации в вузе // Современные проблемы науки и образования, 2012. № 6. С. 330-336.

[361] *Авсентьев О.С., Прийма В.Н., Малышев А.А., Дураковский А.П.* Системные аспекты проблематики подготовки специалистов в области информационной безопасности. //Информационная безопасность. 2009. № 4. С. 621-622; *Новиков Д.А., Борисов В.И., Остапенко А.Г., Калашников А.О., Соколова Е.С.* Инновационные тренды в организации учебного процесса специалистов по защите информации: формирование компетенций в области управления информационными рисками и обеспечения безопасности инфокоммуникационных технологий // Информация и безопасность. 2014. Т. 17. № 3. С. 360-365.

[362] *Кузнецова З.Н.* Обеспечение информационной безопасности Российской Федерации // Вестник образовательного консорциума Среднерусский университет. Информационные технологии. 2016. № 2(8). С.58

профессий: архитектор ИБ, аналитик ИБ, специалист сетевой безопасности, специалист по аудиту и аттестации объектов информатизации и др.[363]

В ноябре 2016 г. на площадке Московского технологического университета МИРЭА состоялся XX юбилейный Пленум Федерального учебно-методического объединения в системе высшего образования по укрупнённой группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ). МТУ МИРЭА и ФГУП НИИ «Восход» была организована Российская научная конференция «Интеллектуальные системы в информационном противоборстве»[364]. В декабре 2017 г. аналогичная конференция была проведена силами МИРЭА, РЭУ им. Г.В. Плеханова и НИИ «Восход»[365]

В 2020 г. ФСТЭК объявила о введении новых, более высоких требований к образованию и квалификации специалистов, работающих в системах обеспечения безопасности критической информационной инфраструктуры России. Как поясняли представители руководства Службы, ведомство не располагало достаточным количеством грамотных специалистов, которые могли бы эффективно реализовывать требования российского законодательства о КИИ. «Поэтому по просьбе трудящихся, про просьбе субъектов мы ввели в свои нормативные документы требования к образованию и квалификации тех, кто будет работать с КИИ, кто будет их защищать», – сказала заместитель начальника управления ФСТЭК Е. Торбенко[366]. С 1 января 2021 г. к руководителям структурных

---

[363] *Бурькова Е.В.* Профессиональная подготовка специалистов в области информационной безопасности // Вестник Оренбургского государственного университета. 2016. № 2(190). С. 3-9.

[364] Электронный архив ФУМО ВО ИБ. Текущие события. 2016 г. URL: http://www.isedu.ru/ (Дата обращения 15.02.2022)

[365] Интеллектуальные системы в информационном противоборстве: сборник научных трудов Российской научной конференции, Москва, 15–17 декабря 2017 года. Под ред. Ю.Ф Тельнова и др. М.: Российский экономический университет имени Г.В. Плеханова, 2018. Т.1. 446 с.

[366] ФСТЭК вводит новые требования к образованию и квалификации тех, кто будет работать с КИИ // «BIS Journal − Информационная безопасность банков». 17 сентября 2020 г. URL: https://ib-bank.ru/bisjournal/news/14213 (Дата обращения: 17.02.2022)

подразделений по безопасности субъектов КИИ предъявлялись следующие требования: наличие высшего профессионального образования по направлению «Информационная безопасность», либо иное высшее образование при условии прохождения профессиональной переподготовки в области информационной безопасности, а также наличие стажа работы по профилю информационной безопасности не менее трех лет. Штатные работники структур обеспечения информационной безопасности КИИ также должны иметь профильное высшее профессиональное образование, либо, при наличии диплома об ином высшем образовании пройти курс переподготовки по направлению «Информационная безопасность». Не реже чем раз в 5 лет все сотрудники системы обеспечения безопасности КИИ обязываются проходитm программы повышения квалификации[367].

Крупным научно-образовательным центром данного профиля выступает Национальный исследовательский университет «Московский институт электронной техники» (НИУ «МИЭТ»), где подготовка кадров в области информационной безопасности началась с 1997 г.[368] В структуре университета действует целый ряд подразделений, обеспечивающих подготовку квалифицированных специалистов в области электротехники и новейших информационных технологий: Институт микроприборов и систем управления (МПСУ), реализующий образовательные направления «Информатика и вычислительная техника», «Радиотехника», «Управление в технических системах», Институт системной и программной инженерии и информационных технологий (СПИНТех), Институт нано- и микросистемной техники (НМСТ), Военно-учебный центр (ВУЦ), где можно получить второе высшее (военное) образование, и др. Кроме того в НИУ «МИЭТ» осуществляется подготовка специалистов по направлениям

[367] ФСТЭК вводит новые требования к образованию и квалификации тех, кто будет работать с КИИ // «BIS Journal − Информационная безопасность банков». 17 сентября 2020 г. URL: https://ib-bank.ru/bisjournal/news/14213 (Дата обращения: 17.02.2022)
[368] МИЭТ 50 лет. Годы, люди, события. М.: МИЭТ, 2015. 392 с.

«Информационные системы и технологии», «Информационная безопасность», «Правовое обеспечение национальной безопасности».

Кафедра информационной безопасности МИЭТ была образована в 2011 г. и быстро завоевала авторитет в научно-образовательном сообществе: в 2015 г. она стал лауреатом премии «Инфофорум – Новое поколение» в номинации «Образовательный центр года»[369]. На кафедре открыты два основных направления подготовки специалистов в области информационной безопасности – по профилю «Техническая защита информации» (бакалавриат) и программа «Аудит информационной безопасности автоматизированных систем» (магистратура). При кафедре действует четыре специализированных лаборатории, в том числе «Технологий и программно-аппаратных средств обеспечения информационной безопасности» и «Технологий и управления информационной безопасностью»[370]. Профессорско-преподавательский коллектив кафедры составляют «люди, проработавшие не один десяток лет в области информационной безопасности в различных ведомствах, в том числе и силовых, и имеющие большой педагогический и научный опыт»[371]. Студенты проходят практику в ведущих организациях и компаниях, занимающихся вопросами информационной безопасности, а также ежегодно участвуют в Добровольном квалификационном экзамене в области информационной безопасности, который проводит Правительство города Москвы, где в большинстве своем набирают высокие баллы. Выпускники кафедры востребованы в крупных компаниях, государственных учреждениях, правоохранительных органах[372].

В число лидеров подготовки специалистов в области техники и технологий, востребованных в сфере информационной безопасности, входит

---

[369] Кафедра информационной безопасности [Электронный ресурс] // Сайт НИУ «МИЭТ» URL: https://www.miet.ru/structure/s/1270 (Дата обращения 15.02.2022)
[370] Там же.
[371] Кафедра ИБ: как и чему учат тех, кто предотвращает утечки информации: Интервью с профессором А.В. Душкиным [Электронный ресурс] // Сайт НИУ «МИЭТ». 27 июля 2020 г. URL: https://www.miet.ru/news/128216(Дата обращения 15.02.2022)
[372] Там же.

Московский государственный технический университет (МГТУ) им. Н.И. Баумана. На кафедру «Информационные технологии» конкурс абитуриентов по ЕГЭ составлял в 2010-х гг. до 166 человек на место. Выпускники кафедры являются специалистами в области программирования, криптографии, стеганографии[373], организационно-правового обеспечения информационной безопасности и др. Выпускники кафедры работают в ведущих IT-компаниях России – Яндекс, Лаборатория Касперского и др.[374] Под эгидой МГТУ действует Центр компьютерного обучения «Специалист», который ведет образовательную деятельность в лучших традициях «бауманки» с упором на практическую работу в сфере IT, в том числе предлагает обучение и переподготовку по направлению «Информационная безопасность». В Центре проходили обучение сотрудники «Лаборатории «Касперского», Росэнергоатома, Банка «Возрождение», Почты России» и многих других компаний и организаций[375].

«Наверное, самым продвинутым ВУЗом России в области информационных и фотонных технологий» с высоким уровнем подготовки и не менее высокими требованиями к студентам является, по мнению эксперта одного из молодежных рекламно-образовательных сайтов, Санкт-Петербургский НИУ «Институт точной механики и оптики» (ИТМО)[376]. В Университете ИТМО имеются факультет безопасности информационных технологий (ФБИТ) и факультет инфокоммуникационных технологий и систем связи (ФИКТ), ведется подготовка по образовательным программам «Технологии зашиты информации», «Организация и технология зашиты

[373] Стеганография – способ передачи или хранения данных при сохранении в тайне самого факта такой передачи (хранения), дословно «скрытопись» (прим. авт.).
[374] Вузы по кибербезопасности: Где учат специалитсов по инфобезу? [Электронный ресурс]. URL: https://storedigital.ru/2019/11/16/vuzy-po-kiberbezopasnosti-gde-uchat-specialistov-po-infobezu/ (Дата обращения 15.02.2022)
[375] Информационная безопасность [Электронный ресурс] // Сайт Учебного центра при МГТУ им. Н.И. Баумана. URL: https://www.specialist.ru/section/information-security?utm_source=yandex&utm_medium=cpc&utm_campaign= (Дата обращения 15.02.2022)
[376] Там же.

информации», «Программирование в инфокоммникационных системах» и др.[377]

На факультете радиотехники и телекоммуникаций Санкт-Петербургского государственного электротехнического университета (СПбГЭТУ «ЛЭТИ») действуют базовые кафедры средств специальной радиоэлектроники (ССР), радиоэлектронных информационных систем и комплексов (РИСК), радиоэлектронных средств, микрорадиоэлектроники и технологии радиоаппаратуры и др.[378] Факультет компьютерных технологий и информатики СПбГЭТУ осуществляет подготовку квалифицированных кадров по направлениям «Информатика и вычислительная техника». «Автоматизация и управление», «Управление в технических системах», «Информационные системы и технологии», «Программная инженерия», «Прикладная математика и информатика» и др. В структуре факультета действует самостоятельная кафедра информационной безопасности, которая готовит специалистов, обладающих «комплексными знаниями в области информационной безопасности, способных выполнять работы по созданию защищенных компьютерных технологий»[379]. Выпускники кафедры обладают компетенциями, которые позволяют им решать задачи в области мониторинга информационных угроз и разработки типовых механизмов оперативного реагирования с целью их устранения или минимизации последствий, а также осуществлять работу в области развития систем защищенных компьютерных технологий в целях повышения их эффективности, в том числе в условиях «целенаправленного информационного противодействия (информационных войн)»[380].

---

[377] Образование. Направления и специальности. [Электронный ресурс] // Свйт ИТМО. URL: https://itmo.ru/ru/page/169/obrazovanie.htm(Дата обращения 15.02.2022)

[378] Факультет радиотехники и телекоммуникаций [Электронный ресурс] // Сайт СПбГЭУ «ЛЭТИ». URL: https://etu.ru/ru/fakultety/fakultet-radiotehniki-i-telekommunikaciy/ (Дата обращения 15.02.2022)

[379] Кафедра информационной безопасности [Электронный ресурс] // Сайт СПбГЭУ «ЛЭТИ». URL: https://etu.ru/ru/fakultety/fkti/sostav/kafedra-cs/ (Дата обращения 15.02.2022)

[380] Там же.

В структуре Российского университета дружбы народов (РУДН) действует Инженерная академия, которая выпускает специалистов по направлению «Фундаментальная информатика и информационные технологии», в том числе со специализацией по информационной безопасности. На сайте РУДН отмечается, что современный специалист в области информационной безопасности должен обладать глубокими компетенциями как в IT-сфере, так и в области «нормативно-правовых знаний, применения организационных и технических мер защиты информации»[381].

Подготовка кадров для системы информационной безопасности ведется также в РГУ нефти и газа им. И.М. Губкина, НИУ «МЭИ», Российском университете транспорта «МИИТ», Московском физико-техническом институте (МИФИ) и др., Оренбургском, Саратовском, Томском и ряде других классических университетов[382]. В Республике Башкортостан образовательное направление «Информационная безопасность» реализуется в Уфимском государственном авиационном техническом университете (УГАТУ), Башкирском государственном университет (БашГУ) и двух его филиалах – в Нефтекамске и Стерлитамаке. Программа бакалавриата «Цифровые технологии и защита информации» открыта в Уфимском государственном нефтяном техническом университете (УГНТУ).

Образовательные программы и программы профессиональной переподготовки по направлению «Информационная безопасность», которые реализуются в вузах и специализированных учебных центрах, проходят согласование в ФСБ России[383].

---

[381] Технологии защиты информации. О профессии [Электронный ресурс] // Сайт РУДН. URL: https://www.rudn.ru/education/educational-programs/53816 (Дата обращения 15.02.2022)

[382] Вузы по кибербезопасности: Где учат специалитсов по инфобезу.? [Электронный ресурс]. URL: https://storedigital.ru/2019/11/16/vuzy-po-kiberbezopasnosti-gde-uchat-specialistov-po-infobezu/ (Дата обращения 15.02.2022)

[383] Сайт ФУМО ВО ИБ. URL: http://www.isedu.ru/documents.dopprof/index.htm(Дата обращения 15.02.2022)

Следует отметить, что вузы различной ведомственной принадлежности (Минобразования РФ, Министерства обороны, ФСБ и др.), осуществляющие подготовку специалистов для российских систем информационной безопасности, взаимодействовали между собой в научно-исследовательской и образовательной сфере. Представители профессорско-преподавательского корпуса, аспиранты и студенты данной группы образовательных учреждений совместно участвовали в научных конференциях, публиковали статьи в журналах «Информационная безопасность», «Информационное общество» и др.

С 2017 г. Департамент информационных систем Минобороны России и 8-е управление Генштаба Вооруженных Сил РФ выступают организаторами различных программ и проектов в области киберспорта и кибоербезопасности, которые проводятся под эгидой движения «Киберпатриот», в том числе викторин, конкурсов и соревнований среди школьников и молодежи. Так, в 2019 г. был проведен Всероссийский турнир по кибербезопасности «Стальная стена – 2019» для воспитанников довузовских учебных заведений Министерства обороны РФ и состоялись Первые Всероссийские соревнования по кибербезопасности «Киберпатриот 2019». В ноябре того же года была торжественно открыта совместная спортивная киберплощадка Минобороны России и компании «Ростелеком»[384]. В мероприятиях «Киберпатриота» в 2020 г. приняли участие более 100 команд из 27 городов России, объединивших более 450 молодых людей и девушек (юниоров, специалистов и курсантов)[385].

19 декабря 2020 г. состоялся финал Всероссийских соревнований по кибербезопасности «Эшелонированная оборона – 2020». Участниками проекта стали 65 студенческих команд, из которых до финала дошли 20 сильнейших, в том числе будущие специалисты в области информационной безопасности из Университета ИТМО (первое место) Академии ФСО России

[384] История движения «Киберпатриот» [Электронный ресурс] // Сайт платформы «Киберпатриот». URL: https://cyberpatriot-ctf.ru/history/ (Дата обращения 15.02.2022)
[385] Там же.

(второе место), МАИ, МГТУ им. Н.Э. Баумана, НИУ МЭИ, НИУ МИЭТ, Национального исследовательского ядерного университета МИФИ и др. Команда Академии ФСО показала также лучший результат среди военных вузов[386].

Растущая общественная значимость вопросов теории и практики информационной безопасности в России начала XXI в., появление новых программных документов и нормативно-правовых актов, отражающих растущее значение темы информационной безопасности в развитии российской государственности, бизнесе, частной жизни граждан, обусловило создание кафедр и научно-образовательных центров информационной безопасности в вузах финансового, управленческого, социально-культурного профиля. Российскими специалистами разрабатывается теория комплексного междисциплинарного подхода к подготовке кадров в области информационной безопасности[387].

Выходят в свет учебные пособия и научно-методические комплексы, посвященные правовым, политологическим, дипломатическим, философским аспектам информатизации и информационной безопасности. Одним из первых крупных центров развития гуманитарного подхода к проблемам информационной безопасности стал Санкт-Петербургский государственный университет, где сложилась творческая группа ученых, исследовавших проблемы информационной безопасности в контексте становления глобального информационного общества. В 1999 г. коллективом авторов СПбГУ под руководством М.А. Вуса было подготовлено учебное пособие, раскрывающие взаимосвязь процессов информатизации и вопросов обеспечения информационной безопасности государственных институтов и

---

386 Эшелонированная оборона 2020 [Электронный ресурс] // Сайт Академии ФСО. https://alt.academ.msk.rsnet.ru/research/reach URL: (Дата обращения 15.02.2022)

387 *Згадзай О.Э.* Вопросы подготовки специалистов в области информационной безопасности // Вестник Казанского юридического института МВД России. 2013. № 3(13). С. 93-97; *Царегородцев А.В., Цацкина Е.П.* Влияние информационного общества на подготовку обучающихся в сфере информационной безопасности // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2019. № 4(833). С. 191-199 и др.

общества России[388]. В 2000 г. в издательстве Санкт-Петербургского университета вышло учебно-методическое пособие «Государственная тайна в Российской Федерации»[389].

В 2003 г. был основан Институт проблем информационной безопасности МГУ имени М.В. Ломоносова, в структуру которого входят два отдела – математических проблем информационной безопасности и гуманитарных проблем информационной безопасности, а также Центр международного научного сотрудничества по проблемам безопасности и противодействия терроризму. Научные разработки специалистов Центра вносят важный вклад в формирование теоретических представлений по проблемам информационной безопасности и их отражение в образовательном процессе МГУ им. М.В. Ломоносова.

В разные годы учебную литературу по теме информационной безопасности выпускали российские экономические вузы и факультеты университетов, в том числе экономический факультет МГУ им. М.В. Ломоносова[390]. Ведомственные вузы правоохранительных органов уделяют внимание подготовке юристов, специализирующихся в области информационного права и безопасности[391].

---

[388] Информационное общество: Информационные войны. Информационное управление. Информационная безопасность: [Учебное пособие] / Виноградова С.М., Войтович Н.А., Вус М.А., Кульба В.В., Малюгин В.Д. Под ред. М.А. Вуса. СПб: Изд-во Санкт-Петербургского университета (СПбГУ), 1999. 211 с.

[389] Государственная тайна в Российской Федерации. Учебно-методическое пособие. / Аникин П.П., Балыбердин А.Л., Вус М.А., Гусев В.С., Рябчук В.Н., Федоров А.В. – СПб: Изд-во Санкт-Петербургского университета, 2000.

[390] Информационная безопасность: Учебное пособие / Кирсанов К.А., Малявина А.В., Попов Н.В. Московская академия экономики и права. – М.: Калита, 2000 229 с.; *Одинцов А.А.* Экономическая и информационная безопасность. Справочник: Учебное пособие для студентов вузов, обучающихся по специальности «Национальная экономика» и другим экономическим специальностям. М.: Экзамен, 2005. 575 с.; *Баданов А.Г.* Информационная безопасность: от теории к практике: учебное пособие / Московский государственный университет им. М.В. Ломоносова. Экономический факультет. М.: ТЕИС, 2010. 127 с. и др.

[391] Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности / В.Ю. Рогозин, И.Б. Галушкин, В.К. Новиков, С.Б. Вепрев. Московская академия следственного комитета. М.: ЮНИТИ-ДАНА, 2017. 287 с.

В число пионеров создания направлений высшего образования в сфере информационной безопасности, объединяющих технологическую и гуманитарную сферу, входит Российский государственный гуманитарный университет (РГГУ). В 1985 г. в Московском государственном историко-архивном институте (МГИАИ), который с 1991 г. входит в структуру РГГУ, начал действовать факультет специального документоведения, где была открыта специальность «Инженер-организатор специальных работ». Во второй половине 1980-х гг. на факультете действовали кафедры по организационно-правовой защите информации, по организации специального делопроизводства и по инженерно-технической защите информации, велась работа в области теории и методики информационной безопасности делопроизводства и архивов. В 1990 г. на этой основе был создан факультет защиты информации, его образовательная и научная деятельность стала проводиться в открытом режиме. С 1999 по 2011 г на факультете велась подготовка по специальности «Юриспруденция» со специализацией «Организационно-правовая защита информации», а с 2000 г.– также по специальностям «Организация и технология защиты информации» и «Комплексная защита объектов информатизации». С 2011 г. РГГУ реализует программу бакалавриата по направлению «Информационная безопасность»[392].

Вопросы информационной безопасности включены в образовательные программы и научно-информационные проекты факультета журналистики МГУ им. М.В. Ломоносова. Главное внимание при подготовке будущих деятелей СМИ уделяется вопросам журналистской этики, законодательству о СМИ, методам противодействия деструктивному контенту в Интернете и др. В 2011 г. был выпущен тематический номер «Информационная безопасность» выходящего на факультете информационно-аналитического бюллетеня «МедиаТренды». В колонке редактора, открывающей номер, в

[392] Краткая историческая справка ФИСБ ИИНТБ [Электронный ресурс] // Сайт РГГУ. URL: https://www.rsuh.ru/upload/iintb|История ФИСБ.pdf (Дата обращения: 15.02.2022).

частности, говорилось: «Механизмы соблюдения этических норм, норм информационной безопасности и механизмы свободы слова прекрасно сосуществуют друг с другом, если вспомнить концепцию социальной ответственности в СМИ»[393].

Заметный вклад в развитие научно-теоретических основ международной информационной безопасности и внедрение проблематики защиты информации в подготовку квалифицированных кадров российских дипломатов и политологов вносит университет МГИМО МИД России, в структуре которого создан Центр международной информационной безопасности и научно-технологической политики, выходят в свет учебно-методические пособия и научные монографии по проблемам информационной безопасности[394].

Таким образом, в течение периода 1990-х – 2010-х гг. отечественная система подготовки кадров специалистов в области информационной безопасности формировалась под влиянием осуществлявшихся в стране реформ органов исполнительной власти, Вооруженных Сил РФ, структур госбезопасности, в ведении которых находился ряд ведущих специализированных учебных заведений технологического профиля. Не менее важными факторами развития данного образовательного направления стали информатизация российского общества и связанный с ней рост информационных рисков для государственного управления и бизнеса.

Подводя итог рассмотрению процесса институционализации системы информационной безопасности в Российской Федерации в 1991 – 2010-е гг., можно сделать следующие выводы:

---

[393] Медиа Тренды. 2011. № 28. [Электронный ресурс] // Сайт факультета журналистики МГУ им. М.В. Ломоносова. URL: https://www.journ.msu.ru/about/mediatrends/4084/ (Дата обращения: 15.02.2022).

[394] *Меньшиков П.В.* Информационная политика России: учебное пособие. М.: МГИМО, 2017. 212 с.; *Федоров А.В., Зиновьева Е.А.* Информационная безопасность: политическая теория и дипломатическая практика: монография Московский государственный институт международных отношений (университет) МИД России (МГИМО), Центр международной информационной безопасности и научно-технологической политики (Москва). М.: МГИМО- Университет, 2017. 357 с.

Проведенное в России 1990-х – начала 2000-х гг. реформирование системы органов исполнительной власти и спецслужб обусловило становление новых концептуальных и правовых подходов к деятельности институтов защиты государственной и служебной тайны. Вместе с тем, переустройство институтов информационной безопасности, проводившееся в первой половине 1990-х гг. методом проб и ошибок, привело к частичной утрате кадрового и технологического потенциала отрасли. В 1996 г. были созданы основы современной системы федеральных институтов государственной безопасности Российской Федерации, ведущими компонентами которой стали Федеральное агентство правительственной связи и информации (ФАПСИ) и Гостехкомиссия при Президенте РФ. К концу 1990-х гг. была в целом сформирована система структур информационной безопасности в органах власти и управления на федеральном и региональном уровне, в ведущих банках и стратегически значимых предприятиях. Институты исполнительной власти, ответственные за обеспечение информационной безопасности находились в постоянном взаимодействии с российским обществом, выполняя задачи в области лицензирования и сертификации деятельности участников рынка компьютерной техники и ПО, формируя с позиций информационной безопасности нормативное пространство работы СМИ и социальных сетей, противодействуя киберпреступности, иностранным техническим разведкам и другим деструктивным явлениям, связанным с информатизацией. При этом складывались различные модели и формы диалога и интеграции государственных и общественных институтов информационной безопасности.

В 2000-е гг. в контексте политики совершенствования системы государственного управления и образовательной реформы в России, начинается качественно новый, модернизационный этап становления современной системы высшего профессионального образования как непосредственно по направлению «Информационная безопасность», так и

широкому спектру технологических специальностей в области информационных технологий, необходимых для реализации задач информационной безопасности.

В XXI в. образовательное направление «Информационная безопасность» получает научно-методическое обоснование, осуществляется его реализация ведущими технологическими вузами, университетами и факультетами финансово-экономического и гуманитарного профиля, растет востребованность квалифицированных специалистов в области информационной безопасности, развиваются межведомственные научно-методические и кадровые связи образовательных учреждений и научно-исследовательских центров, занимающихся проблематикой информационной безопасности.

Глава III. ИНСТИТУТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

3.1. Деятельность Совета Безопасности РФ и комитетов Государственной Думы РФ в сфере формирования государственной информационной политики

Перед центральными органами власти России 1990-х гг. стоял комплекс сложных задач по формированию новой системы государственного управления, включая институты безопасности. Как уже отмечалось выше, концептуальные подходы и правовые нормы, которые характеризовали политику информационной безопасности, на тот момент находились в стадии становления.

Президент России Б.Н. Ельцин 3 июня 1992 г. подписал распоряжение о деятельности Совета безопасности Российской Федерации, в котором, в частности, излагались и первоочередные задачи Совета:

1. организация подготовки материалов к президентскому Докладу Верховному Совету РФ по обеспечению безопасности страны;

2. обеспечение (совместно с профильными комитетами и комиссиями Верховного Совета) разработки законодательных актов, регулирующих сферу безопасности, в том числе закона «О безопасности системы управления РФ и охране руководителей высших органов власти и управления РФ» и других установлений, необходимых для реализации Закона Российской Федерации от 5 марта 1992 г. «О безопасности»[395].

Таким образом, уже в период формирования своей структуры и кадрового состава Совет Безопасности Российской Федерации включается в законотворческий процесс в сфере государственной политики безопасности, одним из составных элементов которой были вопросы информационной

[395] Распоряжение Президента Российской Федерации от 03.06.1992 г. № 266-рп «О первоочередных мерах по обеспечению деятельности Совета безопасности Российской Федерации» [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/acts/bank/1408 (Дата обращения: 15.04.2022)

безопасности, а также являлся координатором деятельности специализированных ведомств, участвующих в ее реализации.

В ноябре 1992 г. в докладе Верховному Совету, на тему «Об обеспечении безопасности РФ», Б.Н. Ельцин отмечал, что при участии Совета Безопасности разработана правовая база, которая станет основой Доктрины безопасности России. Президент подчеркнул, что Доктрина опирается на принцип «всеобъемлющей безопасности, отражающий идею защищенности жизненно важных интересов всех элементов общественной структуры – личности, общества, государства от всевозможных угроз внутреннего и внешнего характера»[396].

Безопасность информации в РФ, согласно определению, данному Б.Н. Ельциным, подразумевала «государственную защиту государственных, общественных и личных банков данных, средств обработки и передачи информации»[397]. Тем самым задачи информационной безопасности получали преимущественно технологический характер, что коррелировало с формирующимся в этот период в странах Запада видением глобальной информатизации и связанных с ней проблем кибербезопасности[398].

Между тем, в России середины 1990-х гг. складываются два крупных направления общественной мысли и деятельности конкретных учреждений и организаций, связанных, в том числе с подготовкой законопроектов и государственных программ в области информатизации и информационной безопасности. Данная тенденция определялась общей картиной общественно-политической жизни России на начальном этапе рыночной трансформации. Совет Безопасности РФ как центр формирования стратегического курса страны в сфере обеспечения безопасности государства и российский парламент, осуществлявший модернизацию соответствующих отраслей

---

[396] Архив Президента России. Ф.6. Оп. 1. Д. 88. Л. 118-119.
[397] Там же. Л.122.
[398] *Крутских А.В., Зиновьева Е.С., Булва В.И. и др.* Международная информационная безопасность: подходы России / Центр международной информационной безопасности и научно-технологической политики МГИМО МИД России. М.: МГИМО (Университет), 2021. С. 8.

законодательства, в период перехода страны к рыночной экономике работали в условиях высокого уровня политизации общественного сознания. На заседаниях Государственной Думы, различных форумах, в прессе и на телевидении шло обсуждение ключевых вопросов развития страны, при этом тема информационной безопасности все чаще ставилась как самостоятельная проблема, имеющая принципиальное, в ряде случаев идеологизированное звучание.

В обсуждении вопросов информационной безопасности России и разработке информационного законодательства в Государственной Думе принимали участие представители Правительства России, Совета Безопасности РФ, российских спецслужб. В условиях новой демократической государственности в процессе формирования государственной информационной политики впервые в истории страны активно участвовали различные общественные группы и организации, в том числе непосредственно представленные в Государственной Думе РФ. Журналисты, политтехнологи, представители IT-сообщества, которые посещали открытые слушания в парламенте, составляли обращения к депутатам, публиковали и рассылали материалы научно-аналитического и публицистического характера по вопросам информационной безопасности России.

22 марта 1996 г. состоялось заседание Общественного экспертного Совета при Комитете по информационной политике и связи Госдумы РФ, посвященное проблемам свободы доступа к информации, на котором секретарь Межведомственной комиссии по информационной безопасности Совета Безопасности РФ А.П. Курило представил проект закона «О защите персональных данных», разработанный группой экспертов[399]. В обсуждении документа приняли участие депутаты Государственной думы РФ, сотрудники

---

[399] *См.: Черешкин Д.Г., Курило А.П.* О проблеме защиты персональных данных в Российской Федерации // Проблемы информатизации. 1995. № 1. С. 32-34; *Курило А.П.* О проблеме персональных данных // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 1996. № 7. С. 12-13.

Комиссии по информатике при Президенте России, представители ведущих столичных СМИ и факультета журналистики МГУ им. М.В. Ломоносова, деятели правозащитных организаций.

14 мая того же года были проведены парламентские слушания по теме «Средства массовой информации в системе национальной безопасности РФ», на которых присутствовало большое число журналистов, в том числе руководителей корпоративных организаций СМИ и связанных с ними профессиональных и творческих объединений[400]. Ряд выступавших, включая секретаря Союза журналистов РФ П.С. Гутионтова и председателя Фонда защиты гласности А.К. Симонова, высказали свое принципиальное несогласие с проектом «Концепции информационной безопасности России», представленным для обсуждения на слушаниях[401]. Их позиция базировалась на убеждении, что приоритетом стратегических документов по информатизации и российского информационного законодательства должна быть защита права на информацию и свобода СМИ, а не противодействие информационным угрозам.

Диаметрально противоположные подходы доминировали среди участников мероприятия 4 июня 1996 г., когда Комитет по информационной политике и связи совместно с Комитетом по делам женщин, семьи и молодежи Госдумы РФ проводили парламентские слушания, посвященные подготовке законопроекта подготовке законопроекта «Об информационной безопасности семьи». Помимо депутатов, в слушаниях приняли участие сотрудники Совета безопасности, Администрации Президента, ФАПСИ, ФСБ, МВД, ученые и журналисты. В центре внимания парламентариев и приглашенных экспертов оказалось отечественное телевидение, которому большинством выступавших была дана оценка как «распространителю социально опасной информации». Федеральные и региональные телеканалы обвинялись депутатами в непристойности, пропаганде насилия, жестокости,

---

[400] Парламентские слушания «Средства массовой информации в системе информационной безопасности» // Думский вестник. 1996. № 5 (20). С. 90-103.
[401] Там же.

ценностей общества потребления, что оказывало, по словам ораторов крайне негативное влияние на детей и молодежь. Депутаты – сотрудники думского Комитета по делам женщин, семьи и молодежи видели выход из сложившейся ситуации в подготовке закона под условным наименованием «Об информационной безопасности семьи»[402]. Реализация данного проекта, как отметила заместитель председателя Комитета Н.В. Кривельская, позволила бы запретить распространение социально опасной информации, установить формы ответственности за нарушения в данной сфере и создать механизмы государственного и общественного контроля над СМИ. Идея подобного законопроекта не получила дальнейшей поддержки, но тема защиты общества, прежде всего, детей и подростков от деструктивных информационных потоков, как отмечалось в предыдущей главе, в разные годы нашла свое выражение в деятельности Лиги безопасного Интернета и других инициативах представителей депутатского корпуса России.

Значительную активность в середине 1990-х гг. в привлечении внимания к теме государственной информационной политики проявила группа журналистов и политологов, близких к Российско-Американскому пресс-центру в Москве, где в январе 1995 г. на одной из встреч деятелей прессы была выдвинута идея о реализации специальной «Программы по свободному доступу журналистов к информации». Продвижением проекта заинтересовалась Межгосударственная телерадиокомпания СНГ «Мир», которая выпустила три передачи с участием известных государственных деятелей и специалистов в области информационных технологий, включая секретаря Совета Безопасности России В.А. Рубанова, на которых обсуждались различные аспекты реализации права журналистов на получение общественно значимой информации и их социальной ответственности при ее публикации. Ведущим передач выступал И.М. Дзялошинский, в последующие годы получивший известность в

[402] Новости ВГТРК [Электронный ресурс] // Сайт Издательского Дома «Новый Взгляд» 6 июня 1996 г. URL: https://www.newlookmedia.ru/?p=3337 (Дата обращения: 15.04.2022)

качестве автора научных трудов в области коммуникаций и медиа[403]. В 1996–2004 гг. он также возглавлял Комиссию по свободе доступа к информации (КСДИ), созданную при Фонде защиты гласности. КСДИ являлась организатором и участником семинаров и круглых столов по тематике свободы доступа к информации, к работе в которых приглашались депутаты Государственной Думы РФ, известные журналисты и ученые. Руководитель КСДИ И.М. Дзялошинский был включен в состав Общественного экспертного совета при Комитете по информационной политике и связи Госдумы РФ[404].

5 июля 1996 г. либеральные журналистские круги и депутаты Государственной Думы провели Международную научно–практическую конференцию «Российская журналистика: свобода доступа к информации. (Правовые, профессиональные, организационные проблемы)». В Заявлении, принятом участниками конференции, в принципе отрицалась «идея информационной конфронтации со странами Запада» и высказывалось несогласие с деятельностью депутатов Государственной Думы, Правительства, российских спецслужб в области обеспечения внешней и внутренней информационной безопасности страны[405].

Между тем, ведущими экспертами Вооруженных Сил и спецслужб России, специалистами в области цифровых технологий, политологами и общественными деятелями в этот период выдвигались, в рамках традиционных для отечественной системы безопасности разработок в области защиты от внешних военных угроз[406], новые идеи и предложения по

---

[403] *Дзялошинский И.М.* Российский журналист в посттоталитарную эпоху. Москва: Издательский дом «Восток», 1995. 300 с.; *Он же.* Медиапространство России: коммуникационные стратегии социальных институтов. Москва: Изд-во АПК и ППРО, 2013. 479 с.; *Он же.* Социальные институты и социальная коммуникация. Введение в теорию коммуникационных матриц. Москва: Ай Пи Ар Медиа, 2020. 900 с. и др.

[404] *Дзялошинский И.М.* История одной комиссии [Электронный ресурс] // Личный сайт И.М. Дзялошинского. URL: https://www.dzyalosh.ru/01-03-Problemi-Dostupa/Istoriya-Odnoi-Komissii.pdf. С.8-9.

[405] Российская журналистика: свобода доступа к информации / Комиссия по свободе доступа к информации. Сост. И. Дзялошинский. М.: КСДИ, 1996.

[406] Архив Президента России. Ф.6. Оп. 1. Д. 88. Л. 118.

проблемам безопасности, связанным с появлением и внедрением в мировую практику информационного оружия[407].

Обеспокоенность российского экспертного сообщества растущими возможностями применения информационных технологий в военно-политическом противостоянии мировых держав, потенциальные (на тот момент) угрозы информационной войны нашли отражение в тематике работы профильных комитетов и комиссий Государственной Думы и Совета Безопасности РФ. Так, 4 июля 1996 г. на заседании Совета Государственной Думы был поставлен вопрос о проведении парламентских слушаний на тему «Угрозы и вызовы в сфере информационной безопасности». С обоснованием необходимости обсуждения данного вопроса выступили представители КПРФ – председатель Государственной Думы РФ Г.Н. Селезнев и депутат Р.С. Попкович – военный инженер, генерал-майор в отставке, до 1995 г. – глава администрации г. Красногорска Московской области, почетный гражданин города. В поддержку слушаний выступил также депутат от ЛДПР О.А. Финько – доктор технических наук, специалист в области защиты информации, профессор специальной кафедры Краснодарского высшего военного училища им. генерала армии С.М. Штеменко[408].

16 июля 1996 г. в Государственной Думе России прошли закрытые парламентские слушания, посвященные проблеме информационного оружия (ИО). Депутатам был представлен доклад Службы внешней разведки (СВР) России, осветивший возможные сферы применения информационного оружия, в том числе в экономике, фннансовом секторе, государственном

---

[407] *Лопатин В.Н., Цыганков В.Д.* Психотронное оружие и безопасность России. – Москва, 1999. 152 с.

[408] Протокол № 34 заседания Совета Государственной Думы РФ от 04.07.96 г. «О проведении 16 июля 1996 года (вторник) парламентских слушаний «Угрозы и вызовы в сфере информационной безопасности Российской Федерации» Электронный ресурс. URL: Сайт Системы обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (Далее: СОЗД). URL; https://sozd.duma.gov.ru/events_document/43C5456B-9E8B-49CB-BD0E-69F6723699DD/1996 (Дата обращения: 15.04.2022)

управлении и др.[409] Указывалось также на потенциальные угрозы осуществления на территории противника крупных техногенных катастроф путем дезорганизации управления объектами и процессами, связанными с большими объемами опасных веществ или энергией высокой мощности. Новейшие разработки в области ИО, говорилось в докладе, включают создание технологий воздействия на сознание людей – внедрение деструктивных поведенческих моделей, провоцирования недовольства, агрессии, паники среди населения и др.[410] Соответственно, благодаря проведению отечественными специалистами в области информационной безопасности квалифицированных исследований, задачи противодействия комплексу новых угроз, связанных с глобальной информатизацией и появлением информационного оружия, учитывались при разработке правовой базы государственной информационной безопасности России, обсуждались в ходе представительных научных форумов. Тема информационного оружия как новой глобальной угрозы рассматривалась в 1999 г. участниками Первой научно-практической конференции «Информационная безопасность – Юг России» в Таганроге[411], которая стала в последующий период ежегодной, а с 2002 г. приобрела международный статус. На конференции «Информационная безопасность – Юг России» 2006 г. был принят итоговый документ, в котором в частности, говорилось: «Признать, что в настоящее время обеспечение информационной безопасности является одним из основополагающих факторов достижения

---

[409] *Лопатин В.Н.* Безопасность как критерий информационного выбора // Право и информатизация общества: Сб. науч. тр. / РАН.ИНИОН. Центр социальных научно-информационных исследований. Отдел правоведения; РАН. ИГП. Центр публичного права. Сектор информационного права; Отв. ред. Бачило И.Л. М., 2002. С. 192.

[410] Там же.

[411] Материалы конференции «Информационная безопасность – Юг России». 23 – 25 июня 1999 г. Таганрог, 1999.

высокого уровня жизнеспособности, терророустойчивости, оборонной и технологической безопасности Российской Федерации»[412].

Организаторами и участниками ежегодной Международной конференции по информационной безопасности в Таганроге традиционно выступают (наряду с Министерством образования и науки РФ, университетами Юга России и академическими структурами) Аппарат Совета Безопасности РФ, ФСТЭК, Министерство обороны РФ и другие федеральные ведомства, крупные научно-технологические центры[413].

В XXI в., когда российское руководство последовательно осуществляет развитие концептуальной и правовой базы государственной информационной политики страны, данная тематика регулярно включается в повестку дня заседаний и рабочих совещаний Совета Безопасности РФ. В том числе существенное значение в контексте формирования современной отечественной системы информационной безопасности имели заседания Совета Безопасности:

- 25 июня 2000 г. «О Доктрине информационной безопасности России»;

- 30 апреля 2002 г. «Обеспечение национальной безопасности Российской Федерации в свете борьбы с международным терроризмом»;

- 24 февраля 2004 г. «О политике Российской Федерации в области развития национальной инновационной системы»;

- 25 июля 2007 г. «О развитии информационного общества в России»;

- 24 марта 2009 г. «О Стратегии национальной безопасности Российской Федерации до 2020 года и комплексе мер по её реализации»;

- 1 октября 2010 г «О создании современных систем связи для нужд обороны и безопасности страны, поддержания правопорядка»;

---

[412] *Бородакий Ю.В., Макаревич О.Б.* Конференция в Таганроге: 10 шагов вперед [Электронный ресурс] // Информационная безопасность. 2006. № 3-4. URL: https://lib.itsec.ru/articles2/bypub/insec-3+4-2006

[413] *Брюхомицкий Ю.А., Макаревич О.Б.* Обзор исследований и разработок по информационной безопасности // Известия ЮФУ. Технические науки. 2012. № 12(137). С. 8-21.

- 1 октября 2014 г. «О противодействии угрозам национальной безопасности в информационной сфере»;

- 26 октября 2017 г. «О защите информационной инфраструктуры государства и мерах по её развитию»;

- 26 марта 2021 г. «О государственной политике в области международной информационной безопасности»;

- 20 мая 2022 г. «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства» и др.[414]

Основная работа Совета Безопасности РФ проходит в закрытом режиме. В 2000-е гг. на официальных сайтах и в прессе публикуются отдельные тексты выступлений и обзоры заседаний, которые отражают наиболее существенные аспекты развития государственной информационной политики России. Так, на заседании Совета Безопасности 1 октября 2010 г. обсуждались меры по развитию современной высокоскоростной связи, которая, как отметил Президент России В.В. Путин, является одним из ключевых факторов укрепления национальной безопасности страны. В качестве приоритетной задачи на данном направлении была определена дальнейшая модернизация систем связи Вооруженных сил РФ, в том числе полная замена диалоговых средств коммуникации цифровыми[415]. Президент также подчеркнул значимость дополнительного стимулирования разработок и производства отечественного телекоммуникационного оборудования и программного обеспечения. Предметом рассмотрения на заседании Совета Безопасности стали подсистемы связи, используемые в общественном пространстве и сфере охраны правопорядка (система экстренной связи

---

[414] Заседания Совета Безопасности РФ [Электронный ресурс] // Совет Безопасности Российской Федерации. Официальный сайт. URL: http://www.scrf.gov.ru/council/session/ (Дата обращения: 15.04.2022)

[415] Заседание Совета безопасности РФ «О создании современных систем связи для нужд обороны и безопасности страны, поддержания правопорядка». 1 октября 2010 г. [Электронный ресурс] // Совет безопасности РФ. URL: Официальный сайт. https://www.scrf.gov.ru/council/session/2048/ (Дата обращения: 15.04.2022)

«Безопасный город» и др.), и вопросы обеспечения институтов информационной безопасности квалифицированными кадрами[416].

Решения Совета Безопасности РФ 1 октября 2010 г. в области обеспечения связи для специальных служб и силовых ведомств явились стимулом для новых отечественных научно-технических разработок в сфере повышения защищенности телекоммуникационных систем органов государственного управления, спецслужб, Вооруженных сил России от несанкционированного доступа, в том числе из-за рубежа[417].

Во второй половине 2010-х гг. на фоне обострения геополитической конкуренции вопросы противодействия внешним информационным угрозам приобретают все более существенное значение в контексте национальной безопасности Российской Федерации. Президент России В.В. Путин на заседании Совета безопасности РФ 1 октября 2014 г. отметил, что специальными ведомствами зафиксирован непрекращающийся рост числа компьютерных атак на информационные ресурсы России, подчеркнув, что «методы, средства и тактика проведения подобных атак совершенствуются, а их интенсивность прямо зависит от текущей международной обстановки»[418].

В.В. Путин отметил также, что усилились угрозы общественной информационной безопасности России, связанные с распространением в глобальной сети материалов террористической и экстремистской тематики,

---

[416] Заседание Совета безопасности РФ «О создании современных систем связи для нужд обороны и безопасности страны, поддержания правопорядка». 1 октября 2010 г. [Электронный ресурс] // Совет безопасности РФ. URL: Официальный сайт. https://www.scrf.gov.ru/council/session/2048/ (Дата обращения: 15.04.2022)

[417] *Елагин В.С., Шполянский Е.А.* Особенности построения защищенных сетей связи государственных организаций и силовых ведомств // T-Comm: Телекоммуникации и транспорт. 2011. № S1. С. 26-27; *Буренин А.Н., Легков К.Е.* Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей // Наукоемкие технологии в космических исследованиях Земли. 2015. №3. С. 46-61; и др.

[418] Заседание Совета Безопасности РФ «О противодействии угрозам национальной безопасности в информационной сфере». 1 октября 2014 г. [Электронный ресурс] // Совет безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/2059/ (Дата обращения: 15.04.2022)

ростом числа преступлений, совершаемых с применением информационных технологий, в отношении российского бизнеса и финансовых учреждений[419].

Президентом России был предложен комплекс дополнительных мер в целях укрепления системы информационной безопасности страны в новых геополитических условиях, в том числе:

1. повышение защищенности отечественных информационно-коммуникационных сетей государственных структур, исключение возможности незаконного доступа, утечки конфиденциальных и персональных данных;

2. обеспечение технологической устойчивости и информационной безопасности российского сегмента интернета при соблюдении свободы СМИ, обеспечении прав граждан на получение и свободное распространение информации;

3. развитие отечественных информационных технологий, цифровой техники и программных продуктов.

4. расширение международного сотрудничества России в сфере информационной безопасности на площадках ООН. БРИКС, ШОС[420].

Как уже поминалось выше, в декабре 2014 г. была утверждена подготовленная под эгидой СБ РФ «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (ГосСОПКА). Согласно Концепции, в стране создаются «Центры обнаружения, предупреждения и ликвидации последствий компьютерных атак», организация которые осуществлялась по ведомственному и территориальному принципам. Их работу координирует Главный центр Системы. Корпоративные центры создаются операторами связи и другими организациями, которые осуществляют лицензируемую деятельность в сфере

---

[419] Заседание Совета Безопасности РФ «О противодействии угрозам национальной безопасности в информационной сфере». 1 октября 2014 г. [Электронный ресурс] // Совет безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/2059/ (Дата обращения: 15.04.2022)

[420] Там же.

информационной безопасности[421]. Соответствующая модель вскоре получила отражение в Федеральном законе от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ».

Вопросы, связанные с развитием информационно-коммуникационных технологий, затрагивались на заседаниях Совета Безопасности РФ, посвященных задачам обеспечения национальной безопасности в российских регионах, развития стратегически значимых отраслей экономики и др. Так, например, в июле 2015 г. состоялось выездное совещание Совета Безопасности РФ в Вологде, по итогам которого было принято решение об активизации работы в области «прогнозирования, выявления и оценки угроз информационной безопасности на Северо-Западе Российской Федерации»[422], о неотложных мерах в области подготовки кадров специалистов в области ИБ, а также отмечена необходимость проведения углубленного экспертного анализа текущего состояния и тенденций развития социально-экономического и военно-политического положения региона[423].

В сфере постоянного внимания руководства России находятся вопросы технологического и организационного обеспечения информационной безопасности государственных органов России. Этой теме было, в частности, посвящено заседание Совета Безопасности РФ 26 октября 2017 г., прошедшее в расширенном составе, с участием заместителя председателя Правительства России Д.О. Рогозина, министра юстиции А.В. Коновалова, мэра Москвы С.С. Собянина и др.

Открывая заседание, Президент России В.В. Путин подчеркнул, что устойчивость информационных систем и средств коммуникации имеет для Российской Федерации стратегическое значение, являясь компонентом

---

[421] Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации // Совет Безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/2301/ (Дата обращения: 15.04.2022)

[422] *Кучерявый М.М., Косов Ю.В., Вовенда Ю.В.* Деятельность органов государственной власти Северо-Западного федерального округа по обеспечению безопасности информации // Управленческое консультирование. 2017. № 10(106). С. 8-14.

[423] Там же.

обеспечения национального суверенитета, обороноспособности, внутреннего социально-экономического развития, эффективного государственного управления. Президент России отметил, что в стране действует надежная система обеспечения информационной защиты государственных органов. Однако в условиях интенсивного роста киберугроз различной направленности в глобальном масштабе, многократно возрастают риски внешнего вторжения в цифровые системы обороны, государственного управления, всей критической информационной инфраструктуры (КИИ). В.В. Путин особо подчеркнул, что в ряде стран осуществляется создание информационного оружия и кибервойск, а также расширяется применение цифровых технологий на международной арене в экономической конкурентной борьбе и в целях продвижения политических интересов в формате «мягкой силы»[424].

С учетом тенденций развития глобального информационного пространства Совет Безопасности РФ обсудил дополнительные меры противодействия потенциальным угрозам и рискам, с которыми может встретиться страна. В том числе, В.В. Путин предложил сконцентрировать усилия на следующих направлениях: дальнейшее совершенствование государственной системы выявления, предупреждения и устранения последствий компьютерных атак на информационные ресурсы Российской Федерации; повышение защищенности государственных информационных систем; минимизация рисков использования иностранного телекоммуникационного оборудования и программного обеспечения; повышение безопасности и устойчивости российского сегмента Интернета.

Данное заседание Совета Безопасности РФ вызвало широкий интерес российской прессы, в том числе цитировались комментарии, высказанные секретарем Совета Безопасности Н.П. Патрушевым и другими участниками

---

[424] Заседание Совета Безопасности РФ «О защите информационной инфраструктуры государства и мерах по её развитию». 26 октября 2017 г. [Электронный ресурс] // Совет Безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/2301/ (Дата обращения: 15.04.2022)

заседания. В СМИ подчеркивалась информация о решениях в сфере усиления персональной ответственности руководителей госучреждений за обеспечение информационной безопасности подведомственных им структур и о последовательном переходе с 2022 – 2023 гг., по прогнозу Д.О. Рогозина, «оборонного и гражданского сектора на производство собственного коммуникационного оборудования и программного обеспечения» в рамках политики импортозамещения[425].

22 мая 2022 г. в онлайн-режиме состоялось заседание Совета Безопасности России, посвященное вопросам повышения устойчивости и безопасности функционирования государственной информационной инфраструктуры. Открывая мероприятие, Президент России В.В. Путин осветил картину серьезного увеличения внешних кибератак на цифровое пространство страны, направленных не только на официальные органы государства, но и на СМИ, финансовые учреждения, социальные ресурсы. Попытки нарушить работу отечественной КИИ сочетаются с вбросами в российское информационное пространство искаженных и ложных сведений о текущих событиях и других материалов деструктивного характера. При этом возросший уровень угроз обусловлен их проведением крупными центрами цифровых технологий, действующими под эгидой спецслужб и военных структур ряда иностранных государств: «По сути, против России развязана настоящая агрессия, война в информационном пространстве»[426]. Дополнительным компонентом данного процесса явилось ограничение доступа России к иностранным цифровым технологиям и оборудованию в рамках экономического санкционного давления со стороны Запада. При этом глава страны подчеркнул, что киберагрессия против России потерпела очевидную неудачу, благодаря системной работе по созданию эффективной

---

[425] *Сафронов И.* Президент РФ Владимир Путин обсудил с ответственными лицами кибербезопасность // Газета «Коммерсантъ». 27 октября 2017 г. № 201 (6195). С.1.

[426] Заседание Совета Безопасности РФ «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства». 20 мая 2022 г. [Электронный ресурс] // Совет Безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/3241/ (Дата обращения: 23.05.2022)

зашиты КИИ России, проводившейся в предшествующие годы в соответствии с вызовами времени. Однако в сложившейся ситуации интенсивного глобального развития цифровых технологий и сложного международного положения Совет Безопасности приступил к формированию нового пакета мер в области защиты критической информационной инфраструктуры страны, выдвигая на первый план работу на опережение в сфере обеспечения безопасности КИИ. Как подчеркнул В.В. Путин, «нам нужно самым серьёзным образом и постоянно, что называется, в режиме реального времени совершенствовать, донастраивать механизмы обеспечения информационной безопасности отраслевых критически важных объектов, от которых напрямую зависит обороноспособность нашей страны, стабильное развитие экономики и социальной сферы»[427]. Было также уделено внимание обсуждению новых мер по противодействию кибератакам на госструктуры России, обеспечению технологического суверенитета страны в сфере цифровых коммуникаций и защиты информации, поддержке отечественных производителей цифровой техники и программного обеспечения, IT-специалистов.

Аппарат Совета Безопасности совместно с Комитетом Госдумы РФ по безопасности традиционно выступили в качестве инициаторов проведения очередного Национального форума информационной безопасности «Инфофорум», который состоялся в Москве 3-4 февраля 2022 г. на площадке столичного Правительства[428]. Пленарное заседание Инфофорума-2022 прошло при участии представителей руководства Аппарата Совета Безопасности РФ, Государственной Думы, ФСБ, Генерального штаба ВС РФ, Минцифры, ФСТЭК, Центрального банка РФ и других ведомств, участвующих в обеспечении информационной безопасности государства,

---

[427] Заседание Совета Безопасности РФ «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства». 20 мая 2022 г. [Электронный ресурс] // Совет Безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/3241/ (Дата обращения: 23.05.2022)

[428] Программа Инфофорума-2022 [Электронный ресурс] // Сайт Инфофорума-2022. URL: https://infoforum.ru/programma-infoforuma-2022 (Дата обращения: 19.04.2022)

общества и бизнеса России. К открытию Инфофорума-2022 была приурочена выставка «Кибер-ЭКСПО»[429].

Первоочередное внимание участники мероприятия уделили обсуждению темы «Информационная безопасность – стратегический национальный приоритет» и Федеральному проекту «Информационная безопасность»: результаты и перспективы». Рассматривались также вопросы цифровизации российских регионов и отраслей экономики, задачи международного диалога в сфере информационной безопасности в форматах СНГ, ОДКБ, ШОС и БРИКС, обеспечения информационной безопасности КИИ, ТЭК, промышленности, транспорта и связи, финансового сектора и др.

Среди выступивших на Форуме были: К. Долгов, зам. председателя Комитета Совета Федерации по экономической политике, и А. Шойтов, зам. министра цифрового развития, связи и массовых коммуникаций России. Глава думского Комитета по информационной политике, информационным технологиям и связи А. Хинштейн посвятил свое выступление законодательной деятельности Государственной Думы по реализации стратегии цифрового суверенитета страны, директор Департамента информационной безопасности Банка России В. Уварова, который представил доклад на тему «Основные направления информационной безопасности в кредитно-финансовой сфере», руководители ведущих IT-компаний Ю. Максимов (Positive Technologies), И. Ляпунов (Ростелеком) и др.[430]

Таким образом, в течение периода 1991 – 2021 гг. Совет Безопасности РФ выполнял задачи по формированию стратегической линии и выработке конкретных шагов по реализации государственной политики России в сфере информационной безопасности, взаимодействуя с органами законодательной и исполнительной власти, правоохранительными институтами, научно-

[429] Программа Инфофорума-2022 [Электронный ресурс] // Сайт Инфофорума-2022. URL: https://infoforum.ru/programma-infoforuma-2022 (Дата обращения: 19.04.2022)

[430] *Тумакова А.* ИНФОФОРУМ 2022: диалог о будущем цифровой безопасности и сегодняшней работе в этом направлении // Инфокоммуникации онлайн: сетевое издание. 8 февраля 2022 г. https://ict-online.ru/news/n206503/ (Дата обращения: 19.04.2022)

технологическими центрами. Во второй половине 2010-х гг. деятельность Совета Безопасности определяется задачами эффективного обеспечения всех направлений и уровней национальной безопасности, причем обеспечение защиты КИИ и развитие отечественных информационно-коммуникационных технологий выступают в качестве ключевых факторов данного направления государственной политики РФ.

В процессе формирования Государственной Думой РФ правовой базы стратегии национальной безопасности и государственной информационной политики тема информационной безопасности выступает как одна из востребованных областей взаимодействия парламентского сообщества с учеными, журналистами, специалистами в области цифровых технологий, развивалось общественное обсуждение различных моделей обеспечения информационной безопасности государственных институтов, общества и бизнеса.

3.2. Обеспечение информационной безопасности системы государственного управления и специальных служб Российской Федерации

На рубеже XX – XXI в. вопросы обеспечения национальной безопасности России приобретали все более тесную зависимость от сферы информационной безопасности органов государственной власти и управления страны, предприятий и организаций оборонной промышленности, космического комплекса и др.

Эффективная информационная защита государства в условиях глобализации, развития цифровых технологий требовала внедрения в работу институтов обеспечения информационной безопасности новых моделей деятельности, соединения лучших традиций отечественных спецслужб с современными технологическими достижениями, высокой квалификации кадров в области применения новейшего электронного оборудования, цифровых средств коммуникации, методов защиты информации.

С середины 2010-х гг. и до настоящего времени обеспечение информационной безопасности государства и общества России осуществляется в условиях нарастающей международной напряженности и усиливающегося внешнего экономического и политического давления[431].

Президент Российской Федерации В.В. Путин в своем выступлении на Коллегии ФСБ России 24 февраля 2021 г. сформулировал задачи по основным направлениям работы по защите национальных интересов России. В том числе руководитель страны подчеркнул, что следует «и дальше повышать уровень защиты конфиденциальной информации, не допускать утечек закрытых сведений военного характера, данных о передовых технологиях и перспективных разработках наших научных центров и предприятий оборонно-промышленного комплекса»[432]. В.В. Путин отметил, что в течение 2020 года число наиболее опасных кибератак на информационное пространство России, в том числе на ресурсы структур власти и управления, увеличилось почти в 3,5 раза. Сложившаяся ситуация требует новых подходов к обеспечению кибербезопасности. В данных условиях, подчеркнул Президент России, стране необходима «долгосрочная, выверенная стратегия действий по защите национальных интересов в цифровой сфере, основанная на прогнозировании ситуации, на учёте потенциальных рисков для общества и государства и, конечно, опирающаяся на самые передовые технологии и технологические решения»[433].

Следует отметить, что государственная политика формирования современной системы институтов информационной безопасности Российской Федерации, проводившаяся в течение ряда лет, обусловила подготовленность отечественных спецслужб и научно-технологических центров к решению сложных задач защиты критической информационной инфраструктуры

---

[431] Выступление Президента РФ В.В. Путина на заседании коллегии ФСБ России. 24 февраля 2021 года [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/events/president/news/65068 (Дата обращения: 19.04.2022)
[432] Там же.
[433] Там же.

(КИИ) России и других направлений негативного информационного воздействия извне на российское общество.

В 2000-е гг. началась модернизация организационных, кадровых и технологических основ работы ФСБ и других спецслужб, что позволило им успешно противодействовать угрозам национальной информационной безопасности. Были созданы условия для обеспечения защиты информационных ресурсов государства и экономики, а также для защиты российского общества от киберпреступлений и социально опасных информационных потоков в рамках ответственности органов информационной безопасности. В 2021 г. в интервью корреспонденту «Комсомольской правды», генерал-полковник С.В. Степашин, занимавший пост директора ФСБ в 1994-1995 гг., сравнивая этот период в истории российских спецслужб с современностью, отметил, что качественный уровень их работы в настоящее время позволяет эффективно обеспечивать национальную безопасность страны, в том числе в информационной сфере: «Здесь – оперативная составляющая, агентура, техническое обеспечение. Мне есть, с чем сравнивать – в каком состоянии мы были в начале 90-х, особенно после развала Союза, и сегодня – день и ночь, чего там говорить»[434].

В течение рассматриваемого периода органами государственного управления и спецслужбами России решались практические задачи в области сохранения государственной тайны[435]. Законом РФ «О Федеральной службе безопасности» от 3 апреля 1995 г. защита государственной тайны была зафиксировано в российском законодательстве в качестве главной функции ФСБ России. Основным организационно-правовым механизмом ее

---

[434] Сергей Степашин – о выступлении Владимира Путина на коллегии ФСБ (Беседовал А. Гамов) [Электронный ресурс] // Комсомольская правда. 24 февраля 2021 г. URL: https://www.kp.ru/daily/27244/4372832/ (Дата обращения: 19.04.2022)

[435] *Амирова Ш.Н.* Обеспечение защиты государственной тайны органами государственной власти / Ш. Н. Амирова // Актуальные проблемы уголовного права и процесса, уголовно-исполнительного права и криминалистики: Материалы V научно-практической конференции. Саранск, 27 февраля 2017 года / Редколлегия: Н.Н. Азисова и др. Саранск: ООО «ЮрЭксПрактик», 2017. С. 19-22.

реализации выступает лицензирование предприятий и организаций, деятельность которых требует доступа к государственной тайне[436].

Неотъемлемой частью работы российских спецслужб является разработка научно-технологическими подразделениями ФСБ, Службы внешней разведки, Федеральной службы охраны, Службы защиты государственной тайны Вооруженных Сил РФ эффективных средств противостояния иностранным электронным разведкам, деструктивным кибервоздействиям в рамках информационной войны, которые могут включать попытки взлома и разрушения стратегических информационных систем России, а также внедрение ложной и деструктивной информации в российское цифровое пространство.

В течение 1990-х гг. продолжала совершенствоваться и развиваться шифровальная служба Вооруженных Сил России, для деятельности которой в этот период было свойственно «увеличение нагрузки практически на все специальные органы», что было связано с «постоянным расширением спектра решаемых службой задач»[437]. Формировался комплексный подход к защите секретной информации, велись разработки новых технологических механизмов и средств обеспечения информационной безопасности.

Как отмечает генерал-лейтенант Ю.В. Кузнецов**,** начальник Восьмого управления Генштаба Вооружённых Сил России, в статье, посвященной 100-летию шифровальной службы российского военного ведомства, в XXI веке развитие системы информационной безопасности, которое осуществляется рамках деятельности Службы защиты государственной тайны ВС РФ, «направлено на создание системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы Вооружённых Сил России»[438].

---

[436] *Дзанагова М.К., Бетеева М.М.* Деятельность государственных органов по защите государственной тайны // Право и государство: теория и практика. 2021. № 4(196). С. 316-317.

[437] *Кузнецов Ю.В.* Сто лет на охране интересов государства // Красная Звезда. 2 ноября 2018 г. URL: https:// redstar.ru/sto-let-na-ohrane-sekretov-gosudarstva/

[438] Там же.

Проблемным аспектом правового обеспечения защиты государственной тайны в 1990-е гг. являлись неоднократные изменения, вносившиеся в перечень должностных лиц, обладавших правом отнесения сведений к государственной тайне, а также межотраслевых и отраслевых перечней сведений, заключающих в себе государственную тайну. За период с 1997 по 2001 г. в России было сформировано до 39 перечней данных, подлежащих засекречиванию, что, по мнению экспертов, затрудняло их реальное включение в работу структур, обеспечивавших защиту государственной тайны. Требовалось также уточнение критериев отнесения информации к категории государственной тайны[439]. В 2000 – 2010-е гг. была проведена работа в области модернизации нормативной базы защиты государственной тайны. Так, 28 мая 2015 г. Президент России В.В. Путин подписал Указ, дополняющий и уточняющий «Перечень сведений, отнесенных к государственной тайне». В 2021 г. Председателем Правительства России М.В. Мишустиным была утверждена новая редакция «Правил отнесения сведений к государственной тайне», которая, по оценкам специалистов, содержат «четкие правовые понятия, определения гостайны, согласно которым все причастные смогут понять, с чем имеют дело»[440]. В том числе были приняты меры для преодоления проблемы расхождения ведомственных подходов к определению государственной тайны; так, из числа организаций, самостоятельно формирующих перечни сведений, составляющих государственную тайну, были исключены государственные корпорации «Роскосмос» и «Росатом». Решение многих задач в сфере защиты государственной тайны, с одной стороны, имеет отраслевую специфику (военное ведомство, МВД, судебная система, Служба внешней разведки и др.). Так, например, существует проблема допуска к

---

[439] *Верютин В.Н.* Отдельные аспекты защиты государственной тайны в Российской Федерации // Вестник Воронежского института МВД России. 2009. № 2. С. 19.

[440] *Задорожный М.* Стало ли понятнее? Утверждены новые правила отнесения сведений к гостайне // Ведомости. 4 ноября 2021 г. URL: https://www.bfm.ru/news/485223 (Дата обращения: 17.04.2022)

государственной тайне военнослужащих[441], адвокатов[442], лиц, оказывающих конфиденциальные услуги органам правопорядка и спецслужбам и др.[443] С другой стороны, охрана государственной тайны требует постоянного межведомственного взаимодействия[444].

Становление единой государственной системы обеспечения информационной безопасности России связано с выходом 15 января 2013 г. Указа Президента РФ В.В. Путина «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», реализация которого была поручена ФСБ России[445].

В последующие годы специалистами ФСБ было подготовлено два законопроекта по обеспечению безопасности КИИ и осуществлен комплекс организационно-технологических мероприятий в данной области. Эксперты ведомства отмечали, что эффективность создававшейся системы в значительной степени зависит от согласованности информационной политики государства и других собственников информационно-коммуникационных сетей, действующих в России, что требовало дополнительного правового урегулирования в данной сфере. При этом

---

[441] *Туровский В.В., Жуков А.В.* Основы допуска к защите государственной тайны военнослужащих и гражданского персонала // Экономика и социум. 2018. № 3(46). С. 512-519.

[442] *Клоков С. Н., Тарнакоп О.Г.* Особенности организации защиты по уголовным делам, в которых имеются сведения, составляющие государственную тайну // Вестник Уральского юридического института МВД России. 2020. № 1(25). С. 5-8; и др.

[443] *Павличенко Н.В., Поправко А.С.* Обеспечение государственной тайны в работе с лицами, оказывающими конфиденциальное содействие // Вестник Волгоградской академии МВД России. 2013. № 1(24). С. 92-97; *Попандопуло Д.В.* Проблемы защиты государственной тайны в оперативно-розыскной деятельности / Д.В. Попандопуло. Ростов-на-Дону: Ростовский юридический институт Министерства внутренних дел Российской Федерации, 2016. 132 с. и др.

[444] *Редкоус В.М., Кившик Д.И.* Факторы, обусловливающие взаимодействие государственных органов в области защиты государственной тайны, и направления совершенствования его правового регулирования // Закон и право. 2018. № 2. С. 153.

[445] Указ Президента РФ от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (с изменениями и дополнениями) [Электронный ресурс] // Информационно-правовая система «Гарант». URL: https://base.garant.ru/70299068/

отмечалась важность расширения взаимодействия с ведущими отечественными компаниями, работающими в сфере ИБ. Специалиста ФСБ в интервью электронному изданию TAdviser в 2013 г. по наиболее успешному решению задач защиты от хакерских DDos-атак поставил на первое место программное обеспечение, разработанное Лабораторией Касперского[446].

Существенную роль в процессе реализации государственной политики информационной безопасности сыграли проводившиеся во второй половине 1990-х – начале 2000-х гг. модернизация, сертификация и лицензирование телекоммуникационных систем, технологические показатели которых во многом определяют их потенциал в сфере защиты информации. Работа, проводившаяся Службой государственного контроля за связью в 1995–1999 гг. позволила в 5 раз снизить количество операторов связи, вывести из обращения значительную часть несертифицированного оборудования, в целом улучшить качество работы с клиентами.

Ряд разработок нормативного характера, способствовавших повышению качественных стандартов оборудования защиты информации, внедрявшегося в государственных учреждениях и на предприятиях России в 1990-е гг., провела Гостехкомиссия РФ. В том числе, специалистами Гостехкомиссии был подготовлен комплекс руководящих документов по данной тематике: «Положение по аттестации объектов информатизации по требованиям безопасности информации» (1994), «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования к защите информации» (1997 г.), «Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (1997), «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от

[446] Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак ГосСОПКА [Электронный ресурс] // Информационно-технологический портал TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Государственная_система_обнаружения,_предупреждения_и_ликвидации_последствий_компьютерных_атак_(ГосСОПКА) (Дата обращения: 20.04.2022)

несанкционированного доступа к информации» (1998), «Защита от несанкционированного доступа к информации. Термины и определения» (1998), «Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (1999) «Специальные требования и рекомендации по технической защите конфиденциальной информации» (2001) и др.

Большой объем технологических и организационных мероприятий, связанных с обеспечением информационной безопасности Правительства РФ, государственных министерств и ведомств, компаний, общественных организаций, выполняют профильные структуры в связи с международными дипломатическими мероприятиями, деловыми форумами, культурными и спортивными событиями. Так, например, в одном только перечне «стратегических задач Роскомнадзора на 2013 г. и среднесрочную перспективу» были обозначены (и впоследствии выполнены) работы обеспечению готовности системы радиоконтроля к участию России в Саммите лидеров стран «G20», по организации Оперативного центра управления радиочастотным спектром на период подготовки, организации и проведения XXII Олимпийских зимних игр и XI Паралимпийских зимних игр 2014 года в Сочи, обеспечению высокого качества управления радиочастотным спектром при проведении XXVII Всемирной летней Универсиады в г. Казани, по обеспечению готовности к проведению экспертизы электромагнитной совместимости (ЭМС) и выдаче разрешений на использование радиочастот или радиочастотных каналов организаторам и участникам Чемпионата мира по легкой атлетике в Москве 2013 года и др.[447]

Региональные управления Роскомнадзора – по Краснодарскому краю, Республике Адыгея, Ростовской области, Ставропольскому краю, Москве и

[447] Расширенное заседание Коллегии Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 21 декабря 2012 г. № 8. [Электронный ресурс] // Сайт Роскомнадзора. URL: https://rkn.gov.ru/about/p403/p677/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (Дата обращения: 20.04.2022)

Московской области, Республике Татарстан – готовясь к спортивным мероприятиям Олимпийских игр и Всемирной Универсиады 2014 г. провели учения Роскомнадзора и предприятий радиочастотной службы, в ходе которых выполнялись задачи по радиочастотному обеспечению тестирования и маркирования РЭС, радиоконтролю и взаимодействию при осуществлении мероприятий радиоконтроля.

Важнейшим компонентом сохранения государственной тайны является противодействие иностранным разведкам на территории России и за рубежом, которое становится все более актуальным в условиях напряженной геополитической обстановки XXI в. Так, только за первое полугодие 2017 г. сотрудниками ФСБ было разоблачено 30 иностранных шпионов[448], а в течение 2020 года пресечена деятельность на территории России 423 агентов и более 70 кадровых сотрудников иностранных спецслужб[449].

Источником информационных угроз национальной безопасности является деятельность запрещенных в России экстремистских и террористических организаций, которые пытаются проводить свое деструктивное идеологическое влияние через сайты и социальные сети, а также осуществляют координацию своих действий через цифровые и телекоммуникации. Соответственно, борьба с данным явлением со стороны российских спецслужб и органов правопорядка также ведется в информационном пространстве. За период 2015-2017 гг. сотрудниками ФСБ было предотвращено более 40 терактов и ликвидировано 66 экстремистских ячеек[450], причем следственные действия осуществлялись на основе использования современных информационных технологий. Число

---

[448] Расширенное заседание Коллегии Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 21 декабря 2012 г. № 8. [Электронный ресурс] // Сайт Роскомнадзора. URL: https://rkn.gov.ru/about/p403/p677/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (Дата обращения: 20.04.2022)

[449] Заседание коллегии ФСБ России. 24 февраля 2021 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/events/president/news/65068 (Дата обращения: 20.04.2022)

[450] Сафронов И. Президент РФ Владимир Путин обсудил с ответственными лицами кибербезопасность // Газета «Коммерсантъ». 27 октября 2017 г. № 201. С.1.

преступлений террористической направленности, совершенных на территории России, снизилось с 776 в 2010 г. до двух в 2020 г. При этом только в течение 2020 года было предотвращено 72 подобных преступления[451]. «За этой статистикой огромная, повседневная, опасная и тяжёлая работа, её новое качество», – подчеркнул В.В. Путин, выступая перед работниками СВР в декабре 2020 г., отметив при этом, что необходимо в дальнейшей работе уделять серьезное внимание вопросам информационной безопасности, поставив эту тему первой в перечне задач современных российских спецслужб[452].

В 2017 г. в «Коммерсанте» были опубликованные данные исследования, проведенного аналитическим центром Zecurion об уровне развития в мире кибервойск. Лидерами в данной сфере в настоящее время являются США и Китай. Функциями кибервойск является электронная разведка, кибератаки и другие форму информационного воздействия на противника. Как отметил руководитель Zecurion В. Ульянов, парадокс современной информационной цивилизации заключается в том, что чем более технологически развитой является страна, тем выше ее уязвимость перед кибератаками и, соответственно, больше потребность в развитии подразделений кибербезопасности. По оценкам экспертов, Россия входит в пятерку государств с наиболее многочисленными и технологически развитыми кибервойсками, численность которых на момент публикации исследования составляла около тысячи человек[453].

В 2014 – 2020 гг. последовательно осуществляется комплекс мер организационного характера в области усиления информационной защиты

---

[451] Заседание коллегии ФСБ России. 24 февраля 2021 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: http://www.kremlin.ru/events/president/news/65068 (Дата обращения: 20.04.2022)

[452] Поздравление Президента России В.В. Путина с Днем работника российских спецслужб 20 декабря 2020 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/events/president/news/64681 (Дата обращения: 18.04.2022).

[453] *Коломыченко М.* В Интернет ввели кибервойска [Электронный ресурс] // Коммерсантъ. 10 января 2017 г. URL: https://www.kommersant.ru/doc/3187320(Дата обращения: 18.04.2022).

государственных органов России. Наряду с научно-методическими мероприятиями ФСТЭК и ФСБ России по обеспечению безопасности критической информационной инфраструктуры страны началась подготовка к созданию региональных и ведомственных центров информационной безопасности. В июле 2014 г. было осуществлено проведение межведомственных тренировок по предупреждению кибератак на государственные информационные ресурсы[454]. В структуре ФСБ создавался Национальный координационный центр по компьютерным инцидентам (НКЦКИ). Приказом от 24 июля 2018 г. ФСБ установило перечень сведений, связанных с обеспечением безопасности критической информационной инфраструктуры, которые госучреждения и предприятия должны в обязательном порядке сообщать в ГосСОПКА[455].

В 2016 г. были выпушены «Методические рекомендации по созданию ведомственный и корпоративных центров ГосСОПКА», что позволило развернуть практическую работу в данном направлении. Так, в том же году начал действовать Центр обнаружения, предупреждения и ликвидации последствий компьютерных атак (КЦОПЛ) при государственной корпорации «Ростех».

В 2019–2020 гг. были созданы аналогичные центры в ряде федеральных ведомств, госкорпорациях «Росатом» и «Роскосмос», в крупных компаниях. Решение данной задачи требовало привлечения IT-специалистов высшего класса, установки новейшего оборудования и программного обеспечения. Поскольку большинство государственных учреждений и организаций не обладало собственными ресурсами такого

---

[454] Заседание Совета безопасности РФ «О противодействии угрозам национальной безопасности в информационной сфере». 1 октября 2014 г. [Электронный ресурс] // Совет безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/2059/ (Дата обращения: 18.04.2022).

[455] Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак ГосСОПКА [Электронный ресурс] // Информационно-технологический портал TAdviser. URL: https://www.tadviser.ru/index.php/ Статья: Государственная_система_обнаружения,_предупреждения_и_ликвидации_последствий_компьютерных_атак_(ГосСОПКА)

рода, к участию в запуске ГосСОПКА подключились ведущие российские компании, системные интеграторы, работающие в сфере информационной безопасности. Positive Technologies и Solar Security, создавшие совместный проект по созданию «под ключ» ведомственных и отраслевых центров ГосСОПКА. Positive Technologies брала на себя проведение экспертиз и разработку программ, Solar Security вела мониторинг хакерских атак и обеспечивала мероприятия по устранению последствий несанкционированных внешних воздействий на государственные информационные ресурсы. Компания по управлению информационными рисками ООО «БИЗон» («Безопасная информационная зона»), работающая в сотрудничестве со Сбербанком, заявила о своей готовности проводить подключение к ГосСОПКА предприятий малого и среднего бизнеса. Ведущие системные интеграторы в области ИБ получили возможность участвовать в строительстве системы информационной безопасности государства совместно с ФСБ РФ на договорной основе. Так, в январе 2019 г. было подписано соглашение между ФСБ России и компанией «Информзащита».

В июле того же года началось сотрудничество Национального координационного центра по компьютерным инцидентам (НКЦКИ) ФСБ России и компании «Инфосекьюрити»; в октябре состоялось подписание соглашения между НКЦКИ и компанией Angara Professional Assistance. В 2020 г. договоры о взаимодействии НКЦКИ заключили компании «Инфосистемы Джет», «Код безопасности» и др. Действующие в данных компаниях структуры мониторинга и реагирования на инциденты в области информационной безопасности получали право выполнять функции центров ГосСОПКА[456]. Лицензированный бизнес в сфере информационной безопасности оказывал аналогичные услуги в субъектах Российской

[456] Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак ГосСОПКА [Электронный ресурс] // Информационно-технологический портал TAdviser. URL: https://www.tadviser.ru/index.php/ Статья: Государственная_система_обнаружения,_предупреждения_и_ликвидации_последствий_компьютерных_атак_(ГосСОПКА)

Федерации. Так, например, группа компаний «ИнфоТеКС» в 2019 г. осуществила подключение к ГосСОПКА Правительства Республики Тыва, и т.п. В 2020 г. АО «ДиалогНаука» осуществила проект по интеграции в систему ГосСОПКА Федерального фонда обязательного медицинского страхования[457]. К 2022 г. было развернуто создание отраслевых центров компетенций в области обнаружения и ликвидации последствий кибератак в Минэнерго, Минздраве, Минцифры и других федеральных министерствах.

Во второй половине 2010-х гг. уровень киберугроз в отношении государственного сектора и бизнеса России существенно возрос. Представители ФСБ сообщили прессе, что только за 2016 г. было зафиксировано около 70 млн кибератак на отечественные предприятия, банки и операторов связи. При этом, как подчеркнул руководитель отдела аналитики информационной безопасности Positive Technologies Евгений Гнедин, каждая пятая атака была направлена на IT-системы государственных организаций[458].

При этом, если ранее российские сетевые коммуникации и серверы предприятий испытывали воздействие глобальных киберугроз наравне с IT-системами других стран и регионов (вирус WannaCry и т.п.), то по мере усиления международной напряженности начались усиленные целенаправленные попытки взлома и нарушения работы российских информационных систем. Существенную угрозу представляют собой вредоносные рассылки от имени федеральных ведомств, действующих в сфере информации и связи, портала «Госуслуги», Банка России и других структур, коммуникационные сети которых пользуются доверием граждан и организаций как защищенные. В частности, 25 мая 2022 г. Центром

---

[457] Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак ГосСОПКА [Электронный ресурс] // Информационно-технологический портал TAdviser. URL: https://www.tadviser.ru/index.php/ Статья: Государственная_система_обнаружения,_предупреждения_и_ликвидации_последствий_компьютерных_атак_(ГосСОПКА)

[458] *Иванова Е.* Хакеры пошли простым путем [Электронный ресурс] // Сайт Радил «Ъ FM». 14 июня 2017 г. URL: https://www.kommersant.ru/doc/3325386 (Дата обращения: 18.04.2022).

государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак ФГБУ «НИИ «Интеграл» было зафиксировано распространение опасного ПО якобы от Минцифры России[459].

Мониторинги информационных угроз и технологические решения по их преодолению ведущие IT-компании регулярно представляли на конференциях и семинарах, причем информация об этих мероприятиях публиковались в «Коммерсанте», «Ведомостях» и других ведущих СМИ, что отражает широкий общественный интерес к теме информационной безопасности, выходящий за рамки специальных технологических вопросов. Так, например, 6 февраля 2019 г. состоялась пресс-конференция компаний Positive Technologies и Qrator Labs провели пресс-конференцию, на которой были представлены основные новейшие тренды в области кибератак и оценок сетевой безопасности бизнеса. Мероприятие проводилось в помещении ресторана «I Van Gogh» на ул. Большая Лубянка, что подчеркивало его неформальный статус, однако посвященные ему статьи появились в «Российской газете»[460].

Большим авторитетом в сообществе специалистов в области цифровых технологий пользуется ежегодная Международная конференция по проблемам промышленной кибербезопасности Kaspersky Industrial Cybersecurity Conference в Сочи, которая в 2021 г. состоялась в 9-й раз.

С 2017 г. ежегодно проводится Конференция по информационной безопасности в ракетно-космической отрасли (РКО), актуальность тематики которой в современных условиях также существенно возрастает. В мероприятии участвуют ведущие IT-компании, работающие в сфере защиты информации, – Positive Technologies, Ростелеком-Солар, ЗАО НИП

---

[459] Специалисты пресекли вредоносную рассылку якобы от Минцифры [Электронный ресурс] // Министерство цифрового развития, связи и массовых коммуникаций РФ. Официальный сайт. URL: https://digital.gov.ru/ru/events/41582/ (Дата обращения: 27.05.2022)

[460] Пресс-конференция Qrator Labs и Positive Technologies: Главные тренды и итоги 2019 года в области кибератак и сетевой безопасности. Публикации в СМИ. [Электронный ресурс] // Сайт Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/about/press/events/304630/ (Дата обращения: 17.04.2022)

«Информзащита», Лаборатория Касперского и др. Директор Департамента защиты государственной тайны и информации Госкорпорации «Роскосмос» И. Виноградов, выступая с приветственным словом перед участниками IV-й Конференции, проходившей 1-2 октября 2020 г. в Ногинске Московской области, отметил, что проблематика информационной сферы неразрывно связана с национальными интересами России. «Сегодня развитие информационных ресурсов проводится в рамках задачи по цифровизации отрасли, которая решением Президента России определена одним из важнейших драйверов развития оборонно-промышленного комплекса страны», – подчеркнул представитель Роскосмоса, отметив также, что современные цифровые технологии выводят информационные ресурсы космической отрасли на качественно новый уровень, но и, вместе с тем, создают дополнительные риски[461].

14-15 октября 2021 г. очередная V Конференция, посвященная информационной безопасности в РКО, состоялась на площадках Технопарка Сколково и Московской школы управления Сколково. В центре внимания участников мероприятия были наиболее актуальные для ракетно-космического сектора технологические и организационные вопросы информационной безопасности, в том числе взаимодействие с ГосСОПКА, задачи импортозамещения и др.[462]

Поскольку создание центров ИБ представляет собой дорогостоящую задачу, в октябре 2019 г. Правительством РФ было принято решение о предоставлении из государственного бюджета субсидий, которые распределяются на конкурсной основе Министерством цифрового развития, связи и массовых коммуникаций РФ[463]. В сентябре 2020 г. в текст документа

---

[461] Роскосмос проводит IV конференцию по информационной безопасности в РКО [Электронный ресурс] // Роскосмос. Официальный сайт. 1 октября 2020 г. URL: https://www.roscosmos.ru/29330/ (Дата обращения: 17.04.2022)

[462] Роскосмос провел V отраслевую конференцию по информационной безопасности [Электронный ресурс] // Роскосмос. Официальный сайт. 18 октября 2021 г. URL: https://www.roscosmos.ru/33017/ (Дата обращения: 17.04.2022)

[463] Постановление Правительства РФ от 7 октября 2019 г. № 1285 «Об утверждении Правил предоставления субсидий из федерального бюджета на создание отраслевого

был внесен ряд изменений, касающихся объемов и структуры расходования средств, в том числе снималось ограничение (в размере 30%) на приобретение аппаратуры и ПО, а также предоставлялась возможность частичной компенсации расходов на приобретение товаров и услуг у третьих лиц[464].

Выступая на заседании Совета Безопасности РФ 20 мая 2022 г., Президент России В.В. Путин сообщил, что в стране действует Национальный кризисный штаб по предупреждению целевых компьютерных атак и сеть комиссий по информационной безопасности при полномочных представителях Президента РФ в федеральных округах. В то же время, как подчеркнул В.В. Путин, проверки, которые были проведены в течение 2021 г., показали, что необходимо дальнейшее системное повышение уровня ИБ в государственных органах, примерно 30% организаций и предприятий, имеющих объекты критической информационной инфраструктуры, еще предстоит создать ведомственные центры ГосСОПКА[465].

В рамках политики интенсификации повышения уровня безопасности КИИ и всего информационного пространства России министерства и ведомства информационного профиля выступили с инициативами, направленными на обеспечение технологического развития и защищенности отечественных IT-систем в условиях западных санкций в сочетании с взрывным ростом интенсивности кибератак из-за рубежа. Так, Российское

центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и включение его в систему автоматизированного обмена информацией об актуальных киберугрозах» // СЗ РФ, 2019, № 41, ст.5716

[464] Постановление Правительства Российской Федерации от 28 сентября 2020 № 1556 «О внесении изменений в Правила предоставления субсидий из федерального бюджета на создание отраслевого центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и включение его в систему автоматизированного обмена информацией об актуальных киберугрозах» // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202009300016

[465] Заседание Совета Безопасности РФ «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства». 20 мая 2022 г. [Электронный ресурс] // Совет Безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/3241/ (Дата обращения: 23.05.2022)

энергетическое агентство Минэнерго России в 2021 г. открыло цикл образовательных семинаров, посвященных вопросам кибербезопасности. В середине мая 2022 г. Министерство цифрового развития, связи и массовых коммуникаций РФ совместно с компанией «Ростелеком-Солар» организовало программу повышения квалификации для своего коллектива по совершенствованию навыков в области кибербезопасности. «Обучение прошли как рядовые сотрудники ведомства, так и руководители. Как показали результаты проведенных работ, сейчас более 90% сотрудников ведомства могут успешно распознать вредоносную рассылку», – отметил руководитель департамента обеспечения кибербезопасности Минцифры В. Бенгин[466].

Одним из важнейших направлений государственной политики России в области информационной безопасности в рассматриваемый период явилась информационная защита кредитных организаций и проводящихся ими операций от несанкционированного доступа и кибератак. Задачи нормативно-методического и технологического плана в данной сфере, выполнявшиеся в течение рассматриваемого периода Банком России и Министерством финансов приобретали все более важное значение в условиях расширения международных связей российских банков, в том числе в рамках формирования Валютного союза и других интеграционных программ на пространстве Евразии[467].

Дополнительным фактором интенсификации деятельности институтов информационной безопасности явилась пандемия COVID-19, следствием корой стало резкое увеличение цифрового трафика, в том числе в работе кредитных организаций, сетевой торговли и т.п. В этой связи Банк России в 2020 г. выпустил специальные рекомендации для финансовых компаний и организаций в сфере ИБ в целях снижения рисков ошибок и эффективного

[466] Минцифры обучило ИБ-навыкам своих сотрудников. [Электронный ресурс] // Сайт АНО «Радиочастотный спектр». 16 мая 2022 г. URL: https://rspectr.com/novosti/minczifry-obuchilo-ib-navykam-svoih-sotrudnikov (Дата обращения: 23.05.2022)

[467] Ершов В.Ф. Модернизационный этап развития банковской сферы России в контексте процессов глобализации // Наука и бизнес: пути развития. 2019. № 7 (97). С. 171-176.

распознавания мошеннических операций. В феврале 2021 г. Центробанк РФ впервые провел дистанционные антихакерские учения, в которых приняли участие 22 финансовых организации. В этот же период регулятор начал впервые штрафовать банки за пренебрежение правилами информационной безопасности. В марте 2022 г Центральный банк РФ разослал письмо, в котором просил кредитные организации обеспечить оперативную замену иностранному программному обеспечению в сфере кибербезопасности[468].

Таким образом, в течение периода 1990-х – 2022 гг. в Российской Федерации осуществлялись меры по обеспечению информационной безопасности органов государственной власти и управления, спецслужб, финансовых институтов, систем связи. Данное направление деятельности включало работу спецслужб и отраслевых органов защиты информации по обеспечению сохранности государственной тайны и другой информации ограниченного доступа, а также противодействие иностранным разведкам.

По мере включения России в систему глобальных цифровых коммуникаций на передний план в обеспечении информационной безопасности государства выходят мероприятия в области развития технологических цифровых средств защиты баз данных и коммуникационных систем. Кроме того, возрастает активность и внедряются эффективные высокотехнологичные методы работы российских спецслужб в сфере противодействия информационным угрозам со стороны киберпреступности, международному терроризму и экстремизму. Осуществляется создание киберподразделений в Вооруженных Силах РФ.

Во втором десятилетии XXI в. нарастание геополитической и экономической конкуренции приобретает все более острые формы противостояния, в том числе в информационной сфере, что обусловило переход в рамках государственной политики информационной безопасности строительство единой системы безопасности государственных органов и

[468] Политика ЦБ в сфере защиты информации (кибербезопасности) // Информационно-технологический портал TAdviser. 30 марта 2022 г. URL: https://www.tadviser.ru/index.php/) (Дата обращения: 23.05.2022)

стратегически значимых технологических и финансово-экономических объектов. Реализация данного направления государственной политики в сфере информатизационной безопасности включает совместную деятельность спецслужб, ФСТЭК и других институтов обеспечения информационной безопасности с ведущими IT-компаниями и экспертным сообществом России, государственные меры нормативного характера сочетаются с широким развитием отраслевых и межведомственных форумов, конференций и других площадок обмена опытом в области зашиты информации.

3.3. Российская Федерация и формирование глобальной системы информационной безопасности

Важнейшей составляющей государственной политики России в сфере информационной безопасности является участие в программах и проектах, направленных на формирование безопасного, способствующего глобальному диалогу и развитию международного информационного пространства.

Тема международной информационной безопасности (МИБ) утверждается как самостоятельное направление внешней политики Российской Федерации в течение периода 1990-х - 2000-х гг. по мере усиления фактора цифровых технологий в мировой политике и глобальной экономической конкуренции.

В рассматриваемый период Россия выступает в формате ООН, ШОС, СНГ и ряда других международных организаций инициатором, а также постоянным участником разработки и продвижения комплекса концептуальных документов, оказавших существенное влияние на становление глобальной и региональной систем международной информационной безопасности (МИБ). Одним из ключевых факторов становления данной тенденции явились процессы евразийской интеграции,

формирование нового вектора и реализация российской внешней политики на постсоветском пространстве[469].

Международная позиция России формировалась в русле рассмотренных выше стратегических подходов к обеспечению национальной информационной безопасности. Были приняты «Основы государственной политики Российской Федерации в области международной информационной безопасности» (2013), поставившие цель последовательного всемерного содействия обеспечению безопасности глобальной информационной среды и позволивших «сделать целый ряд значимых практических шагов» в данном направлении на уровне ООН[470].

1 октября 2014 г., открывая очередное заседание Совета Безопасности РФ, Президент России В.В. Путин подтвердил приверженность России политике сотрудничества по проблемам информационной безопасности в рамках СНГ, ШОС и БРИКС и подчеркнул значимость международного диалога в данной сфере, отметив, что «одной из площадок для оценки рисков и выработки совместных мер в сфере информационной безопасности, для анализа правовых последствий принимаемых решений должна стать Организация Объединенных Наций, ее профильные группы и специализированные структуры»[471].

В контексте формирования в XXI в. новых систем глобально-регионального взаимодействия на Евразийском континенте, существенное место во внешней политике России занимает участие в формировании интегрированного и безопасного информационного пространства

---

[469] *Пивовар Е.И.* Евразийский интеграционный проект на постсоветском пространстве: предпосылки, становление, развитие, (1991-2015 гг.). Санкт-Петербург: Алетейя, 2017. 719 с

[470] Вступительное слово Президента России В.В. Путина на заседании Совета Безопасности РФ 26 марта 2021 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.scrf.gov.ru/news/speeches/2952/

[471] Вступительное слово Президента России В.В. Путина на заседании Совета Безопасности России «О противодействии угрозам национальной безопасности в информационной сфере». 1 октября 2014 г. [Электронный ресурс] // Совет безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/2059/

Содружества Независимых Государств[472]. Активную позицию в глобальном диалоге по проблемам информационной безопасности в рассматриваемый период занимает Межпарламентская Ассамблея (МПА) СНГ, что способствует реализации программ в евразийском и глобальном форматах(МИБ)[473]. В 1996 г. член Комитета Государственной Думы по безопасности (председатель подкомитета по законодательству в сфере информационной безопасности) В.Н. Лопатин выдвинул предложение о расширении международного сотрудничества России и стран СНГ в интересах глобальной информационной безопасности[474]. Эта инициатива получила поддержку парламентариев России и ведущих постсоветских стран. В декабре 1997 г. Межпарламентской ассамблеей СНГ было принято обращение к ООН, ОБСЕ и государствам-участникам Межпарламентского союза, с предложением о включении в повестку заседаний Генеральной Ассамблеи ООН вопроса о заключении международной «Конвенции о предотвращении информационных войн и ограничении оборота информационного оружия». Как подчеркивал позднее В.Н. Лопатин, данная инициатива коррелировала с принятой в 2000 г. Доктриной информационной безопасности РФ, в которой заявлено о стремлении России противодействовать разработке, распространению и применению информационного оружия[475].

Вопросы сотрудничества в области информационного обмена и защиты информации стали частью международно-правовой базы СНГ уже на раннем этапе истории Содружества, когда были приняты «Соглашение о

---

[472] *Кучерявый М.М., Плотников В.А.* Региональная модель формирования информационного общества (на примере Содружества Независимых Государств) // Евразийская интеграция: экономика, право, политика. 2012. № 11. С. 138-143.

[473] *Кучерявый М.М.* Роль России и евразийского региона в формировании глобального подхода к обеспечению международной информационной безопасности // Евразийская интеграция: экономика, право, политика. 2012. № 12. С. 125-131.

[474] Международная информационная безопасность: подходы России / А.В. Крутских, Е.С. Зиновьева, В.И. Булва и др. Центр международной информационной безопасности и научно-технологической политики МГИМО МИД России. М.: МГИМО (Университет), 2021. С.194.

[475] *Лопатин В.Н.* Информационная безопасность России: Человек. Общество. Государство. СПб, 2000. С. 97-105.

сотрудничестве в области информации (9 октября 1992 г.) и «Соглашение о взаимном обеспечении сохранности межгосударственных секретов» (22 января 1993 г.).

В 1995 – 1996 гг. в соответствии с решениями Совета глав правительств СНГ был подготовлен текст проекта «Концепции формирования информационного пространства Содружества Независимых Государств» – рекомендательного документа, направленного на обеспечение согласованной информационной политики стран Содружества[476]. Концепция демонстрировала стремление стран СНГ к эффективному использованию возможностей нового этапа развития глобального информационного пространства и технологий в целях расширения международного сотрудничества на постсоветском пространстве. Авторы Концепции отмечали, что в условиях развивающейся транснационализации экономики, информационных и телекоммуникационных систем возрастает информационная взаимозависимость государств друг от друга, что требует повышения качества международных информационных коммуникаций и максимального взаимодействия во всех сферах, связанных с информацией. Концепция ориентировала стран Содружества не только на развитие внутреннего информационного пространства, но и на использование преимуществ глобальной информационной системы для укрепления своих позиций на мировых рынках[477].

На рубеже 1990-х – 2000-х гг., как было показано выше, активизируется и обновляется в концептуальном и правовом отношении государственная политика России в сфере обеспечения информационной безопасности страны. Этот процесс логично соединяется с расширением диалога по проблемам информационной безопасности в формате СНГ, где Россия играет ведущую роль, и появлением инициатив России и СНГ на

---

[476] Решение о Концепции формирования информационного пространства Содружества Независимых Государств (Москва, 18 октября 1996 г.) // Содружество: Информационный вестник Совета глав государств и Совета глав правительств СНГ. 1996. № 4.
[477] Там же.

уровне ООН, направленных на привлечение внимания мирового сообщества к идее обеспечения глобальной информационной безопасности.

В рамках СНГ велась последовательная работа по разработке и принятию документов, определяющих концептуальные подходы и направления взаимодействия по вопросам информационной безопасности. Вопросы развития международного информационного взаимодействия в регионе постсоветской Евразии отражены в ряде документов, принятых странами Содружества на рубеже XX – XXI в.: «Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ» (1999), «Положение о Координационном совете государств – участников СНГ по информатизации» (2002), «Стратегия сотрудничества стран СНГ в области информатизации» (2003, 2006) и др.

Изначально уже при создании СНГ была достигнута договоренность о взаимной защите государственных секретов. Наличие в странах Содружества определенной общности подходов к представлению о государственной тайне и другим аспектам защиты стратегически значимых компонентов национальной информационной безопасности создает почву для диалога и обмена опытом в данной сфере[478]. В XXI веке в рамках процесса евразийской интеграции и на фоне изменений глобальной архитектуры были приняты «Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности на период с 2008 по 2010 год» и Комплексный план мероприятийпо ее реализации (2006).

20 ноября 2013 г. в Санкт-Петербурге было подписано Соглашение о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности. Важной вехой в формировании единой

---

[478] *Вус М.А., Макаров О.С.* Законодательство СНГ: государственные тайны и государственные секреты // Актуальные проблемы права: Материалы IV Международной научной конференции, Москва, 20 - 23 ноября 2015 года. М.: Буки-Веди, 2015. С. 70-75; *Юсупов Р.М., Вус М.А.* К вопросу о совершенствовании модельного законодательства о государственных секретах в рамках Межпарламентской Ассамблеи СНГ // Власть, 2015. № 7. С. 194 – 196.

информационной политики стран Содружества, в том числе подходов к международной информационной безопасности, явилось 41-е пленарное заседании Межпарламентской Ассамблеи СНГ 28 ноября 2014 г., на котором была утвержден проект «Стратегии обеспечения информационной безопасности государств-участников СНГ», подготовленный группой российских и белорусских специалистов и прошедший необходимые согласования[479]

Политика обеспечения информационной безопасности на территории Евразии и согласованных действий стран Содружества в системе глобальных информационных отношений нашла свое выражение в процессе формирования модельного законодательства СНГ. В 2003 г. Межпарламентская Ассамблея (МПА) СНГ утвердила модельный закон «О государственных секретах», в 2005 г. был принят модельный закон модельный закон «Об информатизации, информации и защите информации»[480].

Данное направление межпарламентского сотрудничества государств Содружества нашло отражение в содержании «Перспективного плана модельного законотворчества в СНГ» на 2011–2015 гг. В рамках данного Плана 23 ноября 2012 г. МПА СНГ были утверждены «Рекомендации по совершенствованию и гармонизации национального законодательства государств-участников СНГ в сфере обеспечения информационной безопасности», направленные на «создание правовых условий для системной реализации и обеспечения защиты сбалансированных интересов личности, общества и государства в рамках государственной политики развития

---

[479] *Вус М.А., Макаров О.С.* Стратегический вектор обеспечения международной информационной безопасности на пространстве СНГ // Юридические науки: проблемы и перспективы: материалы V Международной научной конференции (г. Казань, октябрь 2016 г.). Казань: Бук, 2016. С. 40-43.

[480] Модельный закон «Об информатизации, информации и защите информации». Принят на 26 Пленарном заседании МПА СНГ. Постановление от 18 ноября 2005 г. № 26-7 [Электронный ресурс] // Электронный фонд правовых и нормативно-технических документов «Кодекс» URL: https://docs.cntd.ru/document/901972159 (Дата обращения: 20.04.2022)

информационного общества»[481]. С этой целью страны – участники МПА СНГ ставили перед собой задачи:

1. по разработке правовых норм, которые создавали бы комплексную эффективную защиту информационной безопасности;

2. по развитию взаимодействия в данной сфере в рамках СНГ;

3. по обеспечению для стран Содружества равноправного участия в международных отношениях в области информации. Решение данных задач, в свою очередь, требовало проработки и унификации правовых дефиниций, касающихся сферы информационной безопасности[482].

Значительный вклад в развитие данного направления сотрудничества стран Содружества внес российско-белорусский научный коллектив по разработке модельного законодательства СНГ, в который вошли специалисты Института государства и права РАН, Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), Института национальной безопасности и Академии МВД Республики Беларусь.

28 ноября 2014 г. МПА СНГ приняла (одновременно со «Стратегией обеспечения информационной безопасности государств участников СНГ») Модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры»[483] и новый вариант Модельного закона «Об информации, информатизации и обеспечении информационной безопасности». Утвержденный МПАпрект «Стратегии обеспечения информационной безопасности государств-участников СНГ» был направлен для дальнейшего рассмотрения в Исполнительный комитет СНГ и прошел экспертизу министерств и ведомств. После внесения ряда замечаний документ был последовательно одобрен Экономическим советом СНГ и

---

[481] Постановление МПА СНГ от 23 ноября 2012 г. № 38-20.

[482] Там же.

[483] Модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры». Принят Постановлением МПА СНГ от 28 ноября 2014 г. № 41-14 [Электронный ресурс] // Информационно-правовая система «Гарант». URL: https://base.garant.ru/71871816/ (Дата обращения: 20.04.2022)

Советом министров иностранных дел СНГ. Окончательно «Стратегии обеспечения информационной безопасности государств-участников СНГ» была принята Советом глав правительств Содружества 25 октября 2019 г., что подтвердило общность позиций стран СНГ в отношении проблем региональной и глобальной безопасности.

Несколько ранее, 5 апреля 2019 г., министр иностранных дел России С.В. Лавров, комментируя итоги очередного заседания Совета министров иностранных дел (СМИД) стран СНГ, отметил, что руководители внешнеполитических ведомств государств Содружества придают большое значение вопросам укрепления международной информационной безопасности и согласованию политики своих стран в данной сфере. Глава МИД России также сообщил журналистам, что на заседании прошло согласование ряда документов, направленных на борьбу с киберпреступностью, участники Совета «поговорили о проблемах, которые возникают в киберпространстве, о необходимости укреплять международную информационную безопасность, координировать наши подходы к той работе, которая развернута в ООН по этой важнейшей теме»[484].

28 сентября 2018 г. было подписано межправительственное «Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий».

Задачи сотрудничества в сфере информационной безопасности в 2010-е гг. решались в рамках согласования правовых норм стран – участниц Таможенного Союза[485]. Развивалось также взаимодействие России с партнерами по СНГ в сфере информационной безопасности на двустороннем уровне. Так, в 2015 г. было подписано российско-белорусское

---

[484] С.В. Лавров назвал безусловным приоритетом для России углубление интеграции в рамках СНГ [Электронный ресурс] // ТАСС. 5 апреля 2019 г. URL: https://tass.ru/politika/6300390 (Дата обращения: 20.04.2022)

[485] *Бакаева О.Ю.* Государственный контроль в сфере защиты государственной тайны: актуальные вопросы правового регулирования // Информационная безопасность регионов. 2013. № 1 (12). С. 95.

межправительственное Соглашение о сотрудничестве в области обеспечения международной информационной безопасности. Президенты России и Узбекистана В.В. Путин и Ш.М. Мирзиёев в ходе официального визита лидера Узбекистана в Москву 19 ноября 2021 г. утвердили «Совместное заявление о сотрудничестве в области обеспечения международной информационной безопасности», в котором обращались к мировому сообществу с призывом о принятии всех необходимых мер для предотвращения применения информационных технологий «в военно-политических целях, противоречащих международному праву, и осуществления враждебных действий и актов агрессии»[486]. Также в документе подчеркивалось, что трансграничная природа ИКТ требует, наряду с мерами информационной безопасности, которые принимаются каждым государством, консолидированных действий как на уровне выстраивания двусторонних отношений, так и в региональном и глобальном форматах мирового сообщества[487].

Проблематика обеспечения региональной и глобальной информационной безопасности составляет важное, постоянно развивающееся направление сотрудничества спецслужб стран Содружества. Осенью 2021 г. состоялось XVII Совещание руководителей органов безопасности и разведывательных служб государств-участников СНГ, на открытии которого выступил секретарь Совета Безопасности России Н.П. Патрушев. Докладчик отметил, что в настоящее время существенно актуализировались задачи информационного взаимодействия стран СНГ в целях обеспечения национальной и региональной безопасности. Он отметил, что на фоне «неуклонно деградирующей ситуации в мире» США и блок НАТО стремятся переложить ответственность на существующие проблемы, в том числе своего

---

[486] Совместное заявление Президента Российской Федерации В.В. Путина и Президента Республики Узбекистан Ш.М. Мирзиёева о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] // Президент России. Официальный сайт. 19 ноября 2021 г. URL: https://www.kremlin.ru/supplement/5739 (Дата обращения: 20.04.2022)

[487] Там же.

внутреннего положения, на Россию, Китай и другие страны, отстаивающие принципы многополярности и государственного суверенитета[488]. Докладчик сообщил, что США в 2022 г. намерены увеличить до 3 млрд долларов расходы на т.н. «демократизацию» других стран и регионов мира, причем основное внимание обращается на постсоветские страны, ослабление интеграционных связей на пространстве Евразии. В связи с этим возрастает актуальность диалога спецслужб и правоохранительных органов стран СНГ в целях предотвращения реализации сценариев «цветных революций», борьбы с экстремизмом и другими дестабилизирующими обстановку в регионе явлениями. «В данных условиях нам необходимо наращивать получение и обмен разведывательной информацией о планах международных террористических организаций и намерениях Запада по их использованию против наших стран», – подчеркнул Н.П. Патрушев, комментируя вывод американских войск из Афганистана[489].

В тексте доклада Н.П. Патрушева, опубликованном на сайте СБ РФ, значительное место уделено вопросам защиты информации и борьбы с киберпреступностью. В частности, дана характеристика новым информационным угрозам, возникшим в период пандемии COVID-19 в условиях резкого расширения глобальных сетевых коммуникаций при одновременном ограничении международных транспортных и миграционных потоков. Данные обстоятельства стали стимулом для перехода террористов и преступников в цифровое поле, возросли риски хакерских атак в целях экономических преступлений и диверсий в отношении объектов КИИ. «Террористами уже создаются собственные киберподразделения. При этом особую опасность видим в сложности своевременного установления подлинного источника атаки, что может, например, привести к острым

---

[488] Выступление Секретаря Совета Безопасности Российской Федерации Н.П. Патрушева на открытии XVII Совещания руководителей органов безопасности и разведывательных служб государств-участников СНГ по вопросам разведывательной деятельности [Электронный ресурс] // Совет Безопасности РФ. Официальный сайт. 13 октября 2021 г. URL: https://www.scrf.gov.ru/news/speeches/3098/ Дата обращения: 19.04.2022)

[489] Там же.

межгосударственным конфликтам вплоть до вооруженных столкновений», – подчеркнул Н.П. Патрушев. Он также дал характеристику политике НАТО в области развития наступательного информационного потенциала, включая создание национальных и коалиционных кибервойск, разработок в области искусственного интеллекта и др. Секретарем Совета Безопасности РФ был высказан ряд предложений по укреплению взаимодействия спецслужб стран Содружества, расширению предметного диалога силовых структур в сфере обеспечения информационной безопасности. В том числе Н.П. Патрушев предложил активизировать двусторонние консультации по ИБ, модернизировать и расширить международно-правовую базу данного направления сотрудничества, разработать единую классификацию существующих угроз международной безопасности и усилить взаимодействие по линии предотвращения информационных угроз стратегически значимым государственным ресурсам[490].

Важным дополнительным компонентом укрепления международных связей России со странами СНГ в сфере обеспечения задач информационной безопасности является ОДКБ и его Парламентская Ассамблея (ПА ОДКБ) [491]. Так, были разработаны Проект «Рекомендаций по сближения законодательства государств-членов ОДКБ по вопросам государственной тайны» и «Глоссарий основных понятий в законодательстве о государственной тайне государств-членов ОДКБ». Оба документы были приняты Парламентской Ассамблеей ОДКБ 27 октября 2010 г.[492]

---

[490] Выступление Секретаря Совета Безопасности Российской Федерации Н.П. Патрушева на открытии XVII Совещания руководителей органов безопасности и разведывательных служб государств-участников СНГ по вопросам разведывательной деятельности [Электронный ресурс] // Совет Безопасности РФ. Официальный сайт. 13 октября 2021 г. URL: https://www.scrf.gov.ru/news/speeches/3098/ Дата обращения: 19.04.2022)

[491] *Бондуровский В.В., Бачило И.Л., Вус М.А. Кучерявый М.М., Макаров О.С.* Парламентское измерение информационной безопасности в рамках СНГ и ОДКБ на современном этапе // Информатизация и связь. 2014. № 3. С. 8-13.

[492] Постановление Парламентской Ассамблеи ОДКБ от 27 октября 2010 г. № 4-7. [Электронный ресурс] URL: http://paodkb.coalla.ru/uploads/document/file/42/rekomendatsii-po-sblizhen.-i-garmoniz.-natsion.-zak_va-gos._chlenov-odkb-v-sfere-obesp.-inf._kommunik.-bezop.pdf (Дата обращения: 20.04.2022)

30 ноября 2017 г. в Минске было подписано «Соглашение о сотрудничестве государств-членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности», вступившее в силу 1 апреля 2018 г. В последующий период данная тема остается в центре внимания аппарата и экспертных групп ОДКБ. 19 апреля 2021 г. состоялось заседание Комитета секретарей Советов безопасности государств – членов ОДКБ, участники которого обсудили, в том числе вопросы информационной безопасности на постсоветском пространстве[493]. 15 июня того же года, в ходе очередного заседания Комитета в Минске, секретарь Совета Безопасности России Н.П. Патрушев призвал своих коллег провести работу по дальнейшей активизации информационного обмена в рамках борьбы с кибератаками[494]. 29 ноября 2021 г. на Пленарном заседании Парламентской Ассамблеи ОДКБ был принят модельный закон «Об информационной безопасности», который, по словам Н.П. Патрушева, является «основой для сотрудничества по решению задач обеспечения информационной безопасности, предусмотренных Стратегией коллективной безопасности ОДКБ до 2025 года».

Председатель Постоянной комиссии ПА ОДБ по обороне и безопасности по вопросам обороны и безопасности, заместитель председателя Комитета Государственной РФ по безопасности и противодействию коррупции А. Выборный, комментируя принятие закона, отметил, что принятие закона обусловлено комплексом факторов, прежде всего, «расширением спектра угроз информбезопасности, включая изменения их характера и интенсивности; так и попытками иностранных государств

[493] В Душанбе Секретарь Совета Безопасности России Николай Патрушев принял участие в заседании комитета секретарей советов безопасности государств-членов Организации Договора о коллективной безопасности (ОДКБ) [Электронный ресурс] // Совет безопасности РФ. Официальный сайт. URL: http://www.scrf.gov.ru/news/allnews/2979/ (Дата обращения: 19.04.2022)

[494] Патрушев призвал ОДКБ усилить обмен информацией для борьбы с кибератаками [Электронный ресурс] // РИА Новости. 15 июня 2017 г. URL: https://ria.ru/20170615/1496565023.html (Дата обращения: 19.04.2022)

получать конфиденциальную информацию о состоянии обеспечения национальной информбезопасности»[495].

Россия вносит вклад в решение проблем международной информационной безопасности как участник ШОС и БРИКС, растущий авторитет которых в глобальном сообществе, в том числе способствует утверждению общих инициатив на уровне ООН по укреплению МИБ[496].

В 2006 г. начала работу Группа экспертов ШОС по международной информационной безопасности, что сыграло позитивную роль в активизации интереса к данной проблеме в различных глобальных и региональных организациях[497]. 16 июня 2009 г. было подписано Соглашение государств-членов ШОС о сотрудничестве в области обеспечения информационной безопасности, в котором выражают готовность к совместной работе по «определение, согласование и осуществление необходимых совместных мер в области обеспечения международной информационной безопасности»[498].

Примером совместных действий стран ШОС на глобальном уровне являются «Правила поведения в области обеспечения международной информационной безопасности», которые были 12 сентября 2011 г. направлены Генеральному секретарю ООН представителями России, Китая, Таджикистана и Узбекистана при ООН и рассмотрены на 66-й сессии Генеральной Ассамблеи ООН. Разработке и реализации инициатив ШОС в

---

[495] Ассамблея приняла модельный закон «Об информационной безопасности» [Электронный ресурс] // Парламентская Ассамблея ОДКБ. Официальный сайт. 30 ноября 2021 г. URL: https://paodkb.org/events/assambleya-prinyala-modelnyy-zakon-ob-informatsionnoy-bezopasnosti (Дата обращения: 20.04.2022)

[496] Бойко С.М. Проблематика международной информационной безопасности на площадках ШОС и БРИКС // Международная жизнь. 2019. № 1. С. 1-22.

[497] Международная информационная безопасность: дипломатия мира / Под ред. С.А. Комова. М., 2009. 264 с.

[498] Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] // Электронный фонд правовых и нормативно-технических документов «Кодекс». URL: https://docs.cntd.ru/document/902289626 (Дата обращения: 20.04.2022)

области международной информационной безопасности способствует близость позиций России и Китая по данному вопросу[499].

Летом в Уфе 2015 г. состоялся Саммит БРИКС, участники которого выступили с осуждением «актов массовой электронной слежки и сбора данных о частных лицах по всему миру», подчеркнув, что современные государства находятся на разных уровнях развития информационно-коммуникационных технологий, что дополнительно повышает значимость задач в сфере расширения всеобщего доступа к ИКТ и использования их исключительно в целях глобального мира и развития[500].

В 2010-е гг. в разработке и реализации государственной политики России в области международной безопасности участвуют сотрудники академических институтов, университетов, профильных научных обществ. Так, например, по инициативе Института проблем информационной безопасности МГУ имени М.В. Ломоносова в 2010 г. был создан Международный исследовательский консорциум информационной безопасности (МИКИБ). В апреле 2018 г. была создана Национальная ассоциация международной информационной безопасности (НАМИБ), учредителями которой выступили ведущие вузы и научные центры России, в том числе МГУ им. М.В. Ломоносова, МГИМО (Университет) и Дипломатическая академия МИД России, РАНХиГС при Президенте РФ, Институт современных проблем безопасности и др. Главой НАМИБ был избран В.П. Шерстюк, директор Института проблем информационной безопасности МГУ, его заместителем стал А.И. Смирнов, президент Национального исследовательского института глобальной безопасности. Работа НАБИМ, выступающей организатором и участником международных конференций по информационной безопасности и подготовкой

---

[499] Международная информационная безопасность: подходы России / А.В. Крутских, Е.С. Зиновьева, В.И. Булва и др. М.: МГИМО (Университет), 2021. С. 31.

[500] Страны БРИКС осудили акты массовой электронной слежки и сбора данных о людях по всему миру // ТАСС. 9 июля 2015 г. URL: https://tass.ru/politika/2107335?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru

мониторингов, научно-исследовательских проектов, осуществляется пр и поддержке Совета Безопасности РФ.

Площадками диалога руководителей и специалистов национальных органов безопасности, дипломатов, ученых, лидеров IT-бизнеса стран ОБКБ, ШОС и БРИКС в 2010-е гг. стали международные форумы по информационной безопасности, в том числе «Инфофорум-Югра»[501] и ряд других крупных международных конференций, о которых упоминалось выше. Активную позицию в качестве инициатора и организатора подобных мероприятий занимает Китайская Народная Республика. Так, ежегодно с 2010 г. проводится «Международная конференция «Доверие и безопасность в информационном обществе» (Инфофорум-Китай), которая организуется при участии Аппарата Совета Безопасности РФ и профильных комитетов Государственной Думы России. С китайской стороны поддержку данному проекту оказывают Huawei и другие ведущие компании, действующие на рынке информационных технологий, профильные научные центры КНР. Кроме того, вплоть до недавнего времени партнером «Инфофорума-Китай» выступал отдел Китая Альянса облачной безопасности (Cloud Security Alliance-CSA), международной организации, объединяющей преимущественно американских и европейских специалистов в области цифровых технологий безопасности. Какую позицию CSA занял в условиях развернувшейся на Западе весной 2022 г. антироссийской кампании оставалось неясным; во всяком случае, куратор Альянса по региону Большого Китая профессор Йель Ли, который был заявлен как участник очередного Инфофорума-Югра 6-9 июня 2022 г., не присутствовал на его мероприятиях. Заместитель генерального секретаря Альянса облачной безопасности Муди Сюй обратилась онлайн с приветствием к участникам

[501] Инфофорум-Югра 2022. Программа [Электронный ресурс] // Сайт Инфофорума-Югра 2022. URL: https://infoforum.ru/programma-infoforum-jugra-2022 (Дата обращения: 20.04.2022)

форума, подчеркнув его значение как фактора международного цифрового сотрудничества.[502]

В начале XXI в. информационные технологии выступают как один из ключевых факторов развития международных отношений и глобальной безопасности, причем их влияние на геополитические процессы, мировую экономику и культуру имеет двойственный характер. Цифровизация представляет собой качественно новый, по сравнению с предыдущими историческими эпохами стимул развития человечества и в то же время – мощную силу, которая может быть использована в целях конфронтации, в конкурентной борьбе и гибридных войнах[503]. Важную роль вопросы информационной безопасности занимают в деятельности органов правопорядка в контексте борьбы с международным терроризмом и организованной преступностью.

Позиция России в отношении проблем, связанных с международной информационной безопасностью, характеризуется неизменностью и принципиальностью подходов, трактовкой МИБ как модели межгосударственного взаимодействия, которая опирается на действующее международное право и обеспечивает симметричную защищенность всей совокупности интересов участников международных отношений. Это обусловило широкую поддержку российским инициативам в ООН и нашло выражение деятельности экспертных групп ООН, занимающихся выработкой подходов мирового сообщества к проблемам информационной безопасности: Группы правительственных экспертов (ГПЭ) – с 2004 г. и Рабочей группы открытого состава (РГОС) – с 2019 г.

Вклад России в деятельность ООН по разработке и реализации программ обеспечения глобальной информационной безопасности детально рассмотрена в аналитическом докладе, подготовленном коллективом Центра

---

[502] Инфофорум-Югра 2022. Ключевые участники. [Электронный ресурс] // Сайт Инфофорума-Югра 2022. URL: https://infoforum.ru/greetings/g-zha-mudi-sjuj (Дата обращения: 04.07.2022)

[503] *Смирнов А.В.* Современные информационные технологии в международных отношениях: монография. М., МГИМО-Университет, 2017. 334 с.

международной информационной безопасности и научно-технологической политики МГИМО МИД «Международная информационная безопасность: подходы России»[504]. Основными вехами процесса утверждения Российской Федерации в статусе одного из глобальных лидеров – создателей системы международной информационной безопасности стали следующие события:

- специальное послание министра иностранных дел РФ И.С. Иванова генеральному секретарю ООН К. Аннану от 23 сентября 1998 г. о росте угроз международной информационной безопасности со стороны международного терроризма и организованной преступности;

- принятие по инициативе России резолюция Генеральной Ассамблеи ООН 4 декабря 1998 г. «Достижения в сфере информатизации и телекоммуникаций», в которой впервые была сформулирована «триада угроз» МИБ: использование ИКТ в военно-политических целях, использование ИКТ в преступных целях, использование ИКТ в террористических целях[505];

- включение положений подготовленного Россией проекта «Принципы, касающиеся международной информационной безопасности», в Доклад Генерального секретаря ООН 10 июля 2000 г.;

- принятие в 2001 г. по инициативе России решения 56-й сессии Генеральной Ассамблеи ООН решения о формировании первой Группы правительственных экспертов (ГПЭ) государств-членов ООН и последующая работа Группы в период 2004 – 2015 гг.

- выдвижение на 61, 62 и 63 Генеральных Ассамблеях ООН российских проектов резолюций «Достижения в области информатизации и телекоммуникаций в контексте международной безопасности», которые были приняты, несмотря на противодействие США;

---

[504] Международная информационная безопасность: подходы России / А.В. Крутских, Е.С. Зиновьева, В.И. Булва и др. Центр международной информационной безопасности и научно-технологической политики МГИМО МИД России. М.: МГИМО (Университет), 2021: Электронная версия. URL: https://mgimo.ru/upload/2022/03/mezhdunarodnaya-informatsionnaya-bezopasnost-podkhody-rossii.pdf

[505] Там же. С. 8.

- высокая оценка результатов работы ГПЭ первого созыва в резолюции Генеральной Ассамблеи ООН 2010 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»;

- принятие 68-й сессией Генеральной Ассамблеи ООН российского проекта резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

Специалисты МГИМО в своем исследовании подчеркивают, что на площадке ООН с конца 2000-х гг. шли острые дискуссии между США и их единомышленниками, отстаивавшими чисто технологическое видение проблемы МАБ, в то время как Россия, страны СНГ и ШОС целый ряд других государств, представляющих различные регионы мира, поддерживали целостный подход к вопросу информационной безопасности, включающий гуманитарные аспекты и следование базовым принципам равноправия субъектов международного права, представление о недопустимости гонки вооружений в информационном пространстве.

В 2018 г. 73-й сессией Генеральной Ассамблеей ООН по инициативе России была принята резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», ставшая основанием для создания Рабочей группы ООН открытого состава (РГОС) для дальнейшей работы по тематике информатизации и телекоммуникаций, к сотрудничеству в которой приглашались все заинтересованные страны. США предложили свой проект резолюции, также поддержанный ООН, вследствие чего была воссоздана Группа правительственных экспертов, причем в ее состав вошли представители России, а в работе РГОС приняли участие США.

В целом, при продолжающемся противостоянии российского и американского подходов к МИБ по многим позициям были выработаны компромиссные варианты, либо получала поддержку позиция России и ШОС. Это способствовало сдерживанию опасной тенденции, когда страны Запада пытались «закрепить в информационном пространстве «право сильного», провести концепцию силовых контрмер (в т.ч. в обход Совета

Безопасности ООН) и «отнести киберпространство к сфере ведения военных действий»[506]. Наиболее активными сторонниками данного направления помимо США выступали Великобритания, Нидерланды и Канада.

В 2020 – 2021 гг. Россия продолжала следовать курсу взаимодействия с ООН по проблемам обеспечения глобальной информационной безопасности, Президент России В.В. Путин в сентябре 2020 г. высказал идею о возможности возобновления российско-американского диалога в сфере кибербезопасности, в целях снижения рисков «масштабной конфронтации в цифровой сфере»[507]. Российский лидер предложил администрации США реализовать комплекс практических мер в данном направлении, в том числе: восстановить диалог России и США по ключевым вопросам обеспечения МИБ на высоком уровне. В.В. Путин отметил также, что позитивное воздействие на сферу информационной безопасности окажет совместная разработка и заключение двустороннего межправительственного соглашения о предотвращении инцидентов в информационном пространстве, аналогом которого могло бы стать действующее «Соглашением о предотвращении инцидентов в открытом море и воздушном пространстве над ним», заключенное между СССР и США 25 мая 1972 года[508].

В октябре 2020 г. года заместитель Председателя Совета Безопасности РФ Д.А. Медведев в своей колонке для Russia Today напомнил, что «Россия неоднократно призывала мировое сообщество договориться о новых механизмах противодействия киберпреступности и обеспечения стабильности информационной среды»[509]. Дмитрий Медведев предложил

---

[506] Международная информационная безопасность: подходы России / А.В. Крутских, Е.С. Зиновьева, В.И. Булва и др. Центр международной информационной безопасности и научно-технологической политики МГИМО МИД России. М.: МГИМО (Университет), 2021: Электронная версия. URL: https://mgimo.ru/upload/2022/03/mezhdunarodnaya-informatsionnaya-bezopasnost-podkhody-rossii.pdfC.18.

[507] *Тарасенко П.* Путин предложил США восстановить сотрудничество в сфере информационной безопасности // Российская газета. 27 сентября 2020 г. С. 1.

[508] Там же.

[509] Дмитрий Медведев заявил о необходимости общемирового договора о кибербезопасности // Коммерсантъ. 24 октября 2020 г. URL: https://www.kommersant.ru/doc/4547586 (Дата обращения: 20.04.2022)

продолжить, на базе ООН, работу над универсальным международным договором по информационной безопасности, в котором заинтересовано все человечество.

26 марта 2021 гг. состоялось заседание Совета Безопасности РФ, посвященное обсуждению проекта документа «Основы государственной политики Российской Федерации в области международной информационной безопасности». Председатель СБ РФ, Президент России В.В. Путин в своем вступительном слове отметил, что новые технологические решения, с одной стороны являются ступенькой к новому этапу развития человечества, создают огромные преимущества в сфере экономики, культуры, глобальных коммуникаций, но в то же время, и новые риски, возникает жесткое противоборство в глобальном цифровом пространстве, имеют место нечестная конкуренция и кибератаки, что качественно меняет ситуацию на международной арене»[510].

В.В. Путин дал обзор международных инициатив Российской Федерации по созданию международно-правовой базы информационной безопасности, в том числе подчеркнул, что именно предложения России легли в основу резолюций Генеральной Ассамблеи ООН по информационной безопасности в 1998 и 2018 гг., а сама тематика глобальной информационной безопасности прочно вошла в повестку дня ООН. Позиция Российской Федерации по вопросам международной информационной безопасности, подчеркнул он, неизменно определяется принципами открытости и прозрачности, приверженности нормам международного права и идее цифрового суверенитета государств, соблюдению равенства, порядка и взаимного уважения в информационной сфере.[511]

Президент отметил, что в обновленной Стратегии необходимо отразить преемственность стратегического курса России в сфере международной

---

[510] Вступительное слово Президента России В.В. Путина на заседании Совета Безопасности РФ 26 марта 2021 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.scrf.gov.ru/news/speeches/2952/

[511] Там же.

информационной безопасности, показать ее «открытость для диалога и конструктивного взаимодействия со всеми партнёрами» и обозначил ряд конкретных направлений работы. В том числе В.В. Путин предложил активизировать продвижение российских инициатив на международной арене, оказывать ближайшим партнерам России технологическое содействие в создании систем ИБ, развивать сотрудничество по борьбе с киберпреступностью, расширять участие научного сообщества в реализации поставленных задач, включая взаимодействие с Национальной ассоциацией международной информационной безопасности (НАМИБ).

Таким образом, в течение периода 1991 – 2022 гг. в Российской Федерации происходило наращивание и синхронизация деятельности институтов информационной безопасности государства и общества.

Государственная политика России в сфере информационной безопасности формировалась на основе концептуальных подходов и правовой базы, содержание которых коррелировало с изменяющимися параметрами российского и глобального информационного пространства и динамикой международных отношений. Данные задачи осуществлялись Президентом РФ, Аппаратом Совета Безопасности России, Государственной Думой РФ и ее профильными комитетами, и комиссиями, а также органами исполнительной власти и научно-экспертными структурами, участвовавшими в подготовке концепций и законопроектов по информационной безопасности.

В 1990-е гг. российские спецслужбы и структуры защиты информации Вооруженных Сил и органов правопорядка были, насколько позволяют судить открытые источники, сосредоточены на вопросах противодействия информационным угрозам, возникавшим в процессе преодоления внутренней нестабильности и экономическим преступлениям против структур частного бизнеса.

В течение двух первых десятилетий XXI в. модернизация всей системы информационной безопасности и существенные изменения геополитической

обстановки актуализировали деятельность российских спецслужб в вопросах оперативного и технологического противостояния иностранным электронным разведкам, хакерским атакам, а в период 2014 – 2022 гг. проявлениям гибридной кибервойны. В работе Совета Безопасности во главе с Президентом России В.В. Путиным на первый план также выходят вопросы обеспечения защиты государственных органов, российского общества и бизнеса от внешних угроз. При этом качественный уровень и, соответственно, эффективность работы институтов информационной безопасности России в течение 2010-х гг. существенно возросли, что позволило решать задачи, на порядок более сложные по сравнению с эпохой 1991 – 2000-х гг.

Работа государственных институтов информационной безопасности РФ в рассматриваемый период осуществляется во взаимодействии с российским и международным IT-сообществом, стимулируется проведением широкого круга общественных форумов, независимых экспертов и СМИ.

На протяжении всего рассматриваемого периода формировались и развались международные связи России в сфере информационной безопасности по линии СНГ. На рубеже XX – XXI в., когда были сделаны первые реальные шаги в направлении евразийской интеграции, начинается и процесс утверждения в ООН концепции и мониторинга международной информационной безопасности на основе инициатив России и стран Содружества, получивших широкую поддержку на уровне Генеральной Ассамблеи и организаций ООН.

В 2000 – 2010–е гг. развитие международно-договорных основ информационной безопасности в форматах СНГ, ОДКБ, ШОС и БРИКС при дальнейшей реализации российской программы МИБ на площадках ООН позволяет говорить об утверждении Российской Федерации в статусе одного из мировых лидеров формирования системы глобально-региональной системы международной информационной безопасности.

ЗАКЛЮЧЕНИЕ

Проведенный анализ исторического опыта и реализации государственной политики Российской Федерации в сфере информационной безопасности в 1991–2021 гг. позволяет сделать ряд обобщений и выводов.

Основные институциональные и технологические компоненты российской государственной политики в области обеспечения информационной безопасности страны, сформировавшиеся в период СССР, включали систему органов государственной безопасности, научных и образовательных организаций, осуществлявших подготовку кадров специалистов в области криптографии, специальной связи и др.

Целый ряд механизмов, апробированных в рамках советской системы информационной безопасности, например, составление перечней сведений, составляющих государственную и военную тайну, используется в постсоветский период до настоящего времени.

Специфика сложившейся государственной политики информационной безопасности в период СССР была обусловлена влиянием геополитического противостояния двух систем в условиях «холодной войны», что определяло развитие комплексов информационной безопасности, обеспечивающих защиту государственной тайны в Вооруженных силах СССР, органах внутренней и внешней разведки, стратегических важных отраслях промышленности. Организационно-правовые формы обеспечения информационной безопасности включали использование криптографии, режимов секретности и т.п., свойственные в целом всем государствам мира.

Особенностью политики СССР в сфере информационной безопасности являлось противодействие идеологическому проникновению в информационное пространство советского общества идей и образов западного капиталистического мира, подрывавших идейную монополию партии, а также цензурный контроль всех видов СМИ и печатных изданий.

Важным аспектом предыстории современной государственной политики России в области информационной безопасности стало появление в позднем СССР персональных компьютеров, выход в свет первых научных и научно-популярных работ, посвященных феномену информационного общества.

К 1991 г. выявились ключевые тенденции в развитии государственно-общественной жизни и экономики России, непосредственно связанные со сферой информационной безопасности: либерализация СМИ и отмена политической цензуры; высокий интерес населения к компьютерной технике, начало информатизации экономики и образования; зарождение правового института коммерческой тайны и других аспектов защиты информации, связанных со становлением рыночных отношений; установление широких международных финансово-экономических и культурных связей, способствовавших приходу в Россию идей и технологий информационного общества.

В последующий период формирование концепций и правовых норм государственной политики Российской Федерации в области информационной безопасности происходило под влиянием комплекса факторов, среди которых:

- интеграция России в мировое информационное пространство и развитие телекоммуникационных систем, внедрение цифровых технологий в различные сферы экономики и бизнеса, деятельность СМИ, частную повседневную жизнь россиян;

- утверждение в 1990-е гг. новых подходов к внутренней и внешней информационной политике, опирающихся на принципы демократической государственности и концепцию всестороннего сотрудничества со странами Запада и другими зарубежными партнерами;

- формирование с конца 1980-х гг. социально-профессиональных групп, непосредственно вовлеченных в процессы информатизации страны – IT-специалистов, предпринимателей в сфере связи и цифровых услуг,

торговли компьютерной техникой и программным обеспечением и др., становление сетевых сообществ;

- реализация в 2000–2010-е гг. стратегических программ социально-экономической модернизации страны, включавших, с одной стороны, дальнейшее внедрение цифровых технологий, в том числе информатизацию системы государственного управления, с другой – укрепление институтов защиты и контроля информационной безопасности государства, экономики и общества.

Развитие государственной политики Российской Федерации в указанной сфере в течение рассматриваемого периода прошло ряд этапов. В начале 1990-х гг. осуществлялась разработка новых нормативно-правовых механизмов обеспечения информационной безопасности личности и бизнеса, защиты государственной тайны и других видов секретной и конфиденциальной информации. В реформируемой России шло строительство демократической государственности, происходило становление институтов гражданского общества, что находило отражение в законодательном оформлении прав граждан на свободное получение и использование информации. В этот период складываются подходы, характерные для различных групп участников формирования и реализации государственной политики в области ИБ. Так для представителей спецслужб, оборонного ведомства, органов правопорядка приоритетом неизменно остается зашита государственной тайны и служебной информации, для СМИ – реализация права на получение и распространение информации, для бизнеса и пользователей Интернета – в равной мере важны как защищенность от несанкционированного доступа, так и наличие широкого коммуникативного пространства. Соответственно, главной задачей государственной политики РФ в области информационной безопасности на протяжении всего рассматриваемого периода являлось установление баланса между обеспечением государственной безопасности, защитой

конфиденциальности персональной и корпоративной информации – и реализацией принципа свободы информационных коммуникаций в обществе.

Тема информационной безопасности РФ в 1991–2021 гг. неизменно являлась предметом общественных дискуссий, участниками которых были депутаты Государственной Думы РФ, представители органов власти и управления, сотрудники спецслужб, деятели рынка цифровых услуг, ученые, журналисты, правозащитники, дипломаты. Широкий общественный интерес к вопросам ИБ, включение данной проблематики в программы работы научно-исследовательских структур и вузов, как технологического, так и гуманитарного профиля, обусловил на протяжении 1990 – 2010-х гг. создание на высоком качественном уровне научно-теоретической платформы государственной политики в этой сфере, а также стимулировал формирование корпуса кадров квалифицированных специалистов в области ИБ.

Со второй половины 1990-х–2000-е гг. процесс информатизации России определяется интенсификацией развития Интернета в бизнесе, государственном управлении и повседневной жизни, причем экспертные структуры и сетевые сообщества все более активно участвуют в теоретической и технологической разработке проблем защиты информации, выступают как участники формирования государственной политики России в области информационной безопасности.

В XXI в. эта сфера стала органичной частью государственной политики, а ее значимость в общей стратегии развития страны постоянно возрастала.

Важнейшими характеристиками развития государственной политики Российской Федерации в сфере информационной безопасности в XXI веке явились: во-первых, становление стратегических, программно-целевых подходов; во-вторых, утверждение практики совместного участия государственных и общественных, в том числе сетевых институтов в формировании и реализации государственных программ.

На протяжении всего рассматриваемого периода важную роль в формировании государственной политики в сфере ИБ играет Совет Безопасности РФ во главе с Президентом России, а специалисты его аппарата с середины 1990-х гг. выступают в качестве авторов концептуальных научных работ по проблемам безопасности в информационной сфере России.

В 2000-е - 2010-е гг. вопросы информационной безопасности гг. заняли важное место во внешней политике России, которая совместно со странами СНГ выступила инициатором разработки новых принципов обеспечения глобальной информационной безопасности в формате ООН. Российское руководство последовательно поддерживает политику взаимных гарантий и обмена опытом в области информационной безопасности в таких международных объединениях как СНГ, Союзное государство России и Беларуси, Организация Договора коллективной безопасности, Шанхайская организация сотрудничества.

Современная государственная политика информационной безопасности Российской Федерации определяется развитием информационных технологий и сетевых коммуникаций, интеграцией страны в глобальное информационное пространство. Массовое распространение Интернета и программы цифровизации государственного управления потребовали модернизации законодательства, технических регламентов и стандартов банковской деятельности, связанных с задачами информационной защиты служебной и банковской тайны, противодействия киберпреступности и других задач в сфере общественной информационной безопасности. Во второй половине 2010-х гг. в условиях сложной геополитической обстановки, когда нарастают противоречия между Россией и коллективным Западом, российское информационное пространство подверглось как массированному политико-идеологическому воздействию, в том числе внедрению в сетевые сообщества фейков, пропаганды деструктивных моделей социального поведения и т.п., так и технологическому – кибератаки на банки, сайты ведущих СМИ, государственных учреждений и т.п.

В этот период руководство страны уделяет серьезное внимание вопросам обеспечения национальной безопасности, в том числе защиты от внешних информационных и «гибридных» угроз, в обеспечении которой принимают участие как государственные системы безопасности, так и ведущие цифровые компании, экспертные группы, общественные организации.

Важным компонентом государственной политики обеспечения информационной безопасности России стали программы формирования исторического сознания и патриотизма среди молодежи, борьба с фальсификациями истории, прежде всего истории Великой Отечественной войны 1941–1945 гг.

Таким образом, исторический опыт и реализация государственной политики Российской Федерации в области информационной безопасности является существенным компонентом модернизационного транзита страны в период 1991–2021 гг. и одной из наиболее актуальных составляющих платформы стратегического развития страны в XXI в.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Источники

Архивные

1. Российский государственный архив социально-политической документации (РГАСПИ):

Ф. 17. (ЦК КПСС) Оп. 158. Д. 88.

Ф. 17. Оп. 158. Д. 88. Д. 93.

Ф. 17. Оп. 158. Д. 88. Д. 572.

Ф. 17. Оп. 158. Д. 88. Д.1099.

Ф. 17. Оп. 158. Д. 88. Д.1164.

Ф. 17. Оп. 158. Д. 88. Д. 1170.

Ф. 17 Оп. 159.Д. 90.

Ф. 17 Оп. 159.Д. 91.

2. Архив Президента Российской Федерации (оцифрованные документы)

Ф. 6. Коллекция документов Б.Н. Ельцина (личный фонд). Оп. 1. Д. 88.

Ф. 6. Оп. 1. Д. 111.

Ф. 6. Оп. 1. Д. 113.

Законодательно-нормативные документы

3. Государственная программа Информационное общество (2011-2020 г.). Постановление Правительства РФ № 313 от 15.04.2014 // СЗ РФ, 2014, № 18, ч. II, ст. 2159

4. Доктрина информационной безопасности Российской Федерации от 09.09.2000 № Пр-1895 [Электронный ресурс] // Информационно-правовая система «Гарант». URL: https://base.garant.ru/182535/ (Дата обращения: 12.05.2019).

5. Закон Российской Федерации от 4 июля 1996 г. № 85-ФЗ. Об участии в международном информационном обмене // СЗ РФ, 1996, № 28, ст. 3347.

6. Закон РФ от 21 июля 1993 г. № 5485-I «О государственной тайне» // Российская газета. 21 сентября 1993 г. № 183 (799). С.1.

7. Закон РФ от 23 сентября 1992 г. № 3523-1 «О правовой охране программ для ЭВМ и баз данных» // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ, 1992, № 42, ст. 2325.

8. Закон РФ от 27 декабря 1991 г. № 2124-I «О средствах массовой информации» // Ведомости Съезда народных депутатов СССР и Верховного Совета СССР, 1992. № 7, ст. 300.

9. Закон СССР от 12 июня 1990 г. № 1552-1: «О печати и других средствах массовой информации» // Ведомости СНД и ВС СССР, 1990, № 26, ст. 492

10. Конституция Российской Федерации [Принята всенародным голосованием 12 декабря 1993 г.]. М.: Юридическая литература, 1993. 63 с.

11. Модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры». Принят Постановлением МПА СНГ от 28 ноября 2014 г. № 41-14 [Электронный ресурс] // Информационно-правовая система «Гарант». URL: https://base.garant.ru/71871816/ (Дата обращения: 20.04.2022)

12. Модельный закон «Об информатизации, информации и защите информации». Принят на 26 Пленарном заседании МПА СНГ. Постановление от 18 ноября 2005 г. № 26-7 [Электронный ресурс] // Электронный фонд правовых и нормативно-технических документов «Кодекс» URL: https://docs.cntd.ru/document/901972159 (Дата обращения: 20.04.2022)

13. Национальный стандарт РФ ГОСТ Р.50922-2006 «Защита информации Основные термины и определения» [Электронный ресурс] //. Информационно-правовая система «Гарант». URL: https://base.garant.ru/193664/ (дата обращения: 12.05.2019).

14. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020

года. Утверждены Президентом Российской Федерации В.В.Путиным 24 июля 2013 г., № Пр-1753. [Электронный ресурс]. // Сайт Института проблем информационной безопасности. URL: https:////www.iisi.msu.ru/Docs/article43/

15. Положение о Совете Безопасности Российской Федерации: утверждено Указом Президента Российской Федерации от 3 июня 1992 г. № 547 // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1992, № 24, ст. 1323.

16. Постановление Верховного Совета РСФСР от 22.11.1991 № 1920-I «О Декларации прав и свобод человека и гражданина» // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР от 01.01.1991, № 52, стр.1865.

17. Постановление Правительства России от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [Электронный ресурс] URL: https://static.government.ru/media/files/uPA03V4BfqknJWNExcfX3gSlDZi4zuas.pdf (Дата обращения: 26.01.2022)

18. Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» [Электронный ресурс] // Информационно-правовая система «Гарант». URL: https://www.garant.ru/products/ipo/prime/doc/12092469/ (Дата обращения: 21.11.2021)

19. Постановление Правительства РФ от 26.06.1995 г. № 608 «О сертификации средств защиты информации» // СЗ РФ 1995, N 27, ст. 2579; 1996, № 18, ст. 2142.

20. Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] // Электронный фонд правовых и нормативно-технических документов «Кодекс». URL: https://docs.cntd.ru/document/902289626 (Дата обращения: 20.04.2022)

21. Стратегия развития информационного общества в Российской Федерации. 7 февраля 2008 г. № Пр-212. URL: https://digital.gov.ru/uploaded/files/strategiya_razvitiya_inf_obschestva_1.pdf

22. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. (Утверждены приказом ФСТЭК России от 25 декабря 2017 г. №239). СПб.: Стаун-кантри, 2017. 34 с.

23. Указ Президента РФ В.В. Путина от 11 августа 2003 № 960 «Вопросы Федеральной службы безопасности Российской Федерации» (в ред. 21.06.2021). [Электронный ресурс] URL: https://legalacts.ru/doc/ukaz-prezidenta-rf-ot-11082003-n-960/ (Дата обращения: 15.01.2022)

24. Указ Президента РФ от 03 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации // СЗ РФ, 1995, № 15, ст. 1285.

25. Указ Президента РФ от 11 сентября 1991 г. «О мерах по защите свободы печати в РСФСР» [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/acts/bank/185

26. Указ Президента РФ от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской

Федерации» (с изменениями и дополнениями) [Электронный ресурс] // Информационно-правовая система «Гарант». URL: https://base.garant.ru/70299068/

27. Указ Президента РФ от 17.03.2008 № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»

28. Указ Президента РФ от 17.12.1997 г. № 1300 «Об утверждении Концепции национальной безопасности Российской Федерации (в ред. от 10.01.2000 г. № 24) // СЗ РФ. 1997, № 52, ст. 5909

29. Указ Президента РФ от 5 декабря 2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ Российской Федерации. 2016. № 50. Ст. 7074

30. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901

31. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности // СЗ РФ, 1995, № 33, ст.3349.

32. Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» // СЗ РФ, 1995, № 8, ст. 609.

33. Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях».

34. Федеральный закон от 26 июля .2017 г. № 187-ФЗ. «О безопасности критической информационной инфраструктуры Российской Федерации»

35. Федеральный закон от 5 марта 1992 года № 2646-1 «О безопасности // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ, 1992, № 15, ст. 769

36. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // СЗ РФ, 2006, № 31.

Тематические сборники документов

37. История советской политической цензуры. Документы и комментарии / Сост. Горяева Т. М. – М.: РОССПЭН, 1997. – 672 с.

38. Международная информационная безопасность: Теория и практика: В 3-х т. Т. 2: Сборник документов (на русском языке) / Под общ. ред. А.В. Крутских. 2-е изд., доп. – Москва: Аспект Пресс, 2021. – 784 с.

39. План Президента Путина: руководство для будущих президентов России: (комментированный сборник президентских посланий Федеральному Собранию РФ, 2000-2007 гг.) / Павловский Г.О, Чадаев А.В., Шпунт А. В. – М.: Европа, 2007. – 392 с.

40.Российская журналистика: свобода доступа к информации / Комиссия по свободе доступа к информации [Сост. И. Дзялошинский]. – М.: КСДИ, 1996. – 267 с.

Делопроизводственные документы

41.Выписка из «Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Совет Безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/2301/ (Дата обращения: 15.04.2022)

42.Заседание коллегии ФСБ России. 24 февраля 2021 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: http://www.kremlin.ru/events/president/news/65068 (Дата обращения: 20.04.2022)

43. Заседание Совета Безопасности РФ «О защите информационной инфраструктуры государства и мерах по её развитию». 26 октября 2017 г. [Электронный ресурс] // Совет Безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/2301/ (Дата обращения: 15.04.2022)

44. Заседание Совета Безопасности РФ «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства». 20 мая 2022 г. [Электронный ресурс] // Совет Безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/3241/ (Дата обращения: 23.05.2022)

45. Заседание Совета Безопасности РФ «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства». 20 мая 2022 г. [Электронный ресурс] // Совет Безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/3241/ (Дата обращения: 23.05.2022)

46. Заседание Совета Безопасности РФ «О противодействии угрозам национальной безопасности в информационной сфере». 1 октября 2014 г. [Электронный ресурс] // Совет безопасности РФ. Официальный сайт. URL: https://www.scrf.gov.ru/council/session/2059/ (Дата обращения: 15.04.2022).

47. Заседание Совета безопасности РФ «О создании современных систем связи для нужд обороны и безопасности страны, поддержания правопорядка». 1 октября 2010 г. [Электронный ресурс] // Совет безопасности РФ. URL: Официальный сайт. https://www.scrf.gov.ru/council/session/2048/ (Дата обращения: 15.04.2022)

48. Защита персональных данных при предоставлении госуслуг. [Электронный ресурс] // Управление МВД России. 30 Октября 2016 г. https://40.xn--b1aew.xn--p1ai/news/item/8822881 (Дата обращения: 21.11.2021)

49. Парламентские слушания «Средства массовой информации в системе информационной безопасности» // Думский вестник. 1996. № 5 (20). С. 90-103.

50. Перечень межведомственных рабочих групп по основным направлениям реализации «Стратегии информационного общества в Российской Федерации» // Информационное общество. 2009. № 4-5. С. 24-31.

51. Протокол № 34 заседания Совета Государственной Думы РФ от 04.07.96 г. «О проведении 16 июля 1996 года (вторник) парламентских

слушаний «Угрозы и вызовы в сфере информационной безопасности Российской Федерации» Электронный ресурс. URL: Сайт Системы обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (Далее: СОЗД). URL; https://sozd.duma.gov.ru/events_document/43C5456B-9E8B-49CB-BD0E-69F6723699DD/1996 (Дата обращения: 15.04.2022)

52. Расширенное заседание Коллегии Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 21 декабря 2012 г. № 8. [Электронный ресурс] // Сайт Роскомнадзора. URL: https://rkn.gov.ru/about/p403/p677/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (Дата обращения: 20.04.2022)

53. Стенографический отчет о заседании Совета по развитию информационного общества. 12 февраля 2009 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/events/president/transcripts/3161 (Дата обращения: 21.11.2021)

Публицистические документы

54. Вступительное слово Президента России В.В. Путина на заседании Совета Безопасности РФ 26 марта 2021 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.scrf.gov.ru/news/speeches/2952/

55. Вступительное слово Президента России В.В. Путина на заседании Совета Безопасности РФ 26 марта 2021 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.scrf.gov.ru/news/speeches/2952/

56. Вступительное слово Президента России В.В. Путина на заседании Совета Безопасности России «О противодействии угрозам национальной безопасности в информационной сфере». 1 октября 2014 г. [Электронный ресурс] // Совет безопасности РФ. Официальный сайт. URL: https://scrf.gov.ru/council/session/2059/

57. Вступительное слово Президента России В.В. Путина на заседании Совета Безопасности по вопросу об обеспечении национальной безопасности в сфере нераспространения оружия массового уничтожения и средств его доставки. Москва, 3 декабря 2003 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.kremlin.ru/events/president/transcripts/22237 (Дата обращения: 26.01.2022)

58. Путин В.В. Вступительное слово на заседании Совета безопасности по вопросу развития информационного общества в России. Москва, Кремль, 25 июля 2007 года [Электронный ресурс] // Президент России. Официальный сайт. URL: https://www.special.kremlin.ru/events/president/transcripts/24432 (Дата обращения: 20.11.2021).

59. Выступление Секретаря Совета Безопасности Российской Федерации Н.П. Патрушева на открытии XVII Совещания руководителей органов безопасности и разведывательных служб государств-участников СНГ по вопросам разведывательной деятельности [Электронный ресурс] // Совет Безопасности РФ. Официальный сайт. 13 октября 2021 г. URL: https://www.scrf.gov.ru/news/speeches/3098/ (Дата обращения: 19.04.2022)

60. Гостехкомиссия России стала ФСТЭК России. Что изменила реформа? [Интервью с С.И. Григоровым] // Системы безопасности. 2005. № 1. URL: https://secuteck.ru/articles2/oficial/gostehkom_stala_fstek (Дата обращения: 26.01.2022)

61. Государство Россия. Путь к эффективному государству (О положении в стране и основных направлениях внутренней и внешней политики государства): Послание Президента России В.В. Путина Федеральному Собранию Российской Федерации. 8 июля 2000 г. // Президент России. Официальный сайт. URL: https://www.kremlin.ru/acts/bank/22401 (Дата обращения: 20.11.2021).

62. Иванова Е. Хакеры пошли простым путем [Электронный ресурс] // Сайт Радио «Ъ FM». 14 июня 2017 г. URL: https://www.kommersant.ru/doc/3325386 (Дата обращения: 18.04.2022).

63. Интервью с экспертами [Электронный ресурс] // Электронное издание Anti-Malware.ru. URL: https://www.anti-malware.ru/interviews (Дата обращения: 17.02.2022)

64. Интервью Секретаря Совета Безопасности Российской Федерации Н.П. Патрушева // Российская газета. Федеральный выпуск. – 23 декабря 2015 г. – № 6861. – С.4.

65. Инфофорум-2009. [Электронный ресурс]. // CNews: Интернет издание о высоких технологиях. 5 февраля 2009 г. URL: https://www.cnews.ru/articles/infoforum_2009_anonimnost_pugaet_chinovnikov/2 (Дата обращения: 22.11.2021)

66. Кафедра ИБ: как и чему учат тех, кто предотвращает утечки информации: Интервью с профессором А.В. Душкиным [Электронный ресурс] // Сайт НИУ «МИЭТ». 27 июля 2020 г. URL: https://www.miet.ru/news/128216(Дата обращения 15.02.2022)

67. Кодекс профессиональной этики российского журналиста Союза журналистов России. Принят Конгрессом журналистов России 23 июня 1994 г. [Электронный ресурс] // Официальный сайт Союза журналистов России. URL: https://www.ruj.ru (Дата обращения: 16.02.2022)

68. Манифест Международного союза интернет-деятелей ЕЖЕ. 25 октября 2003 года [Электронный ресурс] // Сайт Союза ЕЖЕ URL: https://ezhe.ru/manifest_text.html (Дата обращения: 20.11.2021).

69. Направления прорыва. Из руин – к информационному обществу // Российская газета. 10 января 1991 г. с.1.

70. Нарышкин С.Е. Об обеспечении национальной безопасности и устойчивого социально-экономического развития государств в условиях роста «гибридных» угроз: Выступление на 10-й международной встрече высоких представителей, курирующих вопросы безопасности, на тему «»,

Уфа, 18 июня 2019 г. // МИД России. Официальный сайт. 28 июня 2019 г. URL: https://www.mid.ru/foreign_policy/international_safety/regprla/-/asset_publisher/YCxLFJnKuD1W/content/id/3704728 (Дата обращения: 23.11.2021)

71. Поздравление Президента России В.В. Путина с Днем работника российских спецслужб 20 декабря 2020 г. [Электронный ресурс] // Президент России. Официальный сайт. URL: http://www.kremlin.ru/events/president/news/64681 (Дата обращения: 18.04.2022).

72. Пресс-конференция Qrator Labs и Positive Technologies: Главные тренды и итоги 2019 года в области кибератак и сетевой безопасности. Публикации в СМИ. [Электронный ресурс] // Сайт Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/about/press/events/304630/ (Дата обращения: 17.04.2022)

73. Рубанов В.А. От культа секретности к информационной культуре // Коммунист. 1988. № 13. С. 24-36.

74. Сергей Степашин – о выступлении Владимира Путина на коллегии ФСБ (Беседовал А. Гамов) [Электронный ресурс] // Комсомольская правда. 24 февраля 2021 г. URL: https://www.kp.ru/daily/27244/4372832/ (Дата обращения: 19.04.2022)

75. Совместное заявление Президента Российской Федерации В.В. Путина и Президента Республики Узбекистан Ш.М. Мирзиёева о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] // Президент России. Официальный сайт. 19 ноября 2021 г. URL: https://www.kremlin.ru/supplement/5739 (Дата обращения: 20.04.2022)

76. Страны БРИКС осудили акты массовой электронной слежки и сбора данных о людях по всему миру [Электронный ресурс] // ТАСС. 9 июля 2015 г. URL: https://tass.ru/politika/2107335 (Дата обращения: 20.04.2022)

77. Тумакова А. Инфофорум 2022: диалог о будущем цифровой безопасности и сегодняшней работе в этом направлении // Инфокоммуникации онлайн: сетевое издание. 8 февраля 2022 г. https://ict-online.ru/news/n206503/ (Дата обращения: 19.04.2022)

78. Турченко С. В опасности ... безопасность // Советская Россия. – 18 марта 1993 г.

79. Хартия обязанностей и прав журналистов [Электронный ресурс] // Сайт профсоюза журналистов и работников СМИ. URL: https://profjur.org/hartija-objazannostej-i-prav-zhurnalistov/ (Дата обращения: 16.02.2022)

Мемуары

80. Ельцин Б.Н. Президентский марафон: Размышления, воспоминания, впечатления / Борис Ельцин. М.: АСТ, 2000. 426 с.

81. Исаков В.Б. Председатель Совета Республики. Парламентские дневники. 1990-1991 / Владимир Исаков. Екатеринбург: Уральский рабочий, 1997. 491 с.

82. IT в «лихие 90е» – из воспоминаний бумера [Электронный ресурс] URL: https://habr.com/ru/post/541160/ (Дата обращения: 25.01.2022).

83. Как в СССР продвигали компьютерную грамотность. Микроша и Агат [Электронный ресурс] URL: https://zxdemos.ru/viewtopic.php?id=10997 (Дата обращения: 15.11.2021)

84. Нечаев А. Россия на переломе. Записки первого министра экономики / Андрей Нечаев. – Москва: Русь-Олимп, 2010. – 585 с.

85. «Потерянные ребята» из IT: история программиста из 90-х. [Электронный ресурс] URL: https://techrocks.ru/2020/10/12/programmer-from-90s-it-history/ (Дата обращения: 25.01.2022).

86. Соколова С. История соцсетей, рассказанная пионером Рунета [Электронный ресурс] // Архив RB.ru. 23 апреля 2014 г. URL:

https://rb.ru/article/istoriya-sotssetey-rasskazannaya-pionerom-runeta/7323287.html (Дата обращения: 20.11.2021)

87. «Это было лучшее время»: каким был интернет в России 90-х [Электронный ресурс] // Lenta.ru. 24 октября 2020 г. URL: https://lenta.ru/articles/2020/10/14/beeline_90e/

Справочные и информационные издания

88. База данных ГОСТ [Электронный ресурс] // Росстандарт. Центр сертификации. URL: https://rosstandart.msk.ru/gost/001.001.040.001/gost-r-50922-96/

89. Закрытые города СССР (ЗАТО) и их судьба в РФ [Электронный ресурс]. URL: https://leon-rumata.livejournal.com/3868057.html (Дата обращения: 25.11.2021)

90. Космические разведчики. Советские и российские спутники – шпионы [Электронный ресурс] // Военное обозрение. 8 января 2014 г. URL: https://topwar.ru/37962-kosmicheskie-razvedchikisovetskie-i-rossiyskie-sputniki-shpiony.html (Дата обращения: 20.11.2021)

91. Министры связи РФ с 1990 года. Досье ТАСС [Электронный ресурс] // ТАСС. 18 мая 2018 г. URL: https://tass.ru/info/5214397 (Дата обращения: 20.11. 2021).

92. Наукограды. История развития [Электронный ресурс] // Сайт Союза развития наукоградов. URL: https://naukograds.ru/ (Дата обращения: 20.11.2021)

93. Образование. Направления и специальности. [Электронный ресурс] // Свйт ИТМО. URL: https://itmo.ru/ru/page/169/obrazovanie.htm(Дата обращения 15.02.2022)

94. Тематический сборник «Информационные технологии, связь и защита информации МВД России»-2017. С.5 [Электронный ресурс] // МВД России. Официальный сайт. URL: https://мвд.рф/mvd/structure1/Departamenti/

Departament_informacionnih_tehnologij_sv/informacionnie-tehnologii-sbornik (Дата обращения: 26.01.2022)

95. Технологии защиты информации. О профессии [Электронный ресурс] // Сайт РУДН. URL: https://www.rudn.ru/education/educational-programs/53816 (Дата обращения 15.02.2022)

96. Шифровальная служба СССР / России в годы войны и послевоенный период [Электронный ресурс] // Призма. Армия и ВПК. URL: https://prizmablog.ru/shifrsluzhba-sssr-rossii-ch2/ (Дата обращения: 12.11.2021)

97. Шифровальные машины СССР 1931-1991 гг. (Обзор) [Электронный ресурс] // Призма. Армия и ВПК. URL: https://prizmablog.ru/shifrovalnye-mashiny-sssr-1931-1991-gg-obzor/; Криптология в Холодной войне // Призма. Армия и ВПК. URL: https://prizmablog.ru/kriptologiya-v-holodnoj-vojne/ (Дата обращения: 12.11.2021)

ЛИТЕРАТУРА

На русском языке

1. Абакумов Е.М. В век высоких технологий: к юбилею отделения информационных технологий и информационной безопасности ФГУП «ВНИИА» / Е.М. Абакумов, Н.О. Кожевников, С.А. Петунин; под ред. Ю.Н. Бармакова. Всероссийский научно-исследовательский институт автоматики им. Н. Л. Духова. М.: Кодекс, 2016. 204 с.

2. Авсентьев О.С. Системные аспекты проблематики подготовки специалистов в области информационной безопасности / О.С. Авсентьев, В.Н. Прийма, А.А. Малышев, А.П. Дураковский Системные аспекты проблематики подготовки специалистов в области информационной безопасности // Информационная безопасность. 2009. № 4. С. 621-622.

3. Алексеева Е.В. Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной

безопасности в информационной сфере / Е.В. Алексеева // Ленинградский юридический журнал. – 2016. – № 4(46). – С. 97-103.

4. Артамонов Г.Т. О государственной политике информатизации / Г.Т. Артамонов, А.С. Голубков, Д.С. Черешкин // Вестник Российского общества информатики и вычислительной техники. 1994. № 4-5. С.67.

5. Арутюнов В.В. Об итогах третьей международной научно-практической конференции «Информационная безопасность: вчера, сегодня, завтра» / В.В. Арутюнов // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2020. № 7. С. 38-41.

6. Арутюнов В.В. Об итогах IV Международной научно-практической конференции «Информационная безопасность: вчера, сегодня, завтра» // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2021. № 7. С. 37-40.

7. Арутюнов В.В. О результативности работ российских исследователей - лидеров научной деятельности в области информационной безопасности / В.В. Арутюнов, Н.В. Гришина // Информационная безопасность: вчера, сегодня, завтра: Сборник статей по материалам V Международной научно-практической конференции, Москва, 14 апреля 2022 года. – Москва: Российский государственный гуманитарный университет, 2022. – С. 103-110.

8. Астахова Л.В. Развитие управленческой компетенции будущего специалиста по защите информации в вузе / Л.В. Астахова // Современные проблемы науки и образования. 2012. № 6. С. 330-336.

9. Ахмадиев Ф.В. Свобода слова и ответственность журналиста // Вестник Башкирского университета. 2011. Т. 16. – № 2. С. 529-530.

10. Бабаш А.В. Информационная безопасность. История защиты информации в России / А.В. Бабаш, Е.К. Баранова, Д.А. Ларин. М.: Изд. центр ЕАОИ, 2012. 736 с.

11. Багдасарян В. Э. «Информационная война»: научиться мыслить в парадигме войн нового типа // Блог Багдасаряна. 5 июля 2013.

http://vbagdasaryan.ru/informatsionnaya-voyna-nauchitsya-myislitv-paradigme-voyn-novogo-tipa/(дата обращения: 20.04.2022).

12. Багдасарян В.Э. Великая Отечественная война в фокусе информационно-психологической войны против России // Вестник МГОУ. Серия: История и политические науки. 2015. № 2. С. 25-35.

13. Багдасарян В.Э. Информационные факторы формирования исторического сознания молодежи (на примере изучения представлений о Великой Отечественной войне) / В.Э. Багдасарян, А.Э. Ларионов, С.И. Ряснянский // Вопросы истории. 2022. № 8-1. С. 34-49.

14. Багдасарян В.Э. Перспективы развития искусственного интеллекта в актуальной повестке политических и социальных рисков глобальных трансформаций / В.Э. Багдасарян, П.П. Балдин // Журнал политических исследований. 2020. Т. 4, № 2. С. 10-22.

15. Бакаева О.Ю. Государственный контроль в сфере защиты государственной тайны: актуальные вопросы правового регулирования / О.Ю. Бакаева // Информационная безопасность регионов. 2013. № 1 (12). С.93-97.

16. Балашова М.А. Информационное общество: теоретическая база и российская практика / М.А. Балашова // Известия Иркутской государственной экономической академии. 2013. № 5. С. 5-12.

17. Баранов А.П. Проблемы обеспечения информационной безопасности в информационно-телекоммуникационной системе специального назначения и пути их решения // Информационное общество. 1997. Вып. 1. С. 13-17.

18. Безбородов А.Б., Материалы по истории диссидентского и правозащитного движения в СССР 50-х – 80-х годов / А.Б. Безбородов, М.М. Мейер, Е.И. Пивовар. М.: Историко-архивный институт 1994. 151 с.

19. Безопасность государства и развитие науки, техники, промышленности России (СССР) во второй половине XX в.: вопросы

истории и политики: монография / А.В. Лосик и др.; под ред. В.Н. Скворцова. СПб: Ленинградский гос. ун-т им. А. С. Пушкина (ЛГУ), 2012. 275 с.

20. Блохин В.В. Фальсификация истории Великой Отечественной войны и русофобия в современном политическом контексте либеральных историках, свободе мнений и адвокатах гитлеризма (современные фальсификаторы Великой Отечественной войны против России) / В.В. Блохин // Вестник МНЭПУ. 2021. № 2. С. 179-185.

21. Блохин В.В. «Холодная война» в историческом сознании: фальсификация Великой Отечественной войны в работах Б.В. Соколова / В. В. Блохин // Патриотическое воспитание в системе высшего образования: Материалы Всероссийской научно-практической конференции с международным участием, посвященной 75-летию начала контрнаступления советских войск в битве под Москвой, Москва, 01–02 декабря 2016 года / Ответственный редактор З.З. Мухина. М.: Национальный исследовательский технологический университет «МИСиС», 2017. С. 12-20.

22. Бодрова Е. В., Калинов В. В. Эволюция концептуальных основ научно-технической политики РФ в условиях становления новой государственности (1992-1993 гг.) // История: факты и символы. – 2019. – № 1(18). – С. 151- 164.

23. Бодрова Е. В., Калинов В. В. Реформирование высшего технического образования в РФ в контексте "индустриальной революции 4.0": спорные проблемы // Право и образование. – 2021. – № 11. – С. 27- 38.

24. Бойко С.М. Проблематика международной информационной безопасности на площадках ШОС и БРИКС / С.М. Бойко // Международная жизнь. 2019. № 1. С. 1-22.

25. Бондуровский В.В. Парламентское измерение информационной безопасности в рамках СНГ и ОДКБ на современном этапе / В.В. Бондуровский, И.Л. Бачило, М.А. Вус, М.М. Кучерявый, О.С. Макаров // Информатизация и связь. 2014, № 3. С. 8-13.

26. Брюхомицкий Ю.А. Обзор исследований и разработок по информационной безопасности / Ю. А. Брюхомицкий, О.Б. Макаревич // Известия ЮФУ. Технические науки. 2012. № 12(137). С. 8-21.

27. Бурькова Е. В. Профессиональная подготовка специалистов в области информационной безопасности / Е.В. Бурькова // Вестник Оренбургского государственного университета. 2016. № 2(190). С. 3-9.

28. Василенко И. Информационная война как фактор мировой политики / И. Василенко // Государственная служба. – 2009. – № 3(59). – С. 80-86.

29. Верютин В.Н. Межведомственная комиссия по защите государственной тайны: структура и компетенция / В.Н. Верютин // Вестник Воронежского института МВД России. 2010. № 2. С.22-26.

30. Верютин В.Н. Отдельные аспекты защиты государственной тайны в Российской Федерации / В.Н. Верютин // Вестник Воронежского института МВД России. 2009. № 2. С. 17-22.

31. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / В.Б. Вехов. М.: Право и Закон, 1996. 182 с.

32. Власенко, И.С. Информационная война: искажение реальности / И.С. Власенко, М.В. Кирьянов. М.: ИД «Канцлер», 2011. 196 с.

33. Возможна ли безопасность в информационном обществе? Круглый стол, посвященный 10-летию Закона Российской Федерации «О государственной тайне» [Электронный ресурс] // Санкт-Петербургский университет. 28 ноября 2003 г. № 27 (3652). URL: http://old.journal.spbu.ru/2003/27/3.shtml (Дата обращения: 22.11.2021)

34. Волгин Е.И. Политическая трансформация КПСС (1990-1991 гг.) / Е.И. Волгин // Вестник Московского университета. Серия 12: Политические науки. 2006. № 6. С.26-27.

35. Володенков С.В. Флэшмоб как сетевая технология современного политического менеджмента (на примере России и США) / С.В. Володенков,

С.Н. Федорченко // Вестник Московского государственного областного университета. 2015. № 3. С. 18.

36. Волокитин А.В. Россия: от информатизации – к информационному обществу / А.В. Волокитин, Б.В. Кристальный, С.Д. Черешкин // Информационное общество. 1999. № 3. С. 12-15.

37. Воронцов, С.А. Правоохранительные органы. Спецслужбы. История и современность. Учебное пособие / С.А. Воронцов. – Ростов-на-Дону: Феникс, 1998. 117 с.

38. Вус М.А. Четверть века законодательного регулирования института государственной тайны на постсоветском пространстве / М.А. Вус, О.С. Макаров // Новый юридический вестник. 2017. № 2 (2). С. 1-7.

39. Вус, М.А., Гусев В.С. Государственная тайна – правовой институт суверенного государства / М.А. Вус, В.С. Гусев // Конфидент. 1996. № 1. С. 130-135.

40. Вус М.А., Макаров О.С. Стратегический вектор обеспечения международной информационной безопасности на пространстве СНГ / М.А. Вус, О.С. Макаров // Юридические науки: проблемы и перспективы: материалы V Международной научной конференции (г. Казань, октябрь 2016 г.). Казань: Бук, 2016. С. 40-43.

41. Герасименко В.Г. О проблеме информационной безопасности в банках России: потери, прогноз развития и некоторые пути решения / В.Г. Герасименко, В.В. Сергеев // Вопросы защиты информации. 1996. № 2. С. 52-56.

42. Горяева Т.М. Политическая цензура в период стагнации и кризиса власти и идеологии в СССР (1969–1991 гг.) / Т.М. Горяева // Политическая цензура в СССР. 1917-1991. М.: РОССПЭН, 2009.

43. Государственная политика Российской Федерации в области развития информационного общества / А.В. Коротков, Б.В. Кристальный, И.Н. Курносов; под науч. ред. А.В. Короткова. – М.: Трейн, 2007. 469 с.

44. Государственная тайна и ее защита в Российской Федерации / П.П. Аникин, А.Л. Балыбердин, М.А. Вус, В.С. Гусев, В.Н. Рябчук, А.В. Федоров; под общ. ред. М.А.Вуса и А.В. Федорова. СПб: Юрид. центр Пресс, 2003. 610 с.

45. Давтян С.Л Изменения Закона РФ «О средствах массовой информации» в 1991-2010 гг.: факты как история / С.Л. Давтян // Вестник Московского университета. Серия 10. Журналистика. 2011. № 3. С.12-128.

46. Дзанагова М. К. Деятельность государственных органов по защите государственной тайны /М. К. Дзанагова, М.М. Бетеева // Право и государство: теория и практика. 2021. № 4(196). С. 316-317.

47. Дзялошинский И.М. Медиапространство России: коммуникационные стратегии социальных институтов / И.М. Дзялошинский. М.: Изд-во АПК и ППРО, 2013. 479 с.

48. Евтюшкин А.В. Сотрудничество государства, бизнеса, гражданского общества и научно-образовательного сообщества в подготовке и реализации национальной стратегии перехода России к информационному обществу / А.В. Евтюшкин, Т.В. Ершова, А.В. Коротков, Ю.Е. Хохлов // Информационное общество. 2002. Вып. 1. С. 47-51.

49. Емельянов Г.В. Проблемы обеспечения безопасности информационного общества / Г.В. Емельянов, А.А. Стрельцов // Информационное общество. 1999. № 2. С.15-16.

50. Ершов В.Ф. Модернизационный этап развития банковской сферы России в контексте процессов глобализации / В.Ф. Ершов // Наука и бизнес: пути развития. 2019. № 7 (97). С. 171-176.

51. Есипов В.А. Реформы органов госбезопасности в России и государствах бывшего СССР в 1990-е годы и мировая система их организации / В.А. Есипов // Образование и наука в России и за рубежом. 2019. № 2. С.444-446.

52. Жданчиков П.А. Итоги и перспективы региональной информатизации / П.А. Жданчиков // Региональная экономика: теория и практика. 2018. Т. 16. № 11. С. 2015-203

53. Згадзай О.Э. Вопросы подготовки специалистов в области информационной безопасности / О.Э. Згадзай // Вестник Казанского юридического института МВД России. – 2013. – № 3(13). – С. 93-97.

54. Зеленов М.В. Военная и государственная тайна в РСФСР и СССР и их правовое обеспечение (1917 – 1991 гг.) / М.В. Зеленов // Ленинградский юридический журнал. 2012. Вып. 1. С. 144.

55. Игнатенко, Ю.М., Кикнадзе В.Г На страже радиоэфира // Военно-исторический журнал. 2007. № 9. С.31-35.

56. Интеллектуальные системы в информационном противоборстве: сборник научных трудов Российской научной конференции, Москва, 15–17 декабря 2017 года. Под ред. Ю.Ф Тельнова и др. М.: Российский экономический университет имени Г.В. Плеханова, 2018. Т.1. 446 с.

57. Информационно-коммуникационные технологии третьего тысячелетия / П. В. Меньшиков, Е. Е. Юсупова, В. С. Новикова [и др.]. М.: Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, 2020. 460 с.

58. Информационные вызовы национальной международной безопасности / И.Ю. Алексеева, И.В. Авчаров, А.В. Бедрицкий [и др.]; под общ. ред. А.В. Федорова и В.Н. Цыгичко. М.: ПИР Центр политических исследований, 2001. 327 с.

59. История современной России. Десятилетие либеральных реформ. 1991-1999 гг. / Р.Г. Пихоя, С.В. Журавлев, А.К. Соколов. – М.: Новый хронограф, 2020. 312 с.

60. Кемпф В.А. Особенности субъективных угроз информационной безопасности информационных систем в деятельности органов внутренних

дел Российской Федерации / В.А. Кемпф // Полицейская деятельность. 2019. № 5. С. 47-52.

61. Концепция государственной информационной политики / Под общ. ред. О.А. Финько. М., 1999. 47 с.

62. Кравчук Н.Ю. Государственные информационные ресурсы Российской Федерации на современном этапе: проблемы и перспективы развития / Н.Ю. Кравчук, Д.В. Юрков // Вестник РУДН. Серия: Государственное и муниципальное управление. 2017. Т.4. № 2. С.116-129.

63. Курило А.П. О проблеме персональных данных / А.П. Курило // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 1996. № 7. С. 12-13

64. Курылев К.П. Национальные режимы регулирования сети Интернет в странах СНГ / К.П. Курылев, Н.П. Пархитько, Н. Г. Смолик // Постсоветские исследования. 2021. Т. 4. № 8. С. 705-718.

65. Курылев К.П. Культурно-гуманитарное сотрудничество государств ЕАЭС как инструмент евразийской интеграции в 2015-2021 гг. / К.П. Курылев, М.А. Шпаковская, Д. В. Станис, О. К. Петрович-Белкин // Вопросы истории. 2021. № 11-1. С. 120-126.

66. Кучерявый М.М. Роль России и евразийского региона в формировании глобального подхода к обеспечению международной информационной безопасности / М.М. Кучерявый // Евразийская интеграция: экономика, право, политика. 2012. № 12. С. 125-131.

67. Лопатин В.Н. Информационная безопасность России. Человек. Общество. Государство / В. Н. Лопатин; МВД России, Санкт-Петербургский ун-т – СПб: Университет, 2000. 424 с.

68. Лопатин В.Н. Безопасность как критерий информационного выбора / // Право и информатизация общества: Сб. науч. тр. / В. Н. Лопатин; ИНИОН РАН. Центр социальных научно-информационных исследований. Отдел правоведения; РАН. ИГП. Центр публичного права. Сектор информационного права; Отв. ред. Бачило И.Л. М., 2002.

69. Лысая Д.А. Наукограды России: история развития от научных поселений до инновационного центра «Сколково» / Д.А. Лысая // Architecture and Modern Information Technologies. 2017. №3(40). С. 178-199.

70. Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны. / А.В. Манойло, А.И. Петренко, Д.Б. Фролов. М.: Горячая линия-Телеком, 2003. 541 с.

71. Медовкина, Л.Ю. Политика Президента Российской Федерации Б.Н. Ельцина в области информационной безопасности / Л.Ю. Медовкина // Научные ведомости Белгородского государственного университета. Серия: История. Политология. – 2019. Т. 46. № 1. С.178-187.

72. Международная информационная безопасность: подходы России / А.В. Крутских, Е.С. Зиновьева, В.И. Булва и др. Центр международной информационной безопасности и научно-технологической политики МГИМО МИД России. – Москва: МГИМО (Университет), 2021: Электронная версия. URL: https://mgimo.ru/upload/2022/03/mezhdunarodnaya-informatsionnaya-bezopasnost-podkhody-rossii.pdf

73. Международная информационная безопасность: дипломатия мира / Под ред. С. А. Комова. М., 2009. 264 с.

74. Миркин, В.В. Средства связи как инструмент политической цензуры в СССР (1970-е – начало 1980-х гг.) / В.В. Миркин // Вестник Томского государственного университета. Серия: История. 2018. № 59. С. 53-59.

75. МИЭТ 50 лет. Годы, люди, события. М.: МИЭТ, 2015. 392 с.

76. Нарыков, Д.Н. Исторический аспект создания в России закрытых административно-территориальных образований / Д.Н. Нарыков // Мир науки, культуры, образования. 2012. № 1 (32).

77. Ноговицын, А.А. Информационная безопасность в системе национальной безопасности Российской Федерации / А.А. Ноговицын // Безопасность России – 2010: экспертно-аналитическое обозрение. М.: Триумфальная арка, 2009. С.46-63.

78. Овчинников, С.А. Угрозы личности, обществу и государству при внедрении информационных технологий / С.А. Овчинников, С.Е. Гришин // Информационная безопасность регионов. 2011. № 2 (9). С. 26-31.

79. Основы теории и практики интегрированных коммуникаций и медийной политики в «новой реальности» / П. В. Меньшиков, В.С. Новикова, А.А. Агрба и др. М.: МГИМО (университет) МИД Российской Федерации, 2022. 461 с.

80. Павлова Т.Ф. Доступ к архивным документам спецхранов в начале 1960-х – середине 1980-х гг. / Т.Ф. Павлова // Отечественные архивы. 2014. № 3. С. 13-26.

81. Паредес Д.С. Теория информационной конвергенции в системах как один из подходов к осмыслению государственных и социальных проблем / Д.С. Паредес, Д.В Станис // Вестник РУДН. Серия: Государственное и муниципальное управление. 2016. № 2. С. 50-62.

82. Полонский И. День ФАПСИ (1991-2003). Слово о правительственной связи [Электронный ресурс] / И Полонский // Военное обозрение. 24 декабря 2015 г. URL: https://topwar.ru/88409-den-fapsi-1991-2003-slovo-o-pravitelstvennoy-svyazi.html (Дата обращения: 19.11.2021)

83. Понька Т.И. Информационная политика и информационная безопасность КНР: развитие, подходы и реализация / Т.И. Понька, М.С. Рамич, Ю.У. // Вестник РУДН. Серия: Международные отношения. 2020. Т. 20. № 2. С. 382-394.

84. Попандопуло Д.В. Проблемы защиты государственной тайны в оперативно-разыскной деятельности / Д.В. Попандопуло. Ростов-на-Дону: Ростовский юридический институт МВД России, 2016. 132 с.

85. Право и информационное общество: Сборник научных трудов / Отв. ред. Бачило И.Л. М.: ИНИОН РАН, 2002. 234 с.

86. Проблемы безопасности информационного общества современной России / Г.Б. Прончев, В.В. Лонцов, Д.Н. Монахов, Г.А. Монахова; МГУ им.

М. В. Ломоносова, социологический факультет. Москва: Экон-Информ, 2014. 215 с.

87. Кондратьев Д. В. Проблемы сохранения цифрового культурного наследия в контексте информационной безопасности / Д. В. Кондратьев, А.Н. Ненашев, С.Т. Петров, А.А. Тарасов // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2013. № 14(115). С. 36-52.

88. Пурис А.В. Межведомственная комиссия по защите государственной тайны: структура и компетенция / А.В. Пурис // Государство, право, общество: проблемы взаимодействия: Сборник статей II Международной научно-практической конференции, Пенза, 29 апреля 2015 года / Пензенский государственный университет, Общество «Знание» России; под ред. Н.Г. Карнишиной. – Пенза: Автономная некоммерческая научно-образовательная организация «Приволжский Дом знаний», 2015. – С. 76-79.

89. Разведка США в действии. Шпионаж, тайные операции, саботаж: Сборник материалов американской печати. Пер. с англ. / [общ. ред. и предисл. Н.Н. Яковлева]. – М.: Прогресс, 1988. – 399 с.

90. Ракитов А.И. Наш путь к информационному обществу // Теория и практика общественно-научной информации / А.И. Ракитов. – М.: ИНИОН, 1989. 302 с.

91. Ракитов А.И. Новый подход к взаимосвязи истории, информации и культуры: пример России / А.И. Ракитов. // Вопросы философии. 1994. № 4. С. 14-34.

92. Ракитов А.И. Философия компьютерной революции/ А.И. Ракитов. М.: Политиздат, 1991. 287 с.

93. Рахимов К.Х. Роль Шанхайской Организации Сотрудничества в обеспечении безопасности в Центральной Азии / К.Х. Рахимов, К.П. Курылев. М.: ООО «Издательские решения», 2018. 202 с.

94. Россошанский А.В. Средства массовой информации как институт системы информационной безопасности / А.В. Россошанский // Известия Саратовского университета. Серия: Социология. Политология. 2008. Вып.1. – С. 121-125.

95. Рубанов В.А. Основные направления перестройки режимно-секретной деятельности / В.А. Рубанов // Труды НИИ «Прогноз» КГБ СССР. М., 1988. Вып. 8, № 1101. С. 6 -20.

96. Рыдченко К.Д. «Моральный кодекс» пользователя Интернет и государственная цензура киберпространства: некоторые вопросы законодательного регулирования / К.Д. Рыдченко // Мониторинг правоприменения. 2012. № 3. С. 40-44.

97. Северин В.А. Коммерческая тайна в России / В.А. Северин. М.: Зерцало-М, 2009. 614 с.

98. Смирнов А.В. Современные информационные технологии в международных отношениях / А.В. Смирнов. – М., МГИМО-Университет, 2017. 334 с.

99. Смолькова И.Ю. Актуальные проблемы охраняемых федеральным законом тайн в российском уголовном судопроизводстве / И.Ю. Смолькова. – М.: Юрлитинформ, 2014.

100. Смолян Г.Л., Черешкин Д.С. Двадцать лет спустя (От Концепции информатизации советского общества к Стратегии развития информационного общества в Российской Федерации) // Информационные ресурсы России. 2009. № 2(108). С. 11-18.

101. Стоуньер Т. Информационное богатство: профиль постиндустриальной экономики / Т. Стоуньер // Новая технократическая волна на Западе: сборник / под ред. П. С. Гуревича. – М.: Прогресс, 1986. С.392-409.

102. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / А.А. Стрельцов; под ред. В.А. Садовничего, В.П. Шерстюка. М.: МЦНМО, 2002. 289 с.

103. Тимербулатов Т.А. Юсупов Р.Г. Информационная безопасность: об актуальности исторического исследования проблемы / Т.А. Тимербулатов, Р.Г. Юсупов // Инновационная наука. 2019. № 9. С. 23-27.

104. Тимербулатов Т.А., Юсупов Р.Г. Предпосылки развития правовых основ информационной безопасности в 1991-1993 гг. (по материалам Республики Башкортостан): исторический обзор / Т.А. Тимербулатов, Р.Г. Юсупов // Современная наука: актуальные проблемы теории и практики. Серия: Гуманитарные науки. 2020. № 3-2. С. 23-28.

105. Тимербулатов Т.А. Подход к оценке компетенции специалиста по защите информации на основе нейронной сети / Т.А. Тимербулатов, В.И. Васильев, И.Б. Герасимова // Информационные технологии интеллектуальной поддержки принятия решений: Труды VII Всероссийской научной конференции (с приглашением зарубежных ученых). В 3-х томах, Уфа, 28–30 мая 2019 года. Уфа: ГОУ ВПО «Уфимский государственный авиационный технический университет», 2019. С. 226-232.

106. Тимербулатов Т.А. Об информационной безопасности и периодизации развития средств информационных коммуникаций: историографический обзор / Т.А. Тимербулатов // Россия в XXI веке: модернизационный проект. Образование. Экономика. Общество / Т.Р. Аушев, Р.О. Багаутдинов, Н.А. Болотов и др.; под ред. Р.Г. Юсупова. Москва: ИНФРА-М, 2021. С. 326-353.

107. Тимербулатов Т.А. Развитие принципов информационной безопасности и информационного законодательства РФ в 1990-е и 2000-е годы: сравнительно-исторический аспект / Т.А. Тимербулатов // Власть истории и история власти. 2020. Т. 6. № 5(23). С. 750-762.

108. Тимербулатов Т.А. О предпосылках развития правовых основ информационной безопасности после принятия Конституции России в 1993 году: исторический очерк по материалам Республики Башкортостан / Т.А. Тимербулатов // V Валеевские чтения: научно-философское наследие Дамира Жаватовича Валеева: материалы Всероссийской научной конференции с

международным участием, посвященной 80-летию со дня рождения доктора философских наук, члена-корреспондента Академии наук Республики Башкортостан, основателя башкирской этической школы Д.Ж. Валеева, Уфа, 24 апреля 2020 года. Уфа: Башкирский государственный университет, 2020. С. 118-124.

109. Топорков А.А. Коммерческая тайна и условия ее защиты по российскому законодательству / А.А. Топорков, И.С. Сербин. // Lex Russica. – 2006. Т.65. № 1. С. 78-90.

110. Туровский В.В. Основы допуска к защите государственной тайны военнослужащих и гражданского персонала / В.В. Туровский, А.В. Жуков // Экономика и социум. 2018. № 3(46). С. 512-519.

111. Тэпскотт Д. Электронно-цифровое общество: Плюсы и минусы эпохи сетевого интеллекта / Дон Тапскотт; Пер. с англ. И. Дубинского под ред. С. Писарева. М.: Рефл-бук, 1999. 403 с.

112. Унукович А.С. Деятельность Роскомнадзора по обеспечению безопасности пользователей сети Интернет / А.С. Унукович // Молодой ученый. 2019. № 22 (260). С. 370-372.

113. Уфимцев Ю.С. Информационная безопасность России / Ю.С. Уфимцев, Е.А. Ерофеев. М.: Экзамен, 2003. 558 с.

114. Фатьянов А.А. Тайна как социальное и правовое явление. Ее виды / А.А Фатьянов // Государство и право. 1998. № 6. С.5-14.

115. Федоров А.В. Информационная безопасность: политическая теория и дипломатическая практика / А.В. Федоров, Е.А Зиновьева; Московский государственный институт международных отношений (университет) МИД России (МГИМО), Центр международной информационной безопасности и научно-технологической политики (Москва). М.: МГИМО- Университет, 2017. 357 с.

116. Федорченко С.Н. Сетевая легитимация политических режимов: теория и технологии / С.Н. Федорченко. М.: Московский государственный областной университет, 2018. 202 с.

117. Федорченко С.Н. Феномен искусственного интеллекта: гражданин между цифровым аватаром и политическим интерфейсом / С.Н. Федорченко // Журнал политических исследований. 2020. Т. 4. № 2. С. 34-57.

118. Хохлова Н.И. Обеспечение детской безопасности в Интернете: российский опыт и зарубежные инициативы / Н.И. Хохлова // Пространство и Время. 2012. № 1(7). С. 87-92.

119. Чеботарева А.А. Информационная политика России в обеспечении информационной безопасности личности: история и современность / А.А. Чеботарева // История государства и права. 2015. № 24. С.24-28.

120. Черешкин Д.С. Реалии информационной войны / Д.С. Черешкин, Г.Л. Смолян, В.Н. Цыгичко // Защита информации. Конфидент. 1996. №4. С. 9-12

121. Черешкин Д.Г. О проблеме защиты персональных данных в Российской Федерации /Д.Г. Черешкин, А.П Курило. // Проблемы информатизации. 1995. № 1. С. 32-34.

122. Черешкин Д.С. Россия начинает движение к информационному обществу / Д.С. Черешкин, Г.Л. Смолян // Информационное общество. – 2000. № 1. С. 23-25.

123. Шайхутдинова Л.С. Социальная ответственность средств массовой информации в современных условиях / Л.С. Шайхутдинова // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – 2016. – № 12 (74). Ч. 3. С. 206-208.

124. Шевцова Г.А. Информационное общество: особенности развития / Г.А. Шавцова, С.А. Батищев // Теория и практика экономики предпринимательства. Труды XVIII Всероссийской с международным участием научно-практической конференции. Симферополь, 2021. С. 387-391.

125. Шевцова Г.А. Информационное пространство Российской Федерации как безопасная информационная среда / Г.А. Шавцова, С.А.

Батищев // Информационная безопасность: вчера, сегодня, завтра. Сборник статей по материалам IV Международной научно-практической конференции. Под редакцией В.В. Арутюнова. Москва, 2021. С. 82-91.

126. Юсупов Р.Г. Функции и роль системы государственного управления в контексте социально-экономической модернизации страны / Р.Г. Юсупов, А.Р. Хайбуллин // Государственное управление в России: историко-правовые аспекты: / Колл. Авт.; под науч. ред. Р.Г. Юсупова. – Москва: ИНФРА-М, 2018. С. 17-24.

127. Юсупов Р.Г. Утверждение принципа информационной открытости государственных и муниципальных учреждений / Р.Г. Юсупов, Т.В. Чинаев // Государственное управление в России: историко-правовые аспекты / Колл. Авт.; под науч. ред. Р.Г. Юсупова. – Москва: ИНФРА-М, 2018. С. 40-49.

На английском языке

128. Arquilla J., Ronfeldt, D. Cyberwar is coming / J. Arquilla, D. Ronfeldt. – Santa-Monica: RAND, 1997. 60 p.

129. Caravelli J., Jones, N. Cyber Security: Threats and Responses for Government and Business (Praeger Security International) / J. Caravelli, N. Jones. – Praeger, 2019. 245 pp.

130. Galushkin A. A. Education in the field of national information security in the Russian Federation and abroad / A. A. Galushkin // Journal of Computer Science. – 2015. – Vol. 11. № 10. P. 988-994.

131. Jason R. Fritz. China’s Cyber Warfare / R. Fritz. Jason. – Lexington Books, 2017. 216 p.

132. Kalic Sean N. US Presidents and the Militarization of Space, 1946–1967 / Sean N. Kalic. – College Station, TX: Texas A&M University Press, 2021.

133. Libicki M. Conquest in cyberspace. National security and information warfare / M. Libicki. – Santa Monica: RAND, 2007. 307 p.

134. Prokhorov S.P. Computers in Russia: Science, Education, and Industry / S.P. Prokhorov // IEEE Annals of the History of Computing. – 1999. – Jul-Sept. – Vol. 21. №. 3.

135. Timerbulatov T.A. Internet of things. Security problems and protocols of interaction /T.A. Timerbulatov, A.V. Slinin, R.A Khasanov. // Themed collection of papers from international conferences by HNRI «National development» (Saint-Petersburg, October 2018), Санкт-Петербург, 27–31 октября 2018 года / Выпускающий редактор Ю.Ф. Эльзессер, отв. за выпуск Л.А. Павлов. СПб: ГНИИ «Нацразвитие», 2018. С. 117-121.

Электронные ресурсы

136. Институт проблем информационной безопасности. Официальный сайт. URL: https://www.iisi.msu.ru/

137. Информационно-правовая система «Гарант». URL: https://base.garant.ru/

138. Информационно-технологический портал TAdviser. URL: https://www.tadviser.ru/

139. Кодекс: Электронный фонд правовой и научно-технической документации. URL: https://docs.cntd.ru/document/901605460

140. Правительство России. Официальный сайт. URL: https://www.goverment.ru

141. Президент России. Официальный сайт. URL: https://www.kremlin.ru

142. Правовой портал «Норматив Контур». URL: https://normativ.kontur.ru/

143. Совет Безопасности Российской Федерации. Официальный сайт. URL: https://www.scrf.gov.ru/council/