Информационная безопасность

УДК 004.056
ББК66.2(2Рос)

ГОРОХОВА Светлана Сергеевна
Финансовый университет при Правительстве Российской Федерации, Ленинградский проспект, 49, Москва, 125993, Россия.
https://orcid.org/0000-0002-4919-1093
Горохова Светлана Сергеевна, кандидат юридических наук, доцент, доцент Департамента правового регулирования экономической деятельности, Москва. E-mail: Swettalana@yandex.ru

О НЕКОТОРЫХ АСПЕКТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация.

Предмет/тема. Предметом исследования являются общественные отношения, складывающиеся в процессе обеспечения информационной безопасности Российской Федерации, в связи с объявленным курсом на построение «общества знаний», и одновременным нарастанием внутренних и внешних угроз в сфере информационной безопасности, в частности, выявление сущности понимания категории «критической информационной инфраструктуры», а также систематизация угроз информационной безопасности России.

Цели/задачи. Целью исследования является комплексный анализ наиболее существенных положений российского законодательства в сфере правовой регламентации и обеспечения информационной безопасности государства, в том числе, ряда положений Федерального закона "Об информации, информационных технологиях и о защите информации", Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации", Доктрины информационной безопасности Российской Федерации, и некоторых других нормативных правовых актов.

Методология. Методологическую основу исследования составляют: всеобщие методы познания; общенаучные методы исследования, включая системный и логический метод, а также анализ, синтез и аналогию; частнонаучные методы, такие как формально-юридический метод и другие.

Вывод. Обеспечение информационной безопасности Российской Федерации, в настоящее время является одной из ключевых задач нашего государства. Такое положение дел обусловлено, с одной стороны, все более возрастающей ролью информационных технологий в общественной жизни, а с другой стороны, увеличением количества угроз национальной информационной безопасности как внутреннего, так и внешнего характера. В сложившейся ситуации следует констатировать отсутствие комплексной основы осуществления мероприятий по обеспечению безопасности информационной инфраструктуры, недостаточный уровень развития конкурентоспособных информационных технологий, а также наличие других негативных факторов, влияющих на состояние и уровень защищенности информационной сферы в Российской Федерации. При этом, приоритетным направлением реализации государственной политики в рассматриваемой области, стоит признать концентрацию государственных и общественных усилий на преодолении в первую очередь, внутренних угроз информационной безопасности, как то:

технологической отсталости и высокому уровню преступности в информационной среде.

Ключевые слова: *информация, общество знаний, информационная безопасность, критическая информационная инфраструктура, угрозы информационной безопасности.*

JEL Classification: K30

Svetlana S. Gorokhova, PhD in Legal Sciences, Associate Professor,
Associate Professor of the Department of Legal Regulation of Economic Activity, Financial University under the Government of the Russian Federation, Moscow. E-mail: Swettalana@yandex.ru

REVISITING SOME ASPECTS OF INFORMATION SECURITY IN THE RUSSIAN FEDERATION

Abstract

Subject / theme The subject of the study is the social relations developing in the process of ensuring information security of the Russian Federation, in connection with the declared course of building a "knowledge society", and the simultaneous increase in internal and external threats in the field of information security, in particular, the identification of the essence of understanding the category of "critical information infrastructure", as well as the systematization of threats to information security of Russia.

Goals / objectives The aim of the study is a comprehensive analysis of the most significant provisions of the Russian legislation in the area of legal regulation and ensuring information security of the state, including several provisions of the Federal law "On information, information technologies and information protection", Federal law "On the security of critical information infrastructure of the Russian Federation," the Information Security Doctrine of the Russian Federation and some other regulatory legal acts.

Methodology The methodological basis of the study include general methods of cognition, general scientific methods of research, including the system and logical method, as well as analysis, synthesis and analogy, private scientific methods such as the formal legal method etc.

Conclusion Ensuring information security of the Russian Federation is currently one of the key goals of our state. On the one hand this state of business is due to the increasing role of information technology in public life, and on the other hand, to the increasing number of threats to national information security, both internal and external. In the current situation, it is necessary to note the lack of a comprehensive framework for the implementation of measures to ensure the security of information infrastructure, the insufficient level of development of competitive information technologies, as well as the presence of other negative factors affecting the state and level of security of the information sphere in the Russian Federation. At the same time, the priority direction of implementation of the state policy in the considered area is to recognize the concentration of state and public efforts to firstly overcome the internal threats to information security such as technological backwardness and high level of crime in the information environment.

Keywords: *information, knowledge society, information security, critical information infrastructure, threats to information security*.

Современное общество, как бы ни оценивалось оно с позиций различных исследователей, принадлежащих к разнообразным отраслям человеческого знания, сейчас, в XXI веке, в первую очередь воспринимается через призму воздействия на него трансграничных, глобальных информационных технологий и ресурсов. Социум, породив данное явление, все больше и больше испытывает на себе воздействие непрерывно нарастающего, становящегося все более доступным, и почти не контролируемого потока информации. Мы уже не мыслим себе нашу повседневную жизнь и трудовую деятельность без присутствия высоких информационных технологий, и даже временное расставание с личными средствами коммуникации, с доступом к сетевым ресурсам и электронным услугам, предоставляемым как государством, так и частными компаниями, оборачивается для нас крайне серьезной проблемой. Причем непредвиденные сбои в работе информационных систем, могут парализовать жизнь и деятельность не только одного, конкретно взятого человека, но и всего общества, да и государства в целом. В некоторых случаях альтернативы просто нет. Мы становимся зависимыми от возможностей и удобств цифрового века. Но, помимо очевидных преимуществ, как любая иная зависимость, технологическая зависимость, таит в себе целый ряд опасностей и угроз. Поэтому, находясь на пороге формирования «общества знаний»[1], очевидно, не стоит забывать, что «во многих знаниях - многие печали».

Наверное, поэтому, принимая во внимание важность и опасность современных информационно-технологических реалий, российский законодатель уделяет вопросом построения информационного общества и обеспечения информационной безопасности значительное внимание.

Безусловно, ключевую роль в регулировании общественных отношений, складывающихся в сфере осуществления права на информацию, применения информационных технологий, и обеспечения защиты информации, играет принятый 27 июля 2006 года Федеральный закон "Об информации, информационных технологиях и о защите информации",[2] который нормативно закрепил категориально-понятийный аппарат, применяемый в данной области правоотношений, установил принципиальные подходы правового воздействия на них, а также определил иные, наиболее важные элементы правового регулирования по указанному предмету.

---

[1] Указ Президента РФ от 9 мая 2017 г. № 203 “О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы”// http://pravo.gov.ru/proxy/ips/?docbody=&nd=102431687

[2] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) "Об информации, информационных технологиях и о защите информации"(с изм. и доп., вступ. в силу с 01.01.2018)// Собрание законодательства РФ, 31.07.2006, N 31 (1 ч.), ст. 3448

Однако, вопросам информационной безопасности, как таковой, в нем уделено достаточно мало внимания. Собственно, само словосочетание «информационная безопасность» упоминается в нем лишь однажды, а именно, в пункте 4 части 1 статьи 12 «Государственное регулирование в сфере применения информационных технологий», устанавливающему, что государственное регулирование в сфере применения информационных технологий предусматривает обеспечение информационной безопасности детей. Данным пунктом указанный закон был дополнен 21 июля 2011 года,[1] что произошло в связи с принятием, другого закона, непосредственным образом относящегося к одному из аспектов обеспечения информационной безопасности - Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию".[2] Этот акт, как ясно из самого названия, посвящен регулированию отношений, связанных с защитой детей от особого рода информации, а именно такой, которая может причинить им вред. Отметим, что это, безусловно, важный аспект информационной безопасности, но, тем не менее, всего лишь ее аспект. Очевидно, чтобы разобраться каким же образом осуществляется правовое регулирование обеспечения информационной безопасности в Российской Федерации, в наиболее полном виде необходимо обратиться к каким-то иным актам. Попробуем их отыскать.

В первую очередь, в данном случае стоит обратиться к Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 года[3], как системе официальных взглядов на обеспечение национальной безопасности России в информационной сфере, заменившей собой ранее действующую Доктрину информационной безопасности, утвержденную Президентом РФ 9 сентября 2000 года.[4]

Новая Доктрина информационной безопасности, в отличие от ранее действовавшей, утверждает более развернутое определение информационной безопасности, под которым предлагает понимать состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет,

---

[1] Федеральный закон от 21.07.2011 N 252-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию"// Российская газета, N 161, 26.07.2011

[2] Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 01.05.2017) "О защите детей от информации, причиняющей вред их здоровью и развитию"// Собрание законодательства РФ, 03.01.2011, N 1, ст. 48

[3] Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"//Собрание законодательства РФ, 12.12.2016, N 50, ст. 7074

[4] "Доктрина информационной безопасности Российской Федерации" (утв. Президентом РФ 09.09.2000 N Пр-1895)// Российская газета от 28 сентября 2000 года, № 187

территориальная целостность, устойчивое социально-экономическое развитие, оборона и безопасность государства.

Данное определение может, в настоящий момент, считаться классическим, поскольку, по сути, практически дословно повторяет формулу дефиниции национальной безопасности [1] (состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации), установленную Стратегией национальной безопасности Российской Федерации.[1] Очевидно, такой подход может быть признан весьма практичным, поскольку создает унифицированную систему регулирования и восприятия как национальной безопасности нашего государства, в целом, так и отдельных ее составных частей, к которым, в том числе, относится и такой вид безопасности, как информационная.

Помимо самого определения информационной безопасности, Доктрина информационной безопасности, раскрывает сущность еще целого ряда основных понятий, среди которых - национальные интересы Российской Федерации в информационной сфере, угроза информационной безопасности, силы, средства и система обеспечения информационной безопасности, и другие.

Остановимся более подробно, на двух из вышеперечисленных определений – национальных интересах и угрозах информационной безопасности.

Говоря о национальных интересах Российской Федерации в информационной сфере, Доктрина информационной безопасности, в подпункте а) пункта два, раздела I. Общие положения, устанавливает, что под таковыми понимаются объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы.

В свою очередь, под информационной сферой, как следует из пункта 1, того же раздела, имеется ввиду совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Более подробно, содержание национальных интересов Российской Федерации в информационной сфере раскрывается в разделе II,

[1] Указ Президента РФ от 31.12.2015 N 683 "О Стратегии национальной безопасности Российской Федерации"// Собрание законодательства РФ, 04.01.2016, N 1 (часть II), ст. 212

рассматриваемой Доктрины, посвященному как раз этому вопросу.

Так, выстраивая градацию национальных интересов Российской Федерации в информационной сфере, Доктрина информационной безопасности ставит на первое место (пп. а), п.8, ч.II): обеспечение и защиту конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий; а также обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа России. [2] Как видим, в данном случае речь идет о первостепенности интересов личности и общества в структуре определяемых национальных интересов, что полностью соответствует системе ценностей, установленных Конституцией РФ.[1] Однако, стоит помнить, что при определенных обстоятельствах интересы человека, общества и государства могут входить в противоречие между собой, что приводит к конфликту интересов, с дальнейшим очевидным пересмотром приоритетов (государство/общество/гражданин).

В качестве следующего национального интереса, Доктрина информационной безопасности указывает на обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время. Здесь, признавая важность указанного блока национальных интересов России в информационной сфере, полагаем, будет небезынтересно, обратить внимание на категорию «критическая информационная инфраструктура», поскольку ранее, в перечне основных понятий, Доктрина информационной безопасности, определения данному термину не дает, хотя далее по тексту еще неоднократно его применяет. Итак, что же такое критическая информационная инфраструктура? Законодательно данная дефиниция установлена совсем недавно, а именно 26 июля 2017 года, то есть в момент принятия Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации",[2] согласно которому, под такой инфраструктурой понимаются объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких

[1] "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ)// Собрание законодательства РФ, 04.08.2014, N 31, ст. 4398

[2] Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"// Собрание законодательства РФ, 31.07.2017, N 31 (Часть I), ст. 4736

объектов. То есть, критическая инфраструктура – есть объекты этой самой инфраструктуры, плюс сети электросвязи, используемые при взаимодействии объектов. Очевидно, для лучшего понимания, предложенного определения, следует выяснить, что понимается под электросвязью и объектами критической инфраструктуры?

На первую часть вопроса, ответ можно отыскать в Федеральном законе "О связи"[1], устанавливающем, в пп.35 статьи 2, что электросвязь, это любые излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам.

Ответ на вторую часть вопроса, предлагает сам Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации", закрепляя в п.7 статьи 2, что: «объекты критической информационной инфраструктуры, это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры». Данное определение, в свою очередь, приводит правоприменителя, и других заинтересованных лиц, пытающихся определиться с пониманием содержания категории критической информационной инфраструктуры, к необходимости искать ответ на вопрос – кто же является субъектами искомой инфраструктуры?

Это можно выяснить, ознакомившись с п.8 статьи 2 рассматриваемого Закона, согласно которому - субъекты критической информационной инфраструктуры - государственные органы и учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Признавая очевидную сложность формулирования определения столь многопланового понятия как критическая информационная инфраструктура, все же отметим, что применение, настолько громоздкого, трехступенчатого формата, когда первое понятие (инфраструктура), определяется через второе понятие (объекты инфраструктуры), а второе – через третье (субъекты инфраструктуры), вряд ли можно считать удачным.

---

[1] Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 05.12.2017) "О связи"// Российская газета, N 135, 10.07.2003

Возможно, стоило бы попытаться объединить в одном определении хотя бы два из трех приведенных понятий. Применив, например, следующую редакцию: «критическая информационная инфраструктура - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры, а также сети электросвязи, используемые для организации их взаимодействия».

Возвращаясь к Доктрине информационной безопасности РФ, отметим, что следующим национальным интересом в информационной сфере, определено развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности. Безусловно, важность указанного приоритета сложно переоценить, поскольку, как указывается в Ежегодном докладе Временной комиссии Совета Федерации по защите государственного суверенитета и предотвращению вмешательства во внутренние дела Российской Федерации: «Благодаря достижениям прошлых поколений мы унаследовали мощный научно-технический потенциал, который, увы, был во многом утрачен в конце 1980-х и 1990-е гг. Без серьезных преобразований именно этот аспект может стать «ахиллесовой пятой» отечественного суверенитета.[1]

Помимо вышеназванных, Доктрина информационной безопасности РФ, относит к национальным интересам в информационной сфере еще два приоритетных направления: доведение до российской и международной общественности достоверной информации о государственной политике России и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности в области культуры; и, содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

Какие же угрозы информационной сфере и национальным интересам в указанной сфере выявляет рассматриваемая Доктрина?

Для простоты восприятия и для придания системности указанным

---

[1] Ежегодный доклад Временной комиссии Совета Федерации по защите государственного суверенитета и предотвращению вмешательства во внутренние дела Российской Федерации. Утвержден на расширенном заседании Временной комиссии по защите государственного суверенитета и предотвращению вмешательства во внутренние дела РФ 5 марта 2018г. // http://www.council.gov.ru/media/files/BX3FqMRAl7ykAmPLRl4cR1ju4RaswiKN.pdf

угрозам разделим их на два блока – угрозы извне, и угрозы внутреннего или смешанного характера.

Рассмотрим сначала внешние угрозы, поскольку их, очевидно, Доктриной информационной безопасности выявлено и представлено больше. К таковым, указанная Доктрина относит:

наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях, с одновременным усилением деятельности организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса;

расширение масштабов использования иностранными специальными службами средств оказания информационно-психологического воздействия на население (в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей);

увеличение масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников;

повышение сложности, увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры;

стремление отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве.

Резюмируя все вышеперечисленное, можно сделать вывод о том, что внешняя угроза для информационной безопасности, по сути всего одна, и сводится она к наращиванию со стороны некоторых иностранных государств информационного воздействия (сложившегося на базе технологического превосходства) на все сферы государственной и общественной жизни, осуществляемого посредством разведки, шпионажа, компьютерных атак, а также психологического воздействия на граждан, в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации. Поэтому, как ни печально, стоит констатировать, что Россия сегодня, вступила в новую эру информационной войны [3], причем, с явным техническим отставанием, по части «информационного вооружения». В пользу этого утверждения, со всей очевидностью свидетельствуют угрозы информационной безопасности, относящиеся ко второму блоку – угроз внутренних и смешанных.

Так, в данной категории можно указать на:

недостаточный уровень развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг;

высокий уровень зависимости отечественной промышленности от

зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи;

недостаточную эффективностью научных исследований, направленных на создание перспективных информационных технологий;

низкий уровень внедрения отечественных разработок и недостаточное кадровое обеспечение в области информационной безопасности, а также низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности;

отсутствие комплексной основы осуществления мероприятий по обеспечению безопасности информационной инфраструктуры.

Здесь же, одновременно можно отметить и рост масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, а также увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий.

Подводя итог, стоит отметить, что принимая во внимание серьезность и опасность внешних угроз информационной безопасности, все-таки усилия государства и общества в деле обеспечения информационной безопасности, стоит сосредоточить именно на внутренних проблемах, поскольку, во-первых они в большей степени поддаются корректировке и преодолению, чем объективно и независимо от нашей воли существующие внешние угрозы, во-вторых, от устранения внутренних проблем, во многом будет зависеть эффективность противостояния внешним угрозам, и в-третьих, «технологическое отставание, зависимость означают снижение безопасности и экономических возможностей страны, а в результате – потерю суверенитета»[1], что, безусловно, является самым нежелательным, из всех возможных вариантов развития событий.

Список литературы:

1. Горохова 2016 - Горохова С.С. Безопасность как правовая категория // Современный юрист, 2016. – № 4.-С.8-14.

2. Молчанов, Матевосова -2017 Молчанов Н. А., Матевосова Е. К. Доктрина информационной безопасности Российской Федерации (новелла законодательства)// Актуальные проблемы российского права, 2017. - № 2 (75). С.159-164

3. Раскин 2016 - Раскин А.В. Сетевые технологии в гибридной войне// Информационные войны, 2016. - № 1(37).-С.2-5

References:

1. Gorokhova 2016- Gorokhova S. S. Security as a legal category [Bezopasnost' kak pravovaya kategoriya]/ / Modern lawyer [Sovremennyj yurist], 2016. – No. 4.- P. 8-14. [in Russian]

[1] Послание Президента РФ Федеральному Собранию от 01.03.2018 "Послание Президента Федеральному Собранию"//Российская газета, N 46, 02.03.2018

2. Molchanov, Matevosova -2017 Molchanov N. A., Matevosova E. K. The Doctrine of information security of the Russian Federation (the novel of the legislation) [Doktrina informacionnoj bezopasnosti Rossijskoj Federacii (novella zakonodatel'stva)]// Actual problems of the Russian law [Aktual'nye problemy rossijskogo prava], 2017. - No 2 (75). P. 159-164 [in Russian]

3. Ruskin 2016- Ruskin V. A. Network technologies in a hybrid war [Setevye tekhnologii v gibridnoj vojne]// Information warfare [Informacionnye vojny], 2016. - No 1 (37).- P. 2-5[in Russian]