ИНФОРМАЦИОННОЕ ПРАВО КАК ВАЖНЫЙ ФАКТОР БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

А.А. Антипов, *доцент кафедры политической экономии и политологии МТУСИ, к.ю.н., antipoff77@yandex.ru;*
Е.М. Гришанова, *зав. кафедрой политической экономии и политологии МТУСИ, доцент, к.э.н., gem-mtuci@mail.ru*

УДК 654.16

Аннотация. Статья посвящена актуальным проблемам правового регулирования, обеспечения и защиты интересов личности, общества и государства в информационной сфере. Информационное право – это молодая отрасль права, возникшая в условиях информатизации общества, нуждающаяся в развитии и совершенствовании, согласовании и взаимодействии различных законов и актов между собой.

Ключевые слова: информационное право, защита информации, информационно-психологическое оружие, информационная безопасность, информационная сфера, национальная безопасность.

INFORMATION LAW AS AN IMPORTANT FACTOR FOR SECURITY AND DATA PROTECTION

Alexey Antipov, *associate professor of the political economy and political science department, Ph. D. in law;*
Elena Grishanova, *head of the political economy and political science department MTUCI, Ph. D. in economic*

Annotation. The article is devoted to topical problems of legal regulation, provision and protection of the interests of the individual, society and the state in the information sphere. Information law is a young branch of law that arose in the conditions of informatization of society, which needs development and improvement, coordination and interaction of various laws and acts among themselves.

Keywords: information law, information security, information psychological-weapons, information environment, national security.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры и субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации [1-3].

Наряду с преимуществами, которые предоставляет интеграция высоких технологий в различные сферы деятельности нашей страны, возникают и нарастают угрозы национальной безопасности. Серьезную опасность представляет собой стремление ряда стран к доминированию в мировом информационном пространстве, к вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Появляется новый термин «информационно-психологическое оружие» – это специальное оружие, которое основано на применении разрушающего информационно-

психологического, а также информационно-управляющего воздействия на психику человека для его принуждения или уничтожения.

Информационная война, которая в настоящее время уже идет – это новое понятие в области мировой науки, включающая различные аспекты политической, экономической и социально-культурной деятельности. В современной России это особенно заметно на примере средств массовой информации.

Объектом информационного воздействия современного вооружения является общественное сознание человека, его дух, воля, идейные установки и представления, при этом используются методы, ведущие к подавлению норм нравственности.

В условиях формирующегося глобального информационного пространства информация становится действенным инструментом власти [4].

Информация – это важнейшая составляющая жизнедеятельности современного общества. В официальных документах ЮНЕСКО информация определяется как универсальная субстанция, пронизывающая все сферы человеческой деятельности, служащая проводником знаний и умений, инструментом общения, взаимопонимания и сотрудничества, утверждения стереотипов мышления и поведения. Современное российское общество трудно представить без широкого применения информационных и телекоммуникационных технологий, являющихся одним из факторов социально-экономического развития государства. Информационное обеспечение государственного управления играет важную роль в обеспечении его эффективности. Информация о деятельности органов государственной власти является одной из основ функционирования политической системы государства. От этой информации зависит качество взаимодействия государства с гражданским обществом [5].

Наиболее важным документом, определяющим понятие «информационная безопасность», является утвержденная Президентом Российской Федерации В.В. Путиным Указом от 05 декабря 2016 г. [6] новая Доктрина информационной безопасности страны, которая представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. Речь идет об актуализированном документе с учетом развития отрасли информационных и коммуникационных технологий, который заменил аналогичный, но уже устаревший документ – Доктрину информационной безопасности 2000 г.

В ст. 2 Доктрины под информационной сферой понимается 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.

В новой Доктрине говорится о том, что информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства, эффективное применение которых является фактором ускорения экономического развития государства и формирования информационного общества, поскольку информационная сфера играет ключевую роль в обеспечении реализации стратегических национальных приоритетов России. Доктрина описывает стратегические цели и направления обеспечения информационной безопасности в различных областях, в частности, это защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры.

Одним из рисков для информационной безопасности в ст. 11 Доктрины называется наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру РФ в военных целях. Кроме того, отмечается усиление деятельности организаций, которые осуществляют «техническую

разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса».

Также речь идет о дискриминации российских СМИ за рубежом. Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики РФ. «Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей», – говорится в доктрине.

Другой важной, и пока непреодолимой угрозой информационной безопасности является высокий уровень зависимости российской промышленности от зарубежных информационных технологий, касающейся электронной компонентной базы, программного обеспечения.

С учетом происходящего в России и в мире Доктрина информационной безопасности является необходимым нормативно-правовым актом для решения многих задач в сфере безопасности и защиты информации. Журналисты так охарактеризовали Доктрину: «Россия получила оружие для сопротивления в информационной войне».

Минкомсвязь анонсировало готовность внесения поправок в отраслевое законодательство в соответствии с указом Президента Российской Федерации № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». В сфере использования современных информационных технологий в деятельности федеральных органов государственной власти действующее законодательство позиционируется несоответствием содержащихся в нормативных правовых актах норм реальным потребностям участников правоотношений, а также, огромным количеством нормативных правовых актов часто несогласованных между собой. Какие-либо изменения и поправки в законодательной базе осуществлялись различными министерствами и ведомствами бессистемно. Действующее законодательство в сфере инфокоммуникаций и связи давно устарело, противоречиво и несовершенно. В настоящее же время к действующему Федеральному закону «О связи» принято около сорока подзаконных актов, которые, обычно создаются, принимаются и не всегда согласуются друг с другом.

Информационная безопасность Российской Федерации – это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Информационная безопасность предполагает и означает состояние, когда в обществе созданы условия, обеспечивающие свободное развитие личности, семьи, государства, которые дают возможность объективно оценивать исторический процесс, истинную обстановку в мире, стране, регионе, вырабатывать и принимать самостоятельные решения на основе современной, достоверной информации, гуманитарного знания, составляющего и создающего истинную духовность каждого народа.

Несовершенство законодательной базы является одним из серьезных факторов, сдерживающих интенсификацию развития современных информационных технологий и обеспечение национальных интересов Российской Федерации в глобальном информационном пространстве. Таким образом, на современном этапе важным вопросом обеспечения информационной безопасности Российской Федерации является необходимость подготовки и принятия новых нормативных правовых актов, а также уточнение существующих концептуальных и доктринальных документов, которые адекватно отражали бы национальные интересы России, в том числе в информационной сфере, и способствовали бы реализации задач обеспечения информационной безопасности.

Когда заходит речь о законодательной базе необходимо сказать, что информационное право определяется совокупностью норм, регулирующих поведение субъектов в информационной сфере – физических и юридических лиц, органов государственной власти и местного самоуправления. Если информационное право регулирует общественные отношения

в информационной сфере, то наука информационного права исследует информационные нормы и отношения, которые возникают при их применении, изучает эффективность действия информационных нормативных актов, кодифицирует, систематизирует, структурирует их.

Компьютерное право, коммуникационный менеджмент, информационное законодательство, а главное – развитие реалий в области информации, информатизации, защиты информации – вот аргументы за выделение отрасли информационного права в системе российского права.

Следует отметить, что и в практике применения права, и в самом нормотворчестве, равно как и в теории, часто происходит подмена понятий «предмет» и «объект» регулирования, что нарушает точность понимания того, о чем идет речь в конкретных обстоятельствах. Обращаясь в архив для получения того или иного документа, человек реализует свое конституционное право на информацию. Предмет его интереса – определенный документ. Законодательство, устанавливая право гражданина на получение информации и соответствующие обязанности архива предоставить интересующий гражданина документ, регулирует взаимоотношения этих взаимосвязанных обстоятельствами и законом субъектов. Эти отношения осуществляются в форме оказания информационной услуги со стороны архива и соблюдения определенных действий самим гражданином, который должен соответствующим образом оформить свой запрос. Так, конкретно выделяются:

- предмет отношений (документ или его копия);
- отношения связанных субъектов по поводу указанного предмета, регулируемые нормами законодательства и подзаконными актами;
- предметная сфера права (механизм регулирования отношений субъектов относительно предмета их интереса с учетом позиции государства – нормативно выраженная совокупность прав и обязанностей всех взаимосвязанных субъектов).

Предметом информационного права является не только сама информация, но и процессы, связанные с ее получением (созданием, снятием), обработкой, хранением, передачей, распространением и так далее [3]. Совокупность этих действий называется информатикой, а создание условий для внедрения новейших технологий в работе с информацией – информатизацией. Таким образом, информация, информатизация, коммуникация информации по различным типам сетей и отношения, возникающие в этой связи, в совокупности составляют предметную область информационного права [7].

Специфическими институтами информационного права являются: свобода, тайна, доступ, правовой режим информации и информационного ресурса, право на информацию, защита информации, виды информации (открытая, ограниченного доступа, массовая, официальная и другие). К межотраслевым институтам можно отнести институты собственности и интеллектуальной собственности, так как корни их лежат в системе гражданского права, но обеспечиваются они и нормами публичного права, а также применяются в системе отношений, регулируемых информационным законодательством.

Наиболее развитыми институтами информационного права в теоретическом и нормативном отношении являются: институт права на информацию, институт массовой информации, институт правового режима информационных ресурсов, институт государственной тайны. Проблематика правового института требует более углубленного исследования, чем это делалось до сих пор. А в области информационной деятельности и информационных отношений этот вопрос требует особого внимания, ибо точность определения института существенным образом влияет не только на процесс нормотворчества, но и на содержание научных исследований и практику право применения [8].

Основными направлениями защиты информационной сферы являются:

- защита интересов личности, общества и государства от воздействия вредной, опасной и недоброкачественной информации;
- защита информации, информационных ресурсов и информационных систем от неправомерного воздействия посторонних лиц;

- защита информационных прав и свобод.

Характеристика правонарушений режима охраняемой информации включает в себя совокупность признаков:

- помогающих уяснить распространенность и структуру правонарушений, в которой они распределены в зависимости от вида тайны (государственная, служебная, коммерческая);
- определяющих сферы профессиональной деятельности исполнителей секретных (конфиденциальных) документов и работ, в которых наблюдается проявление правонарушений режима охраняемой информации;
- отражающих личностные особенности лиц, виновных в совершении правонарушений и режима охраняемой информации, способствующих пониманию возникновения угроз для информационной безопасности, прочих правонарушений режима охраняемой информации и осуществления предупредительной деятельности.

Первая группа признаков служит информационной базой для оценки степени актуальности борьбы с правонарушениями режима охраняемой информации, для определения основных направлений этой деятельности, для достижения наиболее оптимального результата использования сил и средств профилактического воздействия.

Вторая группа признаков показывает ту среду, своего рода «жизненное пространство», в рамках и при наличии которой правонарушения режима охраняемой информации могут существовать, а при определенных условиях и обеспечивать собственное «воспроизводство». Исследование данных признаков имеет значение для реализации практических действий по нейтрализации и искоренению правонарушений, в том числе и преступлений, посягающих на сохранность государственной, служебной, коммерческой и других видов тайн.

Третья группа признаков основана на наличии неразрывной связи между деянием и исполнителем. Она позволяет при решении задач борьбы с правонарушениями в сфере обращения информации с ограниченным доступом изучить особенности проявления этих нарушений, обусловленные особенностями личности тех, кто совершает такого рода правонарушения, и учитывать их в профилактической деятельности.

Перечисленные группы признаков отражают также и социальные явления, и процессы, обуславливающие правонарушения в сфере обращения информации с ограниченным доступом, показывают единство объективных и субъективных элементов в характеристике правонарушений режима охраняемой информации и убеждают в необходимости учитывать подобные явления в законотворческой и предупредительной деятельности. Существенное значение для раскрытия характеристики правонарушений режима охраняемой информации имеет выявление возможных каналов утечки информации.

Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Литература

1. Девяткин Е.Е., Володина Е.Е., Суходольский А.М., Суходольская Т.А. Основные направления развития информационно-коммуникационных технологий в Европе // Труды Научно-исследовательского института радио, 2012. – № 2. – С. 11-22.
2. Володина Е.Е., Девяткин Е.Е. Интернет вещей: тенденции и перспективы развития // в книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 38-ой международной конференции РАЕН. – Шри-Ланка. 2016. – С. 16-17.
3. Кузовкова Т.А., Володина Е.Е., Кухаренко Е.Г. Экономика отрасли инфокоммуникаций. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 190 с.

4. Гришанова Е.М., Орлова Е.Ю. Основные цели государственного регулирования отрасли инфокоммуникаций // T-Comm, 2012. – № 12. – С. 17-18.
5. Гришанова Е.М., Краснослободцева Е.А. Государственное регулирование рынка инфокоммуникаций: проблемы и методы // T-Comm, 2014. – № 8. – С. 32-35.
6. Указ Президента Российской Федерации № 646 от 5 декабря 2016 г.
7. Гришанова Е.М., Антипов А.А. Защита информации и информационное право // T-Comm, 2016. Т. 10. – № 5. – С. 64-66.
8. Бачило И.Л. Информационное право: учебник. – М.: Издательство Юрайт, 2016. – 437 с.