УДК 004.056 (470) + 342:002:004.056 Вестник УрФО № 3(21) / 2016, с. 62–66

Минбалеев А. В.

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Статья посвящена анализу проекта Доктрины информационной безопасности Российской Федерации, официально размещенного на сайте Совета Безопасности Российской Федерации. Автором анализируется действующая Доктрина информационной безопасности, ее значение для формирования российского информационного законодательства. Исследуются вопросы Доктрины информационной безопасности, которые были реализованы, а также нереализованные. Автор исследует понятия в сфере информационной безопасности, предлагаемые в проекте Доктрины, соотносит их с действующим законодательством Российской Федерации, делает вывод о несоответствии ряда определений информационному законодательству. Автором предлагается внесение в Доктрину ряда изменений, направленных на приведение проекта Доктрины действующему информационному законодательству.

Ключевые слова: *информационное право, информационное общество, информационная безопасность, доктрина, национальные интересы, информационные угрозы.*

Minbaleev A. V.

THE INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION: CURRENT STATE AND PROSPECTS OF DEVELOPMENT

The article is devoted to analysis of the project information security doctrine of the Russian Federation, officially posted on the website of the Security Council of the Russian Federation. The author analyzes the current Doctrine of information security, its significance for the development of Russian information legislation. Examines the issues of the informational security Doctrine that was implemented and unimplemented. The author explores concepts in the field of information security proposed in the draft Doctrine, correlates them with the current legislation of the Russian Federation, concludes that the discrepancy of several definitions of information legislation. The author proposes the introduction of the Doctrine of a number of changes aimed at bringing the project to the current Doctrine of information law.

Keywords: *information law, information society, information security, doctrine, national interests, the threat of information.*

Стремительное развитие информационного общества всегда связано с появлением самых разных информационных угроз, в связи с чем его неотъемлемым атрибутом всегда выступает информационная безопасность. Основным документом, которым на концептуальном уровне определяется общее состояние информационной безопасности и перспективы ее развития в Российской Федерации, является Доктрина информационной безопасности (утв. Президентом Российской Федерации от 09 сентября 2000 г. № Пр-1895, далее). Действующая Доктрина информационной безопасности, бесспорно, во многом морально уже устарела. Объясняется это прежде всего тем, что в момент ее принятия в России еще не было полноценной системы правового обеспечения информационной безопасности, не была выстроена система информации ограниченного доступа, теория информационного оружия и информационных войн только в самом первом приближении рассматривалась учеными сквозь призму переводной западной литературы. Поэтому и неудивительно, что многие вопросы информационной безопасности, рассматриваемые на современном этапе общественного развития как обычные, ежедневно реализуемые, в Доктрине нашли лишь незначительное упоминание. Несмотря на то, что положения Доктрины относятся к нормам «мягкого права», большинство вопросов в сфере информационной безопасности, изложенные в ней, нашли реализацию как в российском законодательстве, так и на уровне целого ряда международных актов в рамках региональных международных организациях, в которых участвует или участвовала Российская Федерация (СНГ, ЕврАзЭс, ЕАЭС, ШОС, БРИКС и др.). Положения Доктрины информационной безопасности учитывались при подготовке нормативных правовых актов как в информационной сфере, так и в других, что отчетливо проявляется как в понятийном аппарате современного законодательства, так и в его содержании. Ряд положений Доктрины информационной безопасности находятся в стадии реализации и отражения в законодательстве. Так, до сих пор не сформировано законодательство о служебной тайне, о безопасности критической информационной инфраструктуры. На протяжении последних десяти лет неоднократно поднимался вопрос о реформировании Доктрины информационной безопасности и необходимости принятия новой реакции или новой Доктрины. Однако только в конце 2015 года появляется первый проект новой Доктрины информационной безопасности Российской Федерации, в последующем существенно переработанный и официально представленный на сайте Совета Безопасности Российской Федерации (использован проект, размещенный на сайте Совета Безопасности Российской Федерации по адресу http://www.scrf.gov.ru/documents/6/135.html по состоянию на 26.08.2016 г.)

В целом проект Доктрины информационной безопасности Российской Федерации (далее – проект Доктрины) строится на современных положениях российского информационного законодательства и законодательства о национальной безопасности. Проект Доктрины устанавливает, что ее правовую основу составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права и международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, а сама Доктрина служит основой для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации, выработки мер по совершенствованию системы информационной безопасности Российской Федерации, включая разработку отраслевых документов стратегического планирования Российской Федерации в информационной сфере или затрагивающих данную сферу, а также для развития общественных отношений, связанных с деятельностью в области информационной безопасности Российской Федерации.

В проекте устанавливаются новая редакция перечня национальных интересов в информационной сфере, к которым отнесены:

а) соблюдение конституционных прав и свобод человека и гражданина в области получения и использования информации, включая неприкосновенность частной жизни при использовании информационных технологий, информационную поддержку участия граждан в управлении государством, политической жизни общества, а также сохранение культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры Российской Федерации, включая критическую информационную инфраструктуру Российской Федерации и единую сеть электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

в) развитие отрасли информационных технологий в Российской Федерации, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказания услуг в области обеспечения информационной безопасности;

г) доведение до российской и международной общественности и разъяснение объективной и достоверной информации о государственной политике Российской Федерации и об официальной позиции ее высшего политического руководства по социально значимым событиям в стране и мире, содействие распространению духовных и культурных ценностей народов России по всему миру;

д) содействие формированию международного правового режима, нацеленного на противодействие угрозам использования информационных технологий для нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также обеспечение суверенитета Российской Федерации в информационном пространстве.

Анализ предлагаемых национальных интересов в информационной сфере явно свидетельствует о стремлении государства на системном уровне противодействовать развязыванию информационных противоборств, в том числе использования информационного оружия против Российской Федерации и ее граждан и организаций. При этом ставятся задачи как по формированию и укреплению равноправного стратегического партнерства в области информационной безопасности, так и обеспечения суверенитета Российской Федерации в информационном пространстве.

Деятельность государственных органов в сфере обеспечения информационной безопасности Российской Федерации основывается на следующих принципах:

• законность и правовое равенство всех участников общественных отношений в информационной сфере, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

• соблюдение баланса между потребностью граждан и общества в свободном обмене информацией и необходимыми ограничениями на распространение информации в целях обеспечения национальной безопасности, в том числе в информационной сфере;

• достаточность сил и средств для обеспечения информационной безопасности Российской Федерации, определяемая в том числе за счет постоянного мониторинга угроз в информационной сфере;

• соблюдение общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации с учетом ограничений, установленных законодательством Российской Федерации.

В проекте Доктрины устанавливаются и новые основные направления обеспечения информационной безопасности Российской Федерации. Развитие и совершенствование системы информационной безопасности Российской Федерации достигается путем:

• усиления вертикали и централизации управления силами информационной безопасности Российской Федерации на федеральном, межрегиональном, региональном, муниципальном и объектовом уровне (объекты информатизации, операторы информационных систем и сетей связи);

• совершенствования форм и методов взаимодействия сил обеспечения информационной безопасности Российской Федерации в целях повышения их готовности к противодействию угрозам в информационной сфере;

• совершенствования информационно-аналитического и научно-технического обеспечения функционирования системы информационной безопасности Российской Федерации;

• повышения эффективности взаимодействия между государственными органами, органами местного самоуправления, организациями различных форм собственности и гражданами при решении задач в области информационной безопасности Российской Федерации.

Анализ проекта Доктрины позволяет выделить и ряд дискуссионных моментов, которые необходимо поднять в рамках обсуждения проекта для его совершенствования. Прежде всего, необходимо отметить ряд вопросов связанных с понятийным аппаратом, используемым в проекте Доктрины.

1. В проекте Доктрины под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем и сетей связи, информационных технологий, а также субъектов, деятельность которых связана с данными технологиями и обеспечением информационной безопасности, и механизмов регулирования возникающих при этом общественных отношений. В определении используется категория «информатизация», которая прекратила использоваться с 2006 года в российском информационном законодательстве и была заменена на развитие информационных технологий. В связи с этим не совсем понятно становится, что сегодня является объектами информатизации. Также данная категория используется в определении понятия «информационная инфраструктура Российской Федерации», в связи с чем возникает аналогичное замечание. Вряд ли можно рассматривать частью информационной сферы механизмы регулирования, возникающих в ней общественных отношений. Механизмы регулирования, в том числе правового, технического регулирования, не входят в информационную сферу, а регулируют ее, формируют особый режим существования информационной сферы. Частью информационной системы могут быть лишь механизмы саморегулирования и сорегулирования, а также локального правового регулирования информационных отношений, которые формируются и обеспечиваются во многом субъектами информационной сферы. Таким образом, при построении определения допущена логическая ошибка.

2. Полагаем, что в определении категории «средства обеспечения информационной безопасности Российской Федерации» наряду с организационными, техническими и программно-техническими средствами, используемыми силами обеспечения информационной безопасности Российской Федерации, необходимо обязательно на первом месте указать правовые средства. В качестве правовых средств традиционно выступают нормы и принципы права, правоприменительные акты, договоры, юридические факты, субъективные права, юридические обязанности, запреты, льготы, меры поощрения, меры наказания, акты реализации прав и обязанностей и т.п. Все эти средства активно используются в проекте Доктрины. Указание на правовые средства явно придаст Доктрине характер документа, построенного на основе принципа законности, и будет важной гарантией, что средства обеспечения информационной безопасности Российской Федерации будут использоваться на основе и в прямом взаимодействии с правовыми средствами. В связи с этим название раздел V проекты Доктрины необходимо дополнить и озаглавить как «Правовые и организационные основы обеспечения информационной безопасности Российской Федерации». Фактически в данном разделе говорится и о правовых и об организационных основах. Реализация предложенных мер будет способствовать формированию нормативного компонента системы информационной безопасности Российской Федерации (нормативных средств, используемых силами обеспечения информационной безопасности).

3. В ряде категорий, используемых в проекте Доктрины, используются понятия угрозы в информационной сфере, суверенитет в информационной сфере. Полагаем, что данные категории также нуждаются в определении в Доктрине.

4. При определении понятия «информационная инфраструктура Российской Федерации» устанавливается, что она включает в себя «совокупность объектов информатизации, информационных систем и сетей связи». Между тем, как отмечалось ранее, непонятно, что сегодня представляют собой объекты информатизации. В составе инфраструктуры, к сожалению, не указаны информационные ресурсы Российской Федерации, а также системы средств обеспечения функционирования информационных систем и сетей связи.

5. Определение понятия «информационная безопасность Российской Федерации» предлагается изложить в новой редакции, а именно как «состояние защищенности личности, общества и государства от внутренних и внешних угроз в информационной сфере, при котором обеспечиваются ***в том числе*** реализация конституционных прав и свобод граждан Российской Федерации (далее – граждане), достойные качество и уровень их жизни, суверенитет, территориальная це-

лостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства». Имеющаяся сегодня формулировка заставляет при обеспечении информационной безопасности одновременно обеспечивать и конституционные права и свободы граждан Российской Федерации, и достойные качество и уровень их жизни, и суверенитет, и территориальную целостность, и устойчивое социально-экономическое развитие Российской Федерации, и оборону и безопасность государства, что, фактически, невозможно осуществить в значительном количестве случаев, поскольку Конституция Российской Федерации допускает ограничение конституционных прав и свобод человека и гражданина в ряде случаев. Предлагаемые изменения позволяют учесть данный момент и позволяют обеспечить информационную безопасность Российской Федерации в определенных случаях, когда есть необходимость ограничения конституционных прав и свобод человека и гражданина.

Проект Доктрины определяет состояние информационной безопасности Российской Федерации в отдельных областях. Анализ данных положений явно свидетельствует, что в п. 18 проекта Доктрины при характеристике состояния информационной безопасности Российской Федерации в области науки, технологий и образования, к сожалению, не отмечается ничего о низком уровне медиаобразования и медиаграмотности современной системы образования. При наличии огромных разработок по обучению основам медиаграмотности современных школьников и студентов, в России, к сожалению, не принимаются меры по включению данных знаний в раздел школьной и вузовской образовательной программ. Полагаем, что это необходимо учесть и отразить в Доктрине. Современная молодежь не умеет противостоять негативному информационному воздействию. Государство не сможет оградить молодежь от огромного массива информации, которую они получают из сети Интернет, но сможет научить правильно ее воспринимать, учитывать знания об информационном оружии.

Анализ проекта Доктрины в целом свидетельствует, что при ее подготовке была проделана огромная работа по систематизации как основных угроз в информационной сфере, так и соответствующих перспективных направлениях обеспечения информационной безопасности в Российской Федерации. Проект Доктрины отражает реальное состояние современного информационного общества и многочисленные информационные угрозы национальным российским интересам в информационной сфере.

Минбалеев Алексей Владимирович, профессор кафедры теории государства и права, конституционного и административного права Южно-Уральского государственного университета, доктор юридических наук. Россия, 454080, г. Челябинск, проспект Ленина, 76. E-mail: alexmin@bk.ru.

Minbaleev Aleksey Vladimirovich, professor department of Theory of state and law, constitutional and administrative law of the South Ural State University (national research university). Doctor of Law. Russia, 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: alexmin@bk.ru.