# ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ИНФОРМАЦИОННОЙ СФЕРЕ

Н. А. Молчанов*, Е. К. Матевосова**

# Доктрина информационной безопасности Российской Федерации (новелла законодательства)

***Аннотация.*** *В статье исследуются актуальные вопросы правового и организационного обеспечения информационной безопасности России в свете Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 № 646. Детально анализируя такой документ стратегического планирования, авторы указывают на необходимость качественного совершенствования правовой базы и механизма системы обеспечения информационной безопасности с учетом новых угроз и вызовов современного мира. Объективная оценка новеллы законодательства в области обеспечения информационной безопасности Российской Федерации сопровождается рассуждениями авторов о проблемах обеспечения информационной безопасности на национальном и международном уровне, ответственность за эффективное разрешение которых во многом возлагается именно на право.*

***Ключевые слова:*** *национальная безопасность, информационная сфера, информационная безопасность, международная информационная безопасность, доктрина, стратегическое планирование, информатизация общества, совершенствование законодательства, правовая политика, информационная политика.*

**DOI: 10.17803/1994-1471.2017.75.2.159-165**

Качество политических, социально-экономических, духовно-культурных и иных государственных преобразований сегодня напрямую зависит от состояния национальной и международной информационной безопасности.

Формирование новых угроз и рисков обеспечению информационной безопасности государства на фоне глобализационных процессов во многом определяет приоритетные направления государственной политики в информационной сфере как системообразующего фактора жизни общества.

В своем Послании Федеральному Собранию 01 декабря 2016 года Президент Российской Федерации В. В. Путин отметил необходимость



* *Молчанов Николай Андреевич* — профессор кафедры интеграционного и европейского права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), доктор военных наук, заслуженный деятель науки РФ

namolchanov@msal.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** *Матевосова Елена Константиновна* — старший преподаватель кафедры теории государства и права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук

ekmatevosova@msal.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

укрепления защиты от киберугроз, повышения устойчивости всех элементов инфраструктуры, финансовой системы, государственного управления[1].

В публичных выступлениях руководства многих стран все чаще звучат заявления о наращивании потенциала для эффективного отражения целенаправленной вражеской агрессии со стороны того или иного государства, оправдывающего свои действия защитой национальных интересов от реальных и «мнимых» атак.

Информационные системы органов государственной власти, а также организаций, деятельность которых имеет социально-экономическую значимость (средства массовой информации, банки и др.) превращаются сегодня в театр военных действий с применением информационного оружия массового поражения. Развитие событий этой военной драмы XXI века будет во многом зависеть от готовности государств к международному сотрудничеству в области обеспечения информационной безопасности, осознавая неизбежные для себя в условиях глобализации угрозы и риски.

Находясь в состоянии необъявленной и затянувшейся информационной войны, многие государства уже сегодня создают специальные воинские подразделения в составе своих вооруженных сил – информационные войска особого назначения. С учетом заинтересованности любого государства в расширении сферы своего влияния в поддержании и укреплении авторитета на международной арене велика опасность применения данными подразделениями информационного кибероружия в иных, отличных от декларируемых оборонительных, целях. Очевидно, что основным преимуществом подобного рода войск является не численное превосходство над противником, а наличие передовых информационных технологий и владение необходимыми знаниями и практическими навыками.

Функционирование эффективной национальной системы обеспечения информационной безопасности государства требует совершенствования ее организационного механизма, а, следовательно, нормативного регулирования в данной сфере, исходя из объективной оценки состояния информационной безопасности и различных сценариев развития информационного общества в национальном и международном масштабе.

Доктрина информационной безопасности Российской Федерации 2000 года была признана утратившей свою силу в связи со сменой официальных взглядов на основные вопросы обеспечения информационной безопасности России. В стремительно изменяющемся глобализированном мире возникает потребность в качественно новых доктринальных подходах к решению проблем безопасности, что представляет собой сложную юридическую, управленческую, научную, методологическую задачу.

Новеллой российского законодательства в информационной сфере, несомненно, является Доктрина информационной безопасности Российской Федерации, утвержденная 5 декабря 2016 года Указом Президента Российской Федерации[2].

Разработка такого документа есть объективная потребность в актуализации правовой основы обеспечения информационной безопасности общества, развитие которого сегодня всецело предопределяется процессами информатизации.

Как отмечается в Стратегии национальной безопасности Российской Федерации[3], политика сдерживания России, реализуемая США и их союзниками, стремящимися сохранить свое доминирование в мировых делах, предусматривает оказание давления на Россию в том числе в информационной сфере. Стратегия

[1] Послание Президента Российской Федерации Федеральному Собранию от 01.12.2016 // Парламентская газета. 02.12.2016.

[2] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

[3] Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2016. № 1 (часть II). Ст. 212.

прогнозирует усиление противоборства в глобальном информационном пространстве, которое оказывает прямое влияние на международную обстановку в целом. Следует отметить, что Доктрина информационной безопасности Российской Федерации, в продолжение основных «тезисов» документов стратегического планирования, содержит множество положений об угрозах внешней агрессии, и, несмотря на используемую при этом общую формулировку «рядом зарубежных стран», список этих стран небезызвестен.

Утратившая силу Доктрина информационной безопасности Российской Федерации не содержала разъяснения того, что следует понимать под «информационной сферой», однако и действующая Доктрина, несмотря на предпринятую попытку устранить данный пробел, не внесла должной ясности в таком вопросе, сформулировав определение путем перечисления абсолютно разнопорядковых компонентов (совокупность информации, объекты информатизации, информационные системы, сайты, сети связи, информационные технологии, а также субъекты, деятельность которых связана с обеспечением информационной безопасности, и, наконец, совокупность механизмов регулирования общественных отношений в данной сфере).

Новая Доктрина определяет понятие «информационная безопасность» как 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, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. Очевидно, что при формулировании центрального для всего документа понятия был избран незамысловатый прием точного копирования определения понятия «национальная безопасность», закрепленного в Стратегии национальной безопасности Российской Федерации, с одной лишь подстановкой слова «информационных». Однако, как представляется, совершенствование правового регулирования в рассматриваемой сфере, что, прежде всего, и предполагалось данной Доктриной, должно иметь системный, комплексный характер, устраняя пространность, неоднозначность ключевых понятий и их дефиниций.

В документе обозначаются в целом следующие «сферы» и «области» информационной безопасности: кредитно-финансовая сфера, область обороны страны, область государственной и общественной безопасности, экономическая сфера, область науки, технологий и образования, область стратегической стабильности и равноправного стратегического партнерства, область культуры. Такой многоаспектный подход к информационной безопасности соответствует определяемым Стратегией национальной безопасности Российской Федерации национальным интересам и стратегическим национальным приоритетам государства.

Оценивая состояние информационной безопасности в области науки, технологий и образования, разработчики Доктрины обрушиваются с резкой критикой в адрес российского научного сообщества, указывая на «недостаточную эффективность научных исследований» в соответствующей сфере, «низкий уровень внедрения отечественных разработок», «недостаточное кадровое обеспечение». Кроме того в документе обозначается серьезная проблема — мероприятия по обеспечению безопасности информационной инфраструктуры зачастую не имеют комплексной основы.

Несомненно, от российской науки ожидается значительный вклад в развитие технологических инноваций, укрепляющих информационную безопасность государства. Но потребность в научных знаниях обнаруживается не только при разработке интегральных микросхем, но и при совершенствовании законодательства в области информационной безопасности и модернизации системы ее обеспечения, с использованием конкретных научных результатов фундаментальных и прикладных исследований. В этой связи необходимо акцентирование внимания на проблеме научной обоснованности реализуемой государственной политики в данной области Советом Безопасности

Российской Федерации, в частности такими его рабочими органами, как Межведомственной комиссией по информационной безопасности, а также Научным советом.

Подпункт «г» (развитие отечественного конкурентоспособного производства) пункта 25 Доктрины, определяющего основные направления информационной безопасности в экономической сфере, по своему смысловому содержанию во многом дублирует предыдущий пункт «в» (повышение конкурентоспособности российских компаний). Кроме того, провозглашаемая в пункте 26 Доктрины стратегическая цель обеспечения информационной безопасности в области науки, технологий и образования («поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности») является незначительно измененной формулировкой подпункта «г» пункта 25. Следует также отметить, что поддержка, как таковая, очевидно в значении государственной меры, не может быть понимаема в качестве стратегической цели в данной области, поскольку целесообразно исходить не из процесса, сопутствующего достижению цели, а из конкретного моделируемого результата, каким, собственно, и является сама цель.

Подпункт «а» пункта 27 Доктрины снова заявляет о необходимости «достижения конкурентоспособности российских информационных достижений». Нисколько не оспаривая высокую значимость государственной задачи повышения конкурентоспособности российской экономики в целом, ее сектора в информационной сфере в частности, представляется, что вопрос об уместности столь многократного повторения такого доктринального посыла в одном документе с точки зрения юридической техники остается открытым.

Согласно пункту 32 Доктрины «состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации». Однако данное положение имеет неопределенную смысловую нагрузку в части понимания под «составом системы» исключительно ее элементной структуры или также функциональной взаимосвязи ее звеньев.

Доктрина называет исчерпывающий перечень принципов, на которых основывается деятельность государственных органов по обеспечению безопасности. В подпункте «а» пункта 34 Доктрины обозначен такой принцип, как «законность общественных отношений в информационной сфере», формулировка которого пренебрегает известными современной юридической науке постулатами о понятии и сущности законности. В подпункте «б» того же пункта о принципе конструктивного взаимодействия государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности отсутствует указание на органы местного самоуправления, которые, при этом, согласно положениям Доктрины являются и силами обеспечения информационной безопасности (пп. «д» п. 2), и имеют определенные властные полномочия в информационной сфере (п. 31).

Недостаточно обоснованно указание в Доктрине на самостоятельную группу задач государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности (п. 36), учитывая то, что в предшествующем пункте Доктрина называет задачи государственных органов в рамках деятельности по обеспечению информационной безопасности (п. 35). Представляется, что эффективное обеспечение информационной безопасности государства включает и предполагает развитие и совершенствование ее единой системы, а потому для классификации задач в достижение определенных стратегических целей следовало бы использовать иные исходные критерии.

Доктрина не обходит вниманием проблемы обеспечения международной информационной безопасности, указывая на ряд нерешенных вопросов, затрудняющих формирование ее системы, в числе которых состояние правовой регламентации информационной безопасности на международном уровне, а также отсутствие механизмов и процедур применения соответствующих нормативных требований.

В настоящее время содействие Российской Федерацией установлению международного правового режима, направленное на создание условий для формирования системы международной информационной безопасности, обеспечивается реализацией такого документа стратегического планирования, как Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года[4]. Согласно Основам под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры. Таким образом, международная информационная безопасность может быть представлена как простая математическая совокупность «состояний» информационной безопасности всех стран мира. Следуя данному подходу оценить общее состояние глобальной информационной безопасности невозможно. А потому в рамках этой проблематики необходимо, скорее всего, обращаться к вопросам о международно-правовом регулировании и применяемых государствами мерах в информационной сфере.

Российские инициативы в области формирования системы международной информационной безопасности, и составляющие основу государственной политики страны в данной области, не всегда находят поддержку, что вполне объяснимо усилением политического соперничества государств, вместо достижения согласия и учета взаимных интересов.

Несмотря на реализацию ряда межгосударственных мер, в том числе в рамках международных договоров о сотрудничестве, надо признать, что единый международный правовой режим обеспечения информационной безопасности еще находится в стадии своего формирования, которое невозможно представить без разработки практически применимых международных правовых актов, не противоречащих национальным интересам «договаривающихся» сторон.

Как отмечается российскими исследователями, «по сути, предпринимаются попытки убедить мировое сообщество в неизбежности конфликтов с использованием информационно-коммуникационных технологий и оставить за собой право действовать по своему усмотрению в отсутствии реального правового регулирования данной сферы»[5]. Однако конфликты между странами, активно участвующими в разделе информационного поля, и правда, неизбежны. Отсутствие всеохватывающей важнейшие проблемы информационной безопасности правовой регламентации на международном уровне, несомненно, открывает большие возможности для произвольного, искаженного толкования принципов и норм международного права в сфере использования информационных и коммуникационных технологий.

Обеспечение безопасности — это основная проблема человечества на протяжении всей мировой истории, решить которую намеревались многие когда-либо созданные международные организации.

В своей Резолюции от 02 декабря 2014 года Генеральная Ассамблея ООН отмечая результативную работу Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, выражает озабоченность тем, что информационные технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут

[4] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 № Пр-1753 // Официальный сайт Совета безопасности РФ. URL: http://www.scrf.gov.ru.

[5] *Лапшин В. Д*. Формирование системы международной информационной безопасности: подходы и инициативы России // Научные проблемы национальной безопасности Российской Федерации / сост.: С.М. Буравлев и др. М., 2015. С. 177.

негативно воздействовать на целостность инфраструктуры государств, нарушая их безопасность применительно как к гражданской, так и к военной сферам[6].

Не утрачивая надежд на использование существующими международными организациями (специальными органами в их составе) правовых рычагов обеспечения информационной безопасности, призывая все страны соблюдать правила игры на информационном поле, России, как и всем другим государствам, следует самостоятельно развивать и поддерживать международное сотрудничество, выступая с предложениями, имеющими в своем основании взаимовыгодный интерес.

Сравнительный анализ «доктрин» информационной безопасности Российской Федерации позволяет критично утверждать, что, по структуре, полноте правового регулирования и другим важным характеристикам, Доктрина информационной безопасности Российской Федерации 2016 года, несмотря на то, что носит актуализированный характер, по сути, не является более совершенным правовым актом, чем предыдущая Доктрина.

Реалии глобального информационного взаимодействия и одновременно противостояния требуют коренной переработки всего массива нормативных правовых актов, обозначающих и предлагающих пути решения проблем обеспечения информационной безопасности. Так, в настоящее время на общественное обсуждение вынесен проект Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы[7]. Согласно данному документу принятые в большинстве стран мира подходы к государственному регулированию сферы информации и информационных технологий вынуждены «на ходу» адаптироваться к новым обстоятельствам.

Но, как представляется, выработка единственно верных вневременных подходов — это бесполезная и невыполнимая задача, поскольку отношения в информационном обществе будут все более усложняться, неминуемо порождая новые, с трудом прогнозируемые, обстоятельства.

Утверждение проекта Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы не вызывает сомнений, однако документ требует детального научно-правового анализа всех его положений, каждое из которых должно иметь определенное стратегически направляющее, регулирующее значение.

Актуальность и приоритетность направления совершенствования нормативной правовой базы в области обеспечения информационной безопасности, с учетом соответствующих предложений и рекомендаций Совета Безопасности Российской Федерации, подтверждаются необходимостью создания структурно единой и функционально взаимосвязанной системы обеспечения информационной безопасности на федеральном, региональном и муниципальном уровнях, что, в свою очередь, подчеркивает важность стратегического планирования и правового обеспечения в данной области, а главное, что именно право призвано не допустить состояния полного мирового информационного хаоса.

[6] Официальный сайт Организации Объединенных Наций. URL: http://www.un.org/ru/index.html.

[7] Официальный сайт Совета безопасности РФ.

**БИБЛИОГРАФИЯ**

1. *Лапшин В. Д.* Формирование системы международной информационной безопасности: подходы и инициативы России // Научные проблемы национальной безопасности Российской Федерации / сост.: С. М. Буравлев и др. — М., 2015.

*Материал поступил в редакцию 10 декабря 2016 г.*

**THE DOCTRINE OF INFORMATION SECURITY OF THE RUSSIAN FEDERATION (NEW LAW)**

**MOLCHANOV Nikolay Andreevich** — Profesor at the Department of Integration and European Law, Kutafin Moscow State Law University (MSAL), Doctor of Military Science, Honored Worker of Science of the Russian Federation
namolchanov@msal.ru
123995, Russia, Moscow, Sadovaya-Kudrinskaya Street, 9

**MATEVOSOVA Elena Konstantinovna —** Senior Lecturer, Department of Theory of State and Law of the Kutafin Moscow State Law University (MSaL), PhD in Law
ekmatevosova@msal.ru
123995, Russia, Moscow, Sadovaya-Kudrinskaya Street, 9

***Review.*** *This article takes a look at topical issues of legal and institutional information security of Russia in the light of the doctrine of informational security of the Russian Federation, approved by the Decree of the President of the Russian Federation dated December 5, 2016 No646. Analyzing in detail the document of strategic planning, the authors point to the need for a qualitative improvement of the legal framework and mechanism of information security system in the light of new threats and challenges of the modern world. The objective assessment of a new law in legislation in the field of information security of the Russian Federation is accompanied by reflections on the problems of information security at the national and international level, responsibility for the effective resolution of which largely rests precisely on the law.*

***Keywords:*** *national security, sphere of information, information security, information security, international doctrine, strategic planning, information society, improving legislation, legal policy, information policy.*

**REFERENCES (TRANSLITERATION)**

1. Lapshin V.D. Formirovaniye sistemy mezhdunarodnoy informatsionnoy bezopasnosti: podkhody i initsiativy Rossii // Nauchnyye problemy natsional'noy bezopasnosti Rossiyskoy Federatsii / sost .: S.M. Buravlev i dr. M., 2015.