

УДК 342.9

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ:  
СУЩНОСТЬ, СОВРЕМЕННОЕ ЗНАЧЕНИЕ  
И ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ

В. В. Гриценко

Воронежский государственный университет

Поступила в редакцию 13 января 2017 г.

**Аннотация:** анализируется содержание доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646. Обосновывается понятие, сущность доктрины; раскрываются ее положительные и негативные стороны; аргументируется ее влияние на государственное управление; рассматриваются организационные основы системы обеспечения информационной безопасности России.

**Ключевые слова:** доктрина информационной безопасности, информационная безопасность, информационная сфера, организационные основы обеспечения информационной безопасности, органы исполнительной власти.

**Abstract:** the article analyzes the contents of Information Security Doctrine of the Russian Federation, approved by Presidential Decree of December 5, 2016 № 646. Substantiates the notion, the essence of the doctrine; reveals its positive and negative aspects; argues its impact on governance; considers organizational bases of Russian information security systems.

**Key words:** doctrine of information security, information security, information sphere, organizational bases of maintenance of information security, executive authorities.

Правовая доктрина, являясь разновидностью доктрин, оказывает в настоящее время все большее влияние на законотворческую, правоприменительную деятельность в государстве, а также «определяет стратегию и тактику законодательного развития соответствующей сферы, ее положения в дальнейшем развиваются в текущем законодательстве»<sup>1</sup>.

В словарях термин «доктрина» (от лат. *doctrina* – учение) интерпретируется по-разному. Например, в философском энциклопедическом словаре доктрина – это систематическое, политическое, идеологическое или философское учение, концепция, совокупность принципов<sup>2</sup>; в советском энциклопедическом словаре доктрина – учение, научная и философская теория, система, руководящий теоретический или политический принцип<sup>3</sup>; в толковом словаре русского языка доктрина – учение, научная

<sup>1</sup> Мадаев Е. О. Доктрина в правовой системе Российской Федерации : дис. ... канд. юрид. наук. Иркутск, 2012. С. 14.

<sup>2</sup> См.: Философский энциклопедический словарь. М., 2000. С. 142.

<sup>3</sup> См.: Советский энциклопедический словарь / гл. ред. А. М. Прохоров. 4-е изд.

концепция (обычно о философской, политической, идеологической теории)<sup>4</sup>. Таким образом, доктрина как наиболее устоявшееся понятие – это учение, концепция.

Существуют и другие мнения: например, под правовой доктриной понимается система идей, взглядов и положений основополагающего и концептуального характера, которые разрабатываются юридической наукой, опосредованы юридической практикой и которые в силу этого имеют общезначимый характер для правовой системы, так как основываются на общепризнанных принципах и ценностях, отражают закономерности и тенденции государственно-правового развития и, таким образом, формируют определенный тип правопонимания, в соответствии с которым функционирует и развивается российская правовая система<sup>5</sup>.

Правовые доктрины не являются источником российской правовой системы, наверное, поэтому в общетеоретическом аспекте им уделяется недостаточное внимание.

Справедливым представляется мнение Е. О. Мадаева, что в последние годы в российской политико-правовой практике доктрина приобрела устойчивый характер самостоятельного вида правового документа<sup>6</sup>.

Свидетельством тому являются семь действующих в Российской Федерации правовых доктрин, юридическая природа которых различна. Пять из них утверждены указами Президента РФ:

- доктрина развития российской науки<sup>7</sup>;
- морская доктрина Российской Федерации<sup>8</sup>;
- доктрина продовольственной безопасности Российской Федерации<sup>9</sup>;
- военная доктрина Российской Федерации<sup>10</sup>;
- доктрина информационной безопасности Российской Федерации<sup>11</sup> (далее – доктрина информационной безопасности РФ).

Две доктрины утверждены распоряжениями Правительства РФ: климатическая доктрина Российской Федерации<sup>12</sup> и экологическая доктрина Российской Федерации<sup>13</sup>.

Постановлением Правительства РФ от 29 марта 2014 г. № 245 «О признании утратившим силу некоторых актов Правительства Россий-

---

М., 1988. С. 404.

<sup>4</sup> См.: *Ожегов С. И., Шведова Н. Ю.* Толковый словарь русского языка : 80 000 слов и фразеологических выражений. 4-е изд., доп. М., 2004. С. 172.

<sup>5</sup> URL: <http://aldebaran.com.ru/publications/8848>

<sup>6</sup> См.: *Мадаев Е. О.* Доктрина в правовой системе Российской Федерации. С. 4.

<sup>7</sup> Собр. законодательства Рос. Федерации. 1996. № 25. Ст. 3005 ; 2006. № 9. Ст. 988.

<sup>8</sup> Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

<sup>9</sup> Собр. законодательства Рос. Федерации. 2010. № 5. Ст. 502.

<sup>10</sup> Рос. газета. 2014. 30 дек.

<sup>11</sup> Собр. законодательства Рос. Федерации. 2016. № 50. Ст. 7074.

<sup>12</sup> Там же. 2011. № 18. Ст. 2680 ; 2016. № 39. Ст. 5691.

<sup>13</sup> Там же. 2002. № 36. Ст. 3510.

ской Федерации»<sup>14</sup> прекратила существование национальная доктрина образования, которая была утверждена постановлением Правительства РФ от 4 октября 2000 г. № 751 «О национальной доктрине образования в Российской Федерации»<sup>15</sup>.

Следует подчеркнуть, что до утверждения доктрины информационной безопасности РФ (5 декабря 2016 г.) действовала доктрина информационной безопасности 2000 г. (далее – доктрина-2000), которая являлась характерной для того времени, не учитывала современных особенностей развития Российского государства применительно к нынешним условиям, и поэтому с апреля 2015 г. Совет Безопасности начал работу над новой доктриной, итогом которой стал указ Президента РФ, утвердивший доктрину информационной безопасности РФ.

Краткий анализ положений двух доктрин свидетельствует о том, что и они значительно отличаются друг от друга и по структуре, и по содержанию, и по объему (доктрина информационной безопасности РФ более чем на треть меньше доктрины-2000).

Структура доктрины-2000 включает: преамбулу (введение); четыре раздела и одиннадцать пунктов. В первом разделе определяются положения информационной безопасности Российской Федерации; во втором – методы обеспечения информационной безопасности Российской Федерации; в третьем – основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации; в четвертом – организационная основа системы обеспечения информационной безопасности Российской Федерации. Для данной доктрины присуща преамбула, в которой определялось понятие доктрины информационной безопасности и ее цели. В частности, отмечалось, что эта доктрина служит для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Структура доктрины информационной безопасности РФ состоит из пяти разделов: в первом разделе утверждаются общие положения; во втором – определяются национальные интересы в информационной сфере; в третьем – основные информационные угрозы и состояние информационной безопасности; в четвертом – стратегические цели и основные направления обеспечения информационной безопасности; в пятом – организационные основы обеспечения информационной безопасности.

В доктрине информационной безопасности РФ преамбула отсутствует, она включена первым пунктом в раздел общих положений, в котором

<sup>14</sup> Собр. законодательства Рос. Федерации. 2014. № 14. Ст. 1636.

<sup>15</sup> Там же. 2000. № 41. Ст. 4089.

определяется, что доктрина информационной безопасности представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. В указе Президента РФ подчеркивается, что его целью является обеспечение информационной безопасности.

В доктрине-2000 в более развернутой форме устанавливается, что доктрина – это совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности. При этом в обеих доктринах не раскрывается термин «официальных» взглядов.

Характеризуя обе доктрины, В. Макагонов подчеркивает, что в доктрине-2000 огромное внимание уделялось реализации прав и свобод граждан России на получение необходимой информации, новая доктрина делает основной упор на противостояние враждебным действиям зарубежных стран<sup>16</sup>.

Следует отметить, что в доктрине-2000 не давалось определения информационной сфере, лишь подчеркивалось, что информационная сфера является системообразующим фактором жизни общества и что она активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Учитывая важность данного термина, в информационной доктрине безопасности РФ под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет» (далее – 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.

К положительным моментам доктрины информационной безопасности РФ относится второй пункт, в котором перечисляются основные понятия, используемые в доктрине, например:

– национальные интересы в информационной сфере определяются как объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;

– угроза информационной безопасности Российской Федерации как совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

– 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 устойчи-

---

<sup>16</sup> URL: <https://www.griffon.media/articles/6/12/2016/information-security-in-rf>

вое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

– обеспечение информационной безопасности – осуществление взаимозавязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

– силы обеспечения информационной безопасности – государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

– средства обеспечения информационной безопасности – правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

– система обеспечения информационной безопасности – совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность и используемых ими средств обеспечения информационной безопасности;

– информационная инфраструктура Российской Федерации (далее – информационная инфраструктура) – совокупность объектов информатизации, информационных систем, сайтов в Интернете и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

Несмотря на то что перечень понятий является не полным, поскольку они указаны как «основные», представляется необходимым закрепление и других терминов, которые не вошли в этот перечень, но используются в данной доктрине и имеют ключевой, основополагающий характер. Например, к новеллам доктрины информационной безопасности РФ относится термин «отрасль информационных технологий и электронной промышленности». Данный термин используется в анализируемой доктрине пять раз, в частности:

– в п. 8 к национальным интересам в информационной сфере относится развитие в Российской Федерации отрасли информационных технологий и электронной промышленности;

– в п. 24 подчеркивается, что стратегическими целями обеспечения информационной безопасности в экономической сфере являются сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности;

– в п. 25 среди основных направлений обеспечения информационной безопасности в экономической сфере указывается инновационное развитие отрасли информационных технологий и электронной промышленности; повышение конкурентоспособности российских компаний, осуществляющих деятельность в отрасли информационных технологий и электронной промышленности;

– в п. 26 указывается, что стратегической целью обеспечения информационной безопасности в области науки, технологий и образования является поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности. Практически все положения доктрины информационной безопасности РФ посвящены (в той или иной мере) развитию новой отрасли информационных технологий и электронной промышленности. Выступая в 2016 г. с Посланием Федеральному Собранию РФ, Президент РФ В. В. Путин подчеркнул, что ИТ-индустрия – это одна из самых быстроразвивающихся отраслей, так как «совсем недавно ИТ-технологии составляли цифру, которая приближалась к нулю, сейчас – 7 миллиардов долларов»<sup>17</sup>. Думается, что нераскрытие данного термина в общих положениях является существенным недостатком анализируемой доктрины. Отметим, что данное понятие не использовалось и в доктрине-2000.

Отрасль информационных технологий занимает в экономике страны особое место, ее эффективное функционирование является одним из важнейших факторов, способствующих решению ключевых задач государственной политики<sup>18</sup>.

На наш взгляд, доктрина информационной безопасности РФ более совершенна по содержанию, чем доктрина-2000. Но и ей не удалось, к сожалению, избежать описательного характера, нечеткости, неконкретности определенных терминов, нарушений принципа научности, других специальных и общетеоретических принципов.

Необходимо подчеркнуть, что в юридической науке существуют три вида подходов к оценке правовых доктрин:

– положительный – например, Е. О. Мадаев подчеркивает, что доктрина как политико-правовой документ является важной составной частью законодательной системы Российской Федерации, определяя в настоящее время не только основы государственной политики, но и стратегию и тактику правового регулирования общественных отношений в сферах национальной безопасности и военного строительства, науки, образования, климата, экологии, морского дела, продовольственной и информационной безопасности, а также исходя из их содержания, в даль-

<sup>17</sup> Послание Президента Российской Федерации В. В. Путина Федеральному Собранию Российской Федерации // Рос. газета. 2016. 1 дек.

<sup>18</sup> О развитии информационных технологий в Российской Федерации и мерах поддержки отечественной ИТ-отрасли : постановление Совета Федерации Федерального Собрания РФ // Собр. законодательства Рос. Федерации. 2016. № 17. Ст. 2300.

нейшем строится вся правотворческая, в том числе законотворческая, правоинтерпретационная и правоприменительная практика в соответствующей сфере правового регулирования<sup>19</sup>;

– отрицательный – в частности, С. В. Бошко считает, что доктрины «засоряют пространство неясными произведениями»<sup>20</sup>; в какой-то степени с этим утверждением можно согласиться, так как основные положения доктрин носят декларативный, абстрактный характер, общеизвестно, что даже нормы законов не имеют механизмов их реализации;

– нейтральный – например, Г. Клименко считает, что доктрина – это обозначение целей для Правительства РФ, исполнительной власти; это программа, которая не может ни ухудшить, ни улучшить положение в стране<sup>21</sup>.

Думается, в настоящее время нельзя недооценивать роль доктрины информационной безопасности РФ, потому что как политико-правовой документ она выступает в качестве базы для правового регулирования информационной безопасности, основой государственной политики в установленной сфере.

Следует также отметить, что многие положения доктрины информационной безопасности РФ можно назвать доктринальными правилами, т.е. нормами. В частности, присутствуют доктринальные целеполагающие нормы. Например, термин «цели» используется более 25 раз. Так, по п. 11 одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

К доктринальным декларативным нормам можно отнести 28 положений о том, что стратегической целью обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

Доктринальные нормы-принципы определены в п. 34 доктрины, устанавливающей, что деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений;

б) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью

<sup>19</sup> См.: *Мадаев Е. О.* Доктрина в правовой системе Российской Федерации. С. 181.

<sup>20</sup> *Бошко С. В.* Доктрина как форма и источник права // Журнал рос. права. 2003. № 12. С. 77.

<sup>21</sup> URL: <http://www.bbc.com/russian/features-38225725>

обеспечения национальной безопасности, в том числе в информационной сфере;

г) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

По справедливому замечанию А. Б. Венгерова, информационная природа, прежде всего, заключается в том, что правовая норма – это персонафицированный сигнал и, следовательно, очень важен анализ перевода правовой информации в действия тех, к кому эта информация относится<sup>22</sup>. Любая правовая норма – это источник определенной информации для субъектов конкретных правоотношений.

Представляется, что при реальном действии положений доктрины информационной безопасности РФ она должна оказать положительное влияние на развитие в России эффективного государственного управления, под которым понимается деятельность органов государственной власти по реализации своих полномочий в сфере социально-экономического развития Российской Федерации и обеспечения национальной безопасности РФ<sup>23</sup> и на формирование в России информационного права в целом.

Итоги мероприятий по обеспечению информационной безопасности в Российской Федерации в 2016 г. и меры по ее укреплению являлись объектом рассмотрения на заседании Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности.

На фоне негативной тенденции нарастания угроз в информационной сфере подчеркнута актуальность решения задач по повышению защищенности информационных систем и сетей связи органов государственной власти Российской Федерации с использованием отечественных технических и программных средств обеспечения информационной безопасности. В качестве основной задачи на 2017 г. Межведомственной комиссией определена реализация положений доктрины информационной безопасности в РФ<sup>24</sup>.

Представляется неслучайным, что в проекте Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.<sup>25</sup>,

<sup>22</sup> См.: Венгеров А. Б. Теория государства и права : учебник. 6-е изд. М., 2009. С. 353.

<sup>23</sup> Собр. законодательства Рос. Федерации. 2014. № 26 (ч. 1). Ст. 3378 ; 2016. № 27 (ч. 1). Ст. 4210.

<sup>24</sup> URL: <http://www.scrf.gov.ru/news/1181.html>

<sup>25</sup> В период с 13 по 25 декабря 2016 г. на сайте Совета Безопасности Российской Федерации проводилось обсуждение проекта новой редакции Стратегии развития информационного общества в РФ, подготовленного Управлением Президента РФ по применению информационных технологий и развитию электронной демократии. В подготовке проекта участвовали представители государственных органов, Банка России, экспертного сообщества (URL: <http://www.scrf.gov.ru/news/1180.html>).

являющегося базой для определения целей, задач и мер внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий для развития информационного общества, формирования национальной цифровой экономики, реализации национальных интересов и стратегических национальных приоритетов, определенных Стратегией национальной безопасности Российской Федерации, учитываются положения Доктрины информационной безопасности РФ. Правовой основой данного проекта являются Конституция РФ, Федеральный закон от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации»<sup>26</sup>, в ст. 3 которого закрепляются понятия, используемые в данном законе. В целях единой терминологии представляется целесообразным дополнить их понятием доктрины информационной безопасности, данным в п. 1 указанной доктрины.

Таким образом, доктрина информационной безопасности представляет собой политико-правовой документ стратегического планирования в сфере обеспечения национальной безопасности России, разработанный Советом Безопасности, утвержденный указом Президента РФ, определяющий: доктринальные понятия, национальные интересы в информационной сфере; основные информационные угрозы и состояние информационной безопасности; стратегические цели, основные направления и организационные основы обеспечения информационной безопасности; и направленный на развитие отрасли информационных технологий и электронной промышленности.

Кроме того, данный документ создает концептуальную основу участия России в международном информационном поле, так как «у страны обновилось оружие для сопротивления в информационной войне, впервые официально признается выход сетевых угроз на уровень межгосударственного противостояния»<sup>27</sup>.

Особое значение в доктрине информационной безопасности РФ уделяется ее организационным основам (пятый раздел доктрины), в котором в «сжатом» варианте перечисляются: основы построения системы обеспечения информационной безопасности; органы, осуществляющие организационные основы; участники системы обеспечения информационной безопасности; принципы деятельности государственных органов по обеспечению информационной безопасности; задачи государственных органов в рамках деятельности по обеспечению информационной безопасности; задачи государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности и др.

Следует подчеркнуть роль органов исполнительной власти в сфере обеспечения информационной безопасности в России. Согласно п. 30 информационной доктрины безопасности РФ, система обеспечения инфор-

---

<sup>26</sup> Собр. законодательства Рос. Федерации. 2014. № 26 (ч. 1). Ст. 3378 ; 2016. № 27 (ч. 1). Ст. 4210.

<sup>27</sup> *Замахина Т.* Самое сильное оружие. В России – новая доктрина информационной безопасности // Рос. газета. 2016. 7 дек.

мационной безопасности – это часть системы обеспечения национальной безопасности Российской Федерации, состав которой определяется Президентом РФ.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

В п. 31 доктрины информационной безопасности РФ закрепляется, что система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов РФ, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Важным представляется положение об организационной основе системы обеспечения информационной безопасности, которую составляют: Совет Федерации Федерального Собрания РФ, Государственная Дума Федерального Собрания РФ, Правительство РФ, Совет Безопасности РФ, федеральные органы исполнительной власти, Центральный банк РФ, Военно-промышленная комиссия РФ, межведомственные органы, создаваемые Президентом РФ и Правительством РФ, органы исполнительной власти субъектов РФ, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

В данном разделе доктрины указывается на два вида задач:

– задачи государственных органов в рамках деятельности по обеспечению информационной безопасности (обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере; оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления; планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности; организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-розыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения; выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области);

– задачи государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности (укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи; совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений); совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности; повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности).

Большая часть указанных задач возлагается на органы исполнительной власти федерального и регионального уровней, а также их должностных лиц. По мнению Ю. Н. Старилова, орган исполнительной власти – это государственная организация, часть системы органов государственной власти в Российской Федерации, учрежденная самим государством для исполнения и обеспечения исполнения законов и иных нормативных правовых актов, реализации функций государственного управления во всех сферах жизни государства и общества посредством исполнения специальных форм и методов осуществления управленческих действий, обладающая соответствующей структурой, компетенцией, государственно-властными полномочиями и штатом государственных служащих<sup>28</sup>.

Именно от управленческой деятельности органов исполнительной власти, от эффективности их взаимодействия с другими государственными органами зависит реализация положений доктрины информационной безопасности в Российской Федерации, без административно-правовых норм, регулирующих правовой статус органов, здесь не обойтись, а значит, возрастает, в первую очередь, роль отрасли административного права.

---

88 <sup>28</sup> См.: Общее административное право : учебник : в 2 ч. / под ред. Ю. Н. Старилова. 2-е изд., пересмотр. и доп. Воронеж, 2016. Ч. 1. С. 234. См. также: Старилов Ю. Н. Система федеральных органов исполнительной власти : формирование в порядке транспарентного законодательства или правительственных процедур? // Вестник Воронеж. гос. ун-та. Серия: Право. 2016. № 3. С. 16–57.

*Воронежский государственный университет*

*Гриценко В. В., доктор юридических наук, профессор кафедры административного и муниципального права*

*E-mail: vvgritsenko@mail.ru*

*Тел.: 8-919-240-25-35*

*Voronezh State University*

*Gritsenko V. V., Doctor of Legal Sciences, Professor of the Administrative and Municipal Law Department*

*E-mail: vvgritsenko@mail.ru*

*Tel.: 8-919-240-25-35*