ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ПРАВА

УДК 34:002

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ ДОКТРИНАЛЬНЫХ ПОЛОЖЕНИЙ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Абдусаламов Р.А., Дагестанский государственный университет, г. Махачкала, Российская Федерация, *abd-rus@yandex.ru*

Магдилова Л. В., Дагестанский государственный университет, г. Махачкала, Российская Федерация, *maglar@mail.ru*

Рагимханова Д.А., Дагестанский государственный университет, г. Махачкала, Российская Федерация, *dinarus77@mail.ru*

Статья посвящена исследованию стратегических и доктринальных положений, отражающих современное состояние и направления развития правовых и организационных мер обеспечения информационной безопасности России. В результате анализа определены основные изменения в обеспечении информационной безопасности, отраженные в новой Доктрине информационной безопасности 2016 года, являющейся логическим продолжением Стратегии национальной безопасности РФ. Рассматриваются перспективы развития законодательства в области критической информационной инфраструктуры. Выделены основные нововведения, касающиеся: предотвращения террористической и экстремистской деятельности, связанной с информационным воздействием на индивидуальное, групповое и общественное сознание; развития отечественной ИТ-индустрии; повышения качества подготовки специалистов в области информационной безопасности; развития национальной системы управления российским сегментом сети «Интернет». В результате излагаются основные направления обеспечения информационной безопасности на современном этапе развития информационного общества, их развитие в нормативно-правовых актах, регулирующих информационную безопасность, в том числе в области стратегического международного сотрудничества.

Ключевые слова: информационное общество, информационные угрозы, информационные риски, информационно-правовая культура, доктрина информационной безопасности, критическая информационная инфраструктура.

DOI: 10.21779/2224-0241-2017-24-4-165-169

UDC 34:002

THE ISSUE OF IMPROVING THE DOCTRINAL ISSUES IN THE FIELD OF INFORMATION SECURITY

Abdusalamov R.A., Dagestan State University, Makhachkala, Russian Federation, *abd-rus@yandex.ru*

Magdilova L.V., Dagestan State University, Makhachkala, Russian Federation, *maglar@mail.ru*

Ragimkhanova D.A., Dagestan State University, Makhachkala, Russian Federation, *dinarus77@mail.ru*

The article is devoted to the study of strategic and doctrinal provisions reflecting the current state and directions of development of legal and organizational measures to ensure Russia's information security. As a result of the analysis, the main changes in the information security are reflected in the new Information Security Doctrine of 2016, which is a logical continuation of the National Security Strategy of the Russian Federation. Prospects of development of legislation in the field of critical information infrastructure are considered. The main innovations concerning: prevention of terrorist and extremist activities related to the information impact on individual, group and public consciousness; development of the domestic IT industry; improving the quality of training specialists in the field of information security; the development of a national management system for the Russian segment of the Internet. As a result, the main directions of ensuring information security at the present stage of the development of the information society, their development in regulatory and legal acts regulating information security, including in the field of strategic international cooperation, are outlined.

Key words: information society, information threats, information risks, information and legal culture, information security doctrine, critical information infrastructure.

DOI: 10.21779/2224-0241-2017-24-4-165-169

На современном этапе развития информационно-телекоммуникационных технологий особое внимание уделяется проблеме обеспечения информационной безопасности, которая представляет собой одну из областей информационной сферы, являющейся основой для развития информационного общества, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан [1]. Глобальное информационное пространство и возможности скрытого трансграничного оборота информации все чаще используются для достижения отдельными государствами и организациями геополитических, военно-политических, а также террористических, экстремистских и криминальных целей в ущерб стратегической стабильности и международной безопасности [2].

В этой связи немаловажное значение приобретает развитие международной информационной безопасности, для обеспечения которой создается система международных организаций, способствующих реализации действенных механизмов обеспечения информационной безопасности, деятельность которых основана на концептуальных документах и соглашениях о сотрудничестве в данной области [3].

Глобальные информационные системы — новая сфера для столкновения национальных интересов — потребовали от органов государственного управления инновационных подходов к противодействию угрозам информационной безопасности [4]. В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы к основным условиям формирования информационного пространства относится обеспечение создания и развития систем нормативно-правовой помощи в обнаружении, предупреждении, предотвращении и отражении угроз информационной безопасности. Стратегия национальной безопасности Российской Федерации [5] определяет, что национальная безопасность включает в себя все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего, государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности. Таким образом, законодатель относит информационную безопасность к числу видов национальной безопасности [6]. Среди главных условий укрепления национальной безопасности РФ ряд авторов называют создание системы государственной информационной безопасности, включающей весь спектр методов, средств и механизмов ее обеспечения [7, 8, 9]. Также необходимо отметить значимость принципа сбалансированных интересов личности, общества и государства в области обеспечения информационной безопасности, среди которых особое значение приобретает безопасное удовлетворение информационных потребностей граждан [10,11], их участие в управлении государством посредством современных информационных технологий [12].

На сегодняшний день в Российской Федерации принят ряд нормативно-правовых документов, регламентирующих механизм обеспечения информа-

ционной безопасности личности, общества и государства: Доктрина информационной безопасности РФ [13]; Конвенция об обеспечении международной информационной безопасности (концепция); Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры РФ; Основы государственной политики РФ в области международной информационной безопасности на период до 2020 года; Основные направления научных исследований в области обеспечения информационной безопасности РФ; Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ; Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» [14].

Особый интерес представляет Доктрина информационной безопасности Российской Федерации, утвержденная 5 декабря 2016 года указом Президента РФ. Данный документ пришел на смену Доктрине информационной безопасности РФ, утвержденной 9 сентября 2000 года, которая признается утратившей силу. Новая доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором развиваются положения Стратегии национальной безопасности Российской Федерации, а также других документов стратегического планирования в указанной сфере. В частности, текущее состояние и направления обеспечения информационной безопасности рассматриваются с позиций стратегических национальных приоритетов, обозначенных в Стратегии национальной безопасности РФ. В этой связи новая Доктрина является более структурированной и последовательной в сравнении с документом 2000 года. Таким образом, она не только является логическим продолжением Стратегии национальной безопасности РФ по своей направленности, но и по структуре, что позволит в перспективе выстраивать всю иерархию документов в сфере информационной безопасности с учетом соответствующих стратегических национальных приоритетов.

В документе 2000 года говорится о возрастающем влиянии информационных технологий на национальные интересы страны. В свою очередь, изменения, происшедшие за последние 16 лет в области развития информационно-телекоммуникационных технологий, повлияли на модернизацию административного управления, повысили качество и уровень жизни населения и рассматриваются уже как неотъемлемая часть всех сфер жизнедеятельности.

Положения новой Доктрины соответствуют актуальным тенденциям в сфере информационных технологий и информационной безопасности, действующим и вынесенным на рассмотрение нормативно-правовым актам в сфере разработки и производства программно-технических средств и информационно-телекоммуникационных технологий, обеспечения безопасности критически важной инфраструктуры РФ, противодействия кибератакам и иным актуальным вопросам.

В новой Доктрине развиты положения Стратегии национальной безопасности РФ, касающиеся: защиты интересов личности, общества и государства от осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств, осуществляющихся на основе противоборства в глобальном информационном пространстве; защиты функционирования критической информационной инфраструктуры РФ; осуществления мероприятий, направленных на предотвращение террористической и экстремистской деятельности, связанной с использованием информационных и коммуникационных технологий; развитие отечественных информационных систем и технологий, программно-технического обеспечения и средств информационной защиты.

В Доктрине информационной безопасности не отмечена неразвитость правовых основ обеспечения информационной безопасности, так как за последние два десятилетия принят целый пакет взаимосвязанных документов, регламентирующих информационно-правовые отношения в сфере создания и развития механизмов информационной безопасности. Однако так же, как и 16 лет назад, на недостаточном уровне остается развитие отечественных информационных технологий и средств их обеспечения, в связи с чем используются зарубежные аналоги, создающие угрозы информационной безопасности информационных систем, в том числе объектам критической информационной инфраструктуры.

Понятие критически важного объекта было определено в законодательстве РФ еще в 1994 году в Федеральном законе от 21.12.1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» [15]. На следующий день после принятия Доктрины информационной безопасности, то есть 6 декабря 2016 года, в Госдуму был внесен на рассмотрение проект федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», который был официально опубликован 26 июля 2017 года под № 187 и вступит в силу 1 января 2018 года. Важным является тот факт, что впервые такие понятия, как «критическая информационная инфраструктура», «значимый объект критической информационной инфраструктуры», «субъекты критической информационной инфраструктуры» закреплены на уровне федерального закона. В развитие норм закона планируется принятие подзаконных нормативных актов, которые вместе с федеральным законом и уже существующими документами (Концепция государственной системы обнаружения, предотвращения и ликвидации последствий компьютерных атак (ГосСОПКА), Руководящий документ «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утвержденный Федеральной службой по техническому и экспортному контролю (ФСТЭК России) и др.) образуют целый свод норм и правил, регулирующих защиту критической информационной инфраструктуры РФ. ФСТЭК России может стать ответственной за обеспечение безопасности критической информационной инфраструктуры РФ. В соответствии с феде-

ральным законом «О безопасности критической информационной инфраструктуры РФ» основными полномочиями такого органа являются ведение реестра значимых объектов критической информационной инфраструктуры, установление требований по обеспечению безопасности таких объектов, а также осуществление госконтроля в области обеспечения их безопасности.

Продолжая сравнительный анализ Доктрин информационной безопасности 2000 и 2016 годов, можно отметить некоторые схожие положения:

- определены национальные интересы РФ в информационной сфере, которые практически не отличаются по смысловому содержанию в двух редакциях, с той лишь разницей, что в 2000 году они сгруппированы для личности, общества и государства, а в 2016 году такая классификация отсутствует;

- к угрозам информационной безопасности доктринами отнесены действия, направленные на нарушение 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; информационно-психологическое воздействие на групповое и общественное сознание, приводящее к подрыву суверенитета и территориальной целостности государства; искажение положений государственной информационной политики РФ.

В новой Доктрине особое внимание уделяется угрозам, связанным с широким использованием различными террористическими и экстремистскими организациями механизмов информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

Наряду с этим подчеркивается, что создание благоприятных условий для осуществления деятельности на территории Российской Федерации российских ИТ-компаний должно являться одним из основных направлений развития экономической сферы обеспечения информационной безопасности страны. Эти меры должны позволить увеличить долю продукции отрасли информационных технологий в валовом внутреннем продукте, а также в структуре экспорта страны.

Нововведением Доктрины информационной безопасности РФ 2016 года являются задачи государственных органов в рамках деятельности по развитию и совершенствованию организационных основ обеспечения информационной безопасности, среди которых: укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных си-

стем 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.

Особое внимание в новой Доктрине уделено развитию национальной системы управления российским сегментом сети «Интернет» с целью улучшения состояния информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства. Эти положения находят свое развитие в Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, в которой среди основных мероприятий международного уровня для развития сети «Интернет» и информационной инфраструктуры РФ обозначены: обеспечение суверенного права государства определять информационную, технологическую и экономическую политику в национальном сегменте Интернета; предотвращение попытки использования Интернета в военных целях; развитие Интернета как интегрального источника знаний; разработка международно-правовых стандартов функционирования и развития Интернета; создание механизмов, обеспечивающих конфиденциальность и личную безопасность пользователей, предотвращающих анонимность и безнаказанность правонарушителей в Интернете; интеграция российских стандартов в сфере информационных и коммуникационных технологий в соответствующие международные стандарты.

В соответствии с Доктриной развитие кадрового потенциала в области обеспечения информационной безопасности также является актуальной задачей, а обеспечение защиты интересов граждан в ин-

формационной сфере должно также включать формирование информационной культуры.

В новой версии Доктрины отсутствуют разделы, касающиеся обеспечения информационной безопасности РФ в сфере духовной жизни, в общегосударственных информационных и телекоммуникационных системах, в правоохранительной и судебной сферах, а также раздел, описывающий положения государственной политики обеспечения информационной безопасности РФ. Направления международного сотрудничества затронуты в разделе, посвященном основным направлениям обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства.

Нововведением документа является то, что наряду с органами власти различного уровня, участниками системы обеспечения информационной безопасности признаются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты; средства массовой информации и массовых коммуникаций; организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка; операторы связи; операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности; организации, осуществляющие образовательную деятельность в данной области; общественные объединения; иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Таким образом, новая Доктрина информационной безопасности РФ развивает положения предыдущей версии документа, перестала носить общий и декларативный характер и стала конкретной и направленной в сторону совершенствования национальной безопасности.

Литература

1. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента Рос. Федерации от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 20, ст. 2901.
2. Ищенко А.Н., Прокопенко А.Н., Страхов А.А. Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере // Проблемы правоохранительной деятельности. 2017. № 2. С. 55–62.
3. Чеботарева А.А. Обеспечение информационной безопасности личности: роль международной информационной безопасности и стратегического партнерства // Вестник Академии права и управления. 2016. № 42. С. 48–51.
4. Косов Ю.В. Информационная безопасность и международное право // Управленческое консультирование. 2016. № 3 (87). С. 209–211.
5. О Стратегии национальной безопасности Российской Федерации: указ Президента Рос. Федерации от 31 дек. 2015 г. № 683 // Собр. законодательства Рос. Федерации. 2016. № 1, ч. II, ст. 212.
6. Анохина С.Ю., Логинова Т.Д. Информационная безопасность как основной элемент системы национальной безопасности // Алтайский юридический вестник. 2016. № 16. С. 21–25.
7. Сулимин А.Н. Информационная безопасность России и угрозы глобального информационного сообщества // Каспийский регион: политика, экономика, культура. 2016. № 1 (46). С. 98–104.
8. Маслакова Е.А. Проблемы обеспечения информационной безопасности как составной части национальной безопасности Российской Федерации // Военно-юридический журнал. 2016. № 7. С. 20–23.

9. Алексеева Е.В. Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере // Ленинградский юридический журнал. 2016. № 4 (46). С. 97–103.
10. Чеботарева А.А. Информационная безопасность личности в системе информационных прав и свобод // Вестник Московского городского педагогического университета. Сер.: Юридические науки. 2015. № 4 (20). С. 73–77.
11. Магдилова Л.В. Правовые основы обеспечения информационной безопасности несовершеннолетних // Юридический вестник ДГУ. 2017. Т. 23. № 3. С. 104–108.
12. Федотова Ю.Г. Электронная демократия как средство обеспечения информационной безопасности государства // Информационное право. 2016. № 3. С. 17–24.
13. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Рос. Федерации от 5 дек. 2016 г. № 646 // Собр. законодательства Рос. Федерации. 2016. № 50, ст. 7074.
14. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ // Собр. законодательства Рос. Федерации. 2017. № 31, ч. I, ст. 4736.
15. Баныщикова З.Е., Глебов В.Ю., Кориунов С.С. Нормативно-правовые аспекты, влияющие на деятельность государственных органов исполнительной власти в области защиты населения и территорий от чрезвычайных ситуаций на критически важных объектах // Технологии гражданской безопасности. 2017. Т. 14. № 1 (51). С. 24–28.

References

1. O Strategii razvitiya informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017–2030 gody: ukaz Prezidenta Ros. Federatsii ot 9 maya 2017 g. № 203 // Sobr. zakonodatel'stva Ros. Federatsii. 2017. № 20, st. 2901.
2. Ishchenko A.N., Prokopenko A.N., Strakhov A.A. Novaya doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii kak osnova protivodeistviya ugrozam bezopasnosti Rossii v informatsionnoi sfere // Problemy pravookhranitel'noi deyatel'nosti. 2017. № 2. S. 55–62.
3. Chebotareva A.A. Obespechenie informatsionnoi bezopasnosti lichnosti: rol' mezhdunarodnoi informatsionnoi bezopasnosti i strategicheskogo partnerstva // Vestnik Akademii prava i upravleniya. 2016. № 42. S. 48–51.
4. Kosov Yu.V. Informatsionnaya bezopasnost' i mezhdunarodnoe pravo // Upravlencheskoe konsul'tirovanie. 2016. № 3 (87). S. 209–211.
5. O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii: ukaz Prezidenta Ros. Federatsii ot 31 dek. 2015 g. № 683 // Sobr. zakonodatel'stva Ros. Federatsii. 2016. № 1, ch. II, st. 212.
6. Anokhina S.Yu., Loginova T.D. Informatsionnaya bezopasnost' kak osnovnoi element sistemy natsional'noi bezopasnosti // Altaiskii yuridicheskii vestnik. 2016. № 16. S. 21–25.
7. Sulimin A.N. Informatsionnaya bezopasnost' Rossii i ugrozy global'nogo informatsionnogo soobshchestva // Kaspiiskii region: politika, ekonomika, kul'tura. 2016. № 1 (46). S. 98–104.
8. Maslakova E.A. Problemy obespecheniya informatsionnoi bezopasnosti kak sostavnoi chasti natsional'noi bezopasnosti Rossiiskoi Federatsii // Voenno-yuridicheskii zhurnal. 2016. № 7. S. 20–23.
9. Alekseeva E.V. Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii kak klyuchevoi aspekt pravovogo obespecheniya natsional'noi bezopasnosti v informatsionnoi sfere // Leningradskii yuridicheskii zhurnal. 2016. № 4 (46). S. 97–103.
10. Chebotareva A.A. Informatsionnaya bezopasnost' lichnosti v sisteme informatsionnykh prav i svobod // Vestnik Moskovskogo gorodskogo pedagogicheskogo universiteta. Ser.: Yuridicheskie nauki. 2015. № 4 (20). S. 73–77.
11. Magdilova L.V. Pravovye osnovy obespecheniya informatsionnoi bezopasnosti nesovershennoletnikh // Yuridicheskii vestnik DGU. 2017. Т. 23. № 3. С. 104–108.
12. Fedotova Yu.G. Elektronnaya demokratiya kak sredstvo obespecheniya informatsionnoi bezopasnosti gosudarstva // Informatsionnoe pravo. 2016. № 3. S. 17–24.
13. Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii: ukaz Prezidenta Ros. Federatsii ot 5 dek. 2016 g. № 646 // Sobr. zakonodatel'stva Ros. Federatsii. 2016. № 50, st. 7074.
14. O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii: feder. zakon Ros. Federatsii ot 26 iyulya 2017 g. № 187-FZ // Sobr. zakonodatel'stva Ros. Federatsii. 2017. № 31, ch. I, st. 4736.
15. Ban'shchikova Z.E., Glebov V.Yu., Korshunov S.S. Normativno-pravovye aspekty, vliyayushchie na deyatel'nost' gosudarstvennykh organov ispolnitel'noi vlasti v oblasti zashchity naseleniya i territorii ot chrezvychnykh situatsii na kriticheski vazhnykh ob'ektakh // Tekhnologii grazhdanskoi bezopasnosti. 2017. Т. 14. № 1 (51). С. 24–28.

Поступила в редакцию 22 ноября 2017 г.
Received 22 November, 2017