УДК 342
DOI 10.32326/19931778_2024_5_163

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОЙ РОССИИ: ОТ КРИТИКИ СОДЕРЖАНИЯ ПРАВА К ПРАВОВЫМ ПОСЛЕДСТВИЯМ

Н.А. Трусов

Нижегородская академия МВД России, Н. Новгород
Приволжский филиал Российского государственного университета правосудия, Н. Новгород

nikevor@yandex.ru

Поступила в редакцию 10.08.2024

Представлен критический анализ содержания Доктрины информационной безопасности Российской Федерации от 5 декабря 2016 года в попытке определить правовые последствия выявленных недостатков. В результате проведенного исследования его гипотеза о том, что вопросам правового обеспечения информационной безопасности Российской Федерации нашими органами публичной власти уделяется недостаточное внимание, получила свое подтверждение. Автором делается вывод, что наличие документа стратегического планирования в информационной сфере без должного внимания к дефинитивному ряду, иным вопросам юридической техники, без должного осуществления в отношении него мониторинга снижает потенциал его реализации. Отдельные формулировки национальных интересов России в информационной сфере Доктрины информационной безопасности Российской Федерации 2016 года нуждаются в редакции, поскольку закрепленный аморфный предмет интереса, нивелируя сам интерес, обусловливает отсутствие правовых последствий его обеспечения, реализации и защиты.

Ключевые слова: информация, информационная безопасность, правовое обеспечение безопасности, критика содержания права, правовые последствия.

Современный этап общественного развития характеризуется все большим проникновением информационно-телекоммуникационных технологий в жизнь личности, общества и государства. Казалось бы, еще недавно фраза «мы живем в век информационных технологий» звучала позитивно футуристично и не воспринималась большинством как уже достигнутое состояние, а только лишь приближающееся. Поэтому и в общественном сознании возрастающая роль информации не переходила в разряд реальных угроз, в связи с чем приготовление к их купированию «можно было и отложить». Уже сегодня все та же фраза поменяла оттенки своего восприятия на негативный. Мы уже столкнулись с угрозами и последствиями нашего «отлагательного» приготовления к ним и находимся сейчас в «догоняющем» состоянии. Начало Россией специальной военной операции на Украине резко обострило наши недоработки по обеспечению информационной безопасности: тысячи обманутых граждан России перевели десятки миллиардов рублей украинским телефонным мошенникам, информационные технологии социальных сетей позволили нашим «оппонентам» идейно «раскачивать» наше общество изнутри, смоделировать негативный компонент восприятия проводимой Россией внутренней и внешней политики, информационный компонент «прокси-войны» был полностью проигран в начальной стадии вооруженного противостояния.

Сегодня стало очевидным, что наш «век информационных технологий» характеризуется все возрастающей ролью информационного воздействия во всех и на все сферы жизнедеятельности личности, общества и государства. В связи с этим вопросы и проблематика обеспечения национальной безопасности нашего государства все больше зависят от эффективного обеспечения ее системного элемента (подсистемы) – информационной безопасности России.

Практика показывает, что существенное значение в вопросах обеспечения различных составляющих национальной безопасности имеет состояние их правового обеспечения. Все это обусловливает не только актуальность, но и практическую значимость работ, посвященных правовому обеспечению информационной безопасности Российской Федерации.

Гипотезой нашего исследования является утверждение о том, что вопросам правового обеспечения информационной безопасности Российской Федерации нашими органами публичной власти уделяется недостаточное внимание. В частности, действующий документ стратегического планирования в области обеспечения информационной безопасности – Доктрина информационной безопасности Российской Федерации (далее по тексту – Доктрина) была

утверждена в 2016 году [1]. Юридическим последствием ее принятия стала утрата юридической силы ранее действовавшей Доктрины информационной безопасности Российской Федерации 2000 года [2]. За 16 лет действия Доктрины 2000 года наша страна смогла восстановить экономику, что позволило ей в целом спокойно пройти мировой финансовый кризис 2008 года и экономические санкции, последовавшие в отношении нашей страны за воссоединение ее с Крымом, восстановить армию, которая стала способна проводить серьезные военные операции на чужой территории, например в Грузии в 2008 году, обеспечить широкополосный Интернет по всей стране и так далее. Страна 2016 года совершенно не похожа на Россию 2000 года, которой предрекали распад в 2001 году. Однако при этом с точки зрения правового обеспечения информационной безопасности ничего (!) не произошло. Изменений и дополнений «доктринального документа» не было!

Доктрина 2016 года уже действует 7.5 лет также без изменений. При этом за это время наша страна преодолела ограничения карантинных мероприятий, а с 2022 года столкнулась с мощнейшим информационным (и не только) противостоянием со стороны США и стран Западной Европы. Представляется, что такое положение в вопросе правового обеспечения информационной безопасности в современных геополитических условиях не может быть ничем оправданным. Вряд ли стоит ожидать еще 8.5 лет, чтобы обновить Доктрину 2016 года. Хотелось бы заметить, что действующий «доктринальный документ» изначально не был принят с существенной «нормативной перспективой» и является на настоящий момент не свободным от критики.

В настоящей работе мы попытались с критической точки зрения взглянуть на содержание Доктрины информационной безопасности Российской Федерации от 5 декабря 2016 года и определить правовые последствия выявленных недостатков.

Первое, что обращает на себя внимание, это то, что Доктрина 2016 года в своем содержании ссылается на устаревшую Стратегию национальной безопасности Российской Федерации от 31 декабря 2015 года (п. 5 Доктрины), которая была отменена Указом Президента РФ от 2 июля 2021 года «О Стратегии национальной безопасности Российской Федерации» [3]. Казалось бы, это несущественно с точки зрения содержания и реализации: и так понятно, что надо учитывать «новую Стратегию»! Однако именно это наглядно демонстрирует интенсивность обращения к рассматриваемому документу стратегического планирования и качество осуществляемого в отношении него мониторинга, а значит, и реализации.

Второе. Понятийный ряд Доктрины 2016 года не соответствует легальным определениям, содержащимся в более общих документах стратегического планирования. Заметим, что понятие информационной безопасности в науке имеет множество подходов к своему определению. Многое зависит от объекта безопасности, предметной сферы приложения, уровня территориальной организации. Применительно к информационной безопасности Российской Федерации в науке встречаются следующие определения:

– «состояние защищённости интересов личности, общества и государства в информационном пространстве от преднамеренных или случайных воздействий, нарушающих целостность, объективность, доступность, конфиденциальность и оперативность самой информации или информационно-телекоммуникационной инфраструктуры» [4, с. 17];

– «состояние информационных источников, предполагающее их эффективную защиту от воздействия угроз при получении, обработке, хранении и передаче информации, посредством обеспечения доступности, целостности и конфиденциальности информации при реализации акторами мер защиты информации частного, государственного и межгосударственного характера» [5, с. 157–158];

– «состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам)» [6, с. 15];

– «защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры» [7, с. 18].

Можно привести и иные примеры, хотя и представленных вполне достаточно для того, чтобы понять наличие широкого и узкого подходов к определению рассматриваемого феномена. Широкое понимание является наиболее близким к легальному определению, которое содержится в п. 2 Доктрины 2016 года, а именно – «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 со-

циально-экономическое развитие Российской Федерации, оборона и безопасность государства». Данное определение в целом соответствовало ранее существовавшему (до 2021 года) подходу к определению родового понятия – национальной безопасности Российской Федерации. Стратегия национальной безопасности Российской Федерации 2021 года [3] изменила подход с триединого определения объекта обеспечения безопасности (личность, общество и государство) на единый объект – национальные интересы Российской Федерации, которые, в свою очередь, представляют собой «объективно значимые потребности личности, общества и государства в безопасности и устойчивом развитии» (п. 5 Стратегии 2021 года). В этой связи корректнее было бы сегодня определять информационную безопасность России через состояние защищенности национальных интересов Российской Федерации в информационной сфере.

Более того, если раскрывать легальное определение понятия «информационная безопасность Российской Федерации» через понимание составляющих его ключевых терминов, то в легальном определении вообще произойдет путаница объектов обеспечения, поскольку «информационные угрозы» раскрываются через «национальные интересы в информационной сфере», которые, в свою очередь, понимаются как потребности личности, общества и государства в части, касающейся информационной сферы.

Кроме этого, Доктрина 2016 года использует устаревшее понятие «силы обеспечения безопасности» (использовалось до декабря 2015 года [8]), хотя пытается определять их более корректно, чем было ранее, через перечень органов и организаций. Но и здесь не без нюансов. В отличие от Стратегии 2015 года, положения которой должны бы развиваться в Доктрине 2016 года (п. 5 Доктрины 2016 года), к силам обеспечения информационной безопасности последняя относит «государственные органы, а также подразделения и должностных лиц государственных органов, органов местного самоуправления и организаций», в то время как Стратегия 2015 года – органы государственной власти и органы местного самоуправления. Логично возникает вопрос о соотношении терминов «органы государственной власти» и «государственные органы», что, учитывая положения конституционно-правовой и административно-правовой наук, не в пользу Доктрины 2016 года. Заметим, что Стратегия 2021 года при определении системы обеспечения национальной безопасности использовала более общий термин – органы публичной власти, что автоматически избавляет ее от научных «критических стрел» в этом вопросе.

Третье. Указанное выше не является единственным недостатком легального определения рассматриваемого понятия. Дело в том, что сформулированные в нем цели обеспечения информационной безопасности, а именно 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, являются целями обеспечения родового понятия и более общего феномена «национальной безопасности Российской Федерации» (п. 5 Стратегии 2021 года), которая в рассматриваемом определении также перечисляется в его конце. Получается дефинитивная тавтология.

Эта же «тавтология» встречается и в п. 9 Доктрины 2016 года, в котором перечисляются цели реализации национальных интересов в информационной сфере. К ним опять-таки относятся обеспечение конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации, которая, как уже отмечалось, сама преследует цель «реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны» (п. 5 Стратегии 2021 года).

Четвертое. Согласно Доктрине 2016 года (п. 8, пп. «а») одним из национальных интересов России в информационной сфере является «применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации». Не совсем понятно: о каких таких духовно-нравственных ценностях многонационального народа Российской Федерации идет речь? Может, о ценностях одного из более 190 народов, народностей, этносов и этнических групп, проживающих в современной России? Или, может, о ценностях, которые разделяются всеми, т.е. многонациональным народом России? Тогда, вероятнее всего, следовало бы уточнить, о каких именно ценностях идет речь: о современных или о традиционных? Когда тысячи наших граждан после начала мобилизации осенью 2022 года спешно покинули нашу страну, ссылаясь на то, что они «люди мира» и против войны, это можно рассматривать как современную

ценность многонационального народа России или нет? Так и получается, что аморфный предмет интереса, нивелируя сам интерес, обусловливает отсутствие правовых последствий его обеспечения, реализации и защиты.

В этой связи предлагается внести изменение в пункт 8, пп. «а» Доктрины 2016 года, заменив рассматриваемую формулировку на «применение информационных технологий в интересах сохранения традиционных российских духовно-нравственных и культурно-исторических ценностей». В этой редакции формулировка национального интереса России в информационной сфере будет соответствовать пунктам 25, 26, 87, 91 и др. Стратегии национальной безопасности Российской Федерации 2021 года [3], Основам государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей 2022 года [9], пунктам 5, 8, 9 и др. Основ государственной политики Российской Федерации в области исторического просвещения 2024 года [10].

Нельзя не отметить, что собственно формулировка «традиционные российские духовно-нравственные ценности» не является чуждой для действующей Доктрины информационной безопасности России 2016 года. В частности, она упоминается в ее пункте 12 среди основных информационных угроз и пункте 23 среди основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности. В этой связи причины использования аморфной формулировки при формулировании национального интереса остаются непонятными.

Таким образом, гипотеза нашего исследования получила свое подтверждение. Наличие документа стратегического планирования в информационной сфере без должного внимания к дефинитивному ряду, иным вопросам юридической техники, без должного осуществления в отношении него мониторинга снижает потенциал его реализации. Отдельные формулировки национальных интересов России в информационной сфере Доктрины информационной безопасности Российской Федерации 2016 года нуждаются в редакции, поскольку закрепленный аморфный предмет интереса, нивелируя сам интерес, обусловливает отсутствие правовых последствий его обеспечения, реализации и защиты. Все это в конечном счете не может не сказываться на состоянии обеспеченности национальной безопасности страны в целом.

Список литературы

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

2. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Российская газета. 28.09.2000. № 187.

3. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (часть II). Ст. 5351.

4. Шариков П.А. Политика США в области информационной безопасности: Автореф. дис. … канд. полит. наук. М., 2009. 38 с.

5. Идрисов Х.В. Информационная безопасность как один из элементов национальной безопасности // Международный журнал прикладных наук и технологий Integral. 2021. № 2. С. 152–163.

6. Вострецова Е.В. Основы информационной безопасности: Учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019. 204 с.

7. Гафнер В.В. Информационная безопасность: Учебное пособие в 2 ч. Ч. 1. Екатеринбург: ГОУ ВПО «Урал. гос. пед. ун-т», 2009. 155 с.

8. Трусов Н.А. Общая характеристика субъектов обеспечения национальной безопасности России // Совершенствование деятельности органов государственной власти, местного самоуправления и институтов гражданского общества в сфере обеспечения национальной безопасности: Сборник материалов XVIII Международной научно-практической конференции (24 ноября 2016 года). М.: Академия управления МВД России, Оперативное управление МВД России, ГУ МВД России по противодействию экстремизму, Институт социологии РАН, 2016. С. 326–329.

9. Указ Президента РФ от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» // СЗ РФ. 2022. № 46. Ст. 7977.

10. Указ Президента РФ от 08.05.2024 № 314 «Об утверждении Основ государственной политики Российской Федерации в области исторического просвещения» // СЗ РФ. 2024. № 20. Ст. 2587.

LEGAL PROVISION OF INFORMATION SECURITY IN MODERN RUSSIA: FROM CRITICISM OF THE CONTENT OF LAW TO LEGAL CONSEQUENCES

N.A. Trusov

The article presents a critical analysis of the content of the «Information Security Doctrine of the Russian Federation» dated December 5, 2016 in an attempt to determine the legal consequences of the identified shortcomings. As a result of the conducted research, his hypothesis that insufficient attention is paid to the issues of legal provision of information security of the Russian Federation by our public authorities has been confirmed. The author concludes that the presence of a strategic planning document in the information sphere without due attention to the definitive series,

other issues of legal technology, without proper monitoring of it reduces the potential for its implementation. Certain formulations of Russia's national interests in the information sphere of the Information Security Doctrine of the Russian Federation in 2016 need to be revised, since the fixed amorphous object of interest, leveling the interest itself, causes the absence of legal consequences for its provision, implementation and protection.

Keywords: information, information security, legal security, criticism of the content of the law, legal consequences.

References

1. Decree of the President of the Russian Federation dated 05.12.2016 № 646 «On approval of the Information Security Doctrine of the Russian Federation» // CL RF. 2016. № 50. Art. 7074.

2. The Doctrine of information security of the Russian Federation (approved by the President of the Russian Federation 09.09.2000 № Pr-1895) // Rossiyskaya Gazeta. 28.09.2000. № 187.

3. Decree of the President of the Russian Federation dated 07.02.2021 № 400 «On the National Security Strategy of the Russian Federation» // CL RF. 2021. № 27 (Part II). Art. 5351.

4. Sharikov P.A. U.S. policy in the field of information security: Abstract of the Candidate of Political Sciences. M., 2009. 38 p.

5. Idrisov H.V. Information security as one of the elements of national security // International Journal of Applied Sciences and Technologies «Integral». 2021. № 2. P. 152–163.

6. Vostretsova E.V. Fundamentals of information security: a textbook for university students. Yekaterinburg: Ural University Press, 2019. 204 p.

7. Gafner V. V. Information security: a textbook in 2 parts. State Educational Institution of Higher Education "Ural State Pedagogical University". Yekaterinburg, 2009. Part 1. 155 p.

8. Trusov N.A. General characteristics of the subjects of ensuring national security of Russia // Improving the activities of state authorities, local governments and civil society institutions in the field of national security: a collection of materials from the XVIII International Scientific and Practical Conference (November 24, 2016). Moscow: Academy of Management of the Ministry of Internal Affairs of Russia, Operational Directorate of the Ministry of Internal Affairs of Russia, GU of the Ministry of Internal Affairs of Russia on countering extremism, Institute of Sociology of the Russian Academy of Sciences, 2016. P. 326–329.

9. Decree of the President of the Russian Federation dated 11.19.2022 № 809 «On approval of the Foundations of State Policy for the preservation and strengthening of traditional Russian spiritual and moral values» // CL RF. 2022. № 46. Art. 7977.

10. Decree of the President of the Russian Federation dated 05.08.2024 № 314 «On approval of the Foundations of the State policy of the Russian Federation in the field of historical education» // CL RF. 2024. № 20. Art. 2587.