УДК 359:681
DOI https://doi.org/10.17308/vsu.proc.law.2021.3/3552

ЧЕТВЕРТЫЙ ПРИОРИТЕТ: ПРАВОВОЕ ЗАКРЕПЛЕНИЕ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В НОВОЙ СТРАТЕГИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

А. А. Смирнов

Антитеррористический центр государств – участников СНГ

Поступила в редакцию 25 июля 2021 г.

Аннотация: *анализируются положения новой Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 2 июля 2021 г., касающиеся обеспечения информационной безопасности. Подчеркивается значимость признания информационной безопасности стратегическим национальным приоритетом. Рассматриваются правовые механизмы обеспечения информационной безопасности, заложенные в базовом документе стратегического планирования в области безопасности.*
Ключевые слова: *цифровая эпоха, информационная безопасность, стратегия, приоритет, правовые механизмы.*

Abstract: *the article analyzes the provisions of the new National Security Strategy of the Russian Federation, approved by the Decree of the President of the Russian Federation of July 2, 2021, concerning information security. The importance of recognizing information security as a strategic national priority is emphasized. The legal mechanisms for ensuring information security, laid down in the basic document of strategic planning in the field of security, are considered.*
Key words: *digital era, information security, strategy, priority, legal mechanisms.*

Цифровая эпоха наряду с уникальными возможностями для развития человечества и социального прогресса породила множество новых угроз и вызовов. К их числу относятся риски ведения информационных войн между государствами, использования информационно-коммуникационных технологий для вмешательства во внутренние дела государств, в террористических и экстремистских целях, а также для совершения преступлений и иных правонарушений.

Осознание опасности информационных угроз привело к выработке на уровне национальных государств и международного сообщества комплекса мер по противодействию им. В Российской Федерации в 2000 г. впервые был принят отдельный документ стратегического планирования в данной сфере – Доктрина информационной безопасности Российской Федерации. В ней подчеркивалась системообразующая роль информационной сферы и ее влияние на другие сферы безопасности, на основе чего делался следующий вывод: «национальная безопасность Российской

Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать»[1].

В 2016 г. была утверждена новая Доктрина информационной безопасности Российской Федерации»[2], которая определила перечень основных информационных угроз, приоритетные задачи, направления и механизмы обеспечения информационной безопасности. Принятие новой Доктрины было вполне обоснованным шагом, поскольку за прошедшие 16 лет информационная среда изменилась самым радикальным образом.

Вместе с тем на протяжении длительного времени недооценка значимости информационной безопасности как вида безопасности наблюдалась и в экспертном сообществе, и на официальном уровне[3]. В базовых документах стратегического планирования в области национальной безопасности, начиная с Концепции национальной безопасности 1997 г.[4] и заканчивая Стратегией национальной безопасности 2015 г.[5], информационная безопасность не выделялась в числе приоритетных направлений, хотя тенденция усиления новых информационных угроз все же прослеживалась в тексте этих документов.

Ситуация принципиально изменилась с принятием новой Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента 2 июля 2021 г. № 400[6] (далее – Стратегия). В новом базовом документе стратегического планирования информационная безопасность выделена в качестве четвертого стратегического национального приоритета, т. е. важнейшего направления обеспечения национальной безопасности. Данный приоритет направлен на обеспечение реализации национальных интересов Российской Федерации, связанных с развитием безопасного информационного пространства, защитой российского обще-

[1] Доктрина информационной безопасности Российской Федерации : утв. Указом Президента РФ от 9 сентября 2000 г. № Пр-1895, утратила силу // Рос. газета. 2000. 28 сент.

[2] Доктрина информационной безопасности Российской Федерации : утв. Указом Президента РФ от 5 декабря 2016 г. № 646 // Собр. законодательства Рос. Федерации. 2016. № 50. Ст. 7074.

[3] См.: *Смирнов А. А.* Проблемы обеспечения информационно-психологической безопасности России на современном этапе // Национальная безопасность : научное и государственное управленческое содержание : материалы Всероссийской науч. конф. (Москва, 4 декабря 2009 г.). М., 2010. С. 897–907.

[4] Концепция национальной безопасности : утв. Указом Президента РФ от 17 декабря 1997 г. № 1300, утратила силу // Собр. законодательства Рос. Федерации. 1997. № 52. Ст. 5909.

[5] Стратегия национальной безопасности Российской Федерации : утв. Указом Президента РФ от 31 декабря 2015 г. № 683, утратила силу // Собр. законодательства Рос. Федерации. 2016. № 1 (ч. 2). Ст. 212.

[6] Стратегия национальной безопасности Российской Федерации : утв. Указом Президента РФ от 2 июля 2021 г. № 400 // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202107030001 (дата обращения: 08.07.2021).

ства от деструктивного информационно-психологического воздействия (подп. 4 п. 25 Стратегии).

Проанализируем основные положения Стратегии, касающиеся обеспечения информационной безопасности.

Отражение угроз информационной безопасности в Стратегии

Подраздел «информационная безопасность» Стратегии начинается с анализа существующих угроз информационной безопасности. В качестве первого блока угроз выделяются вызовы межгосударственного информационного противоборства, включая использование ИКТ для вмешательства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности. Отмечается существенное возрастание количества компьютерных атак на российские информационные ресурсы, большая часть из которых осуществляется с территории иностранных государств. Акцентируется внимание на проведении иностранными спецслужбами разведывательных и иных операций в российском информационном пространстве.

Нашла отражение в Стратегии и угроза недостоверной информации (фейков). Отмечено, что такая информация, включая заведомо ложные сообщения об угрозе совершения террористических актов, распространяется в целях дестабилизации общественно-политической ситуации в Российской Федерации. Отмечены также иные контентные угрозы, включая распространение в сети «Интернет» материалов террористических и экстремистских организаций, призывов к массовым беспорядкам, осуществлению экстремистской деятельности, совершению самоубийства, а также пропаганду криминального образа жизни, потребления наркотиков.

В Стратегии сделан акцент и на актуальной проблеме последних лет, связанной с применением крупными иностранными технологическими компаниями (Big Tech) методов цензуры и блокировки альтернативных интернет-платформ. В качестве угрозы выделено также навязывание интернет-пользователям искаженного восприятия исторических и актуальных фактов и событий в России и мире.

Угрозообразующим фактором названа анонимность использования ИКТ в целях совершения преступлений, легализации полученных преступным путем доходов и финансирования терроризма, распространения наркотических средств и психотропных веществ. В качестве еще одного риска указано использование в Российской Федерации иностранных информационных технологий и телекоммуникационного оборудования, в том числе в объектах критической информационной инфраструктуры.

Подводя итог правовой регламентации угроз информационной безопасности в Стратегии, можно сделать вывод об адекватном отражении в документе наиболее острых информационных вызовов. Особенно отрадно устранение существовавшего длительный период крена в сторону информационно-технических угроз при недооценке рисков, связанных с деструктивным информационно-психологическим воздействием, состав-

ляющих предметное поле информационно-психологической безопасности[7]. Вместе с тем в Стратегии следовало бы большее внимание уделить угрозе киберпреступности. Ведь по последним данным ГИАЦ МВД России удельный вес преступлений в сфере высоких технологий составляет уже более 25 % (26,8 % по итогам пяти месяцев 2021 г.)[8]. Хотя тенденцию роста таких преступлений разработчики Стратегии все же выделили в другом подразделе документа, посвященном государственной и общественной безопасности.

Основные задачи обеспечения информационной безопасности

В качестве основной цели обеспечения информационной безопасности в Стратегии названо *укрепление суверенитета Российской Федерации в информационной сфере* (п. 56). Достижение данной цели осуществляется путем реализации государственной политики, направленной на решение комплекса задач. В стратегии выделено 16 таких задач. Сгруппируем несколько из них и представим обобщенный перечень, который включает в себя:

1) формирование безопасной среды оборота достоверной информации, защищенной и устойчивой информационной инфраструктуры РФ;

2) развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности, оперативной ликвидации их последствий;

3) предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы, повышение защищенности и устойчивости объектов информационно-коммуникационной инфраструктуры России, включая российский сегмент сети «Интернет»;

4) снижение количества утечек информации ограниченного доступа, противодействие иностранным техническим разведкам;

5) предупреждение, выявление и пресечение преступлений и иных правонарушений, совершаемых с использованием ИКТ;

6) защита персональных данных;

7) укрепление информационной безопасности Вооруженных сил и других воинских формирований, разработчиков и изготовителей вооружения, военной и специальной техники;

8) развитие сил и средств информационного противоборства;

9) противодействие деструктивному информационному воздействию на граждан и общество со стороны террористических и экстремистских организаций, специальных служб и пропагандистских структур иностранных государств;

[7] См.: *Смирнов А. А.* К вопросу о понятии, объекте и содержании информационно-психологической безопасности // Административное право и процесс. 2013. № 1. С. 34–39.

[8] Краткая характеристика состояния преступности в Российской Федерации за январь-май 2021 года // МВД России. 21 июня 2021 г. URL: https://мвд.рф/reports/item/24742236/ (дата обращения: 28.06.2021).

10) совершенствование средств и методов обеспечения информационной безопасности на основе применения передовых технологий, включая технологии искусственного интеллекта и квантовые вычисления;

11) обеспечение приоритетного использования российских информационных технологий и оборудования, отвечающих требованиям информационной безопасности, в российской информационной инфраструктуре;

12) развитие международного сотрудничества в сфере обеспечения информационной безопасности, а также взаимодействия органов публичной власти и институтов гражданского общества в данной сфере;

13) доведение до российской и международной общественности достоверной информации о внутренней и внешней политике Российской Федерации.

На наш взгляд, очерченный круг задач достаточно полно охватывает содержание сферы информационной безопасности и основные информационные угрозы, требующие нейтрализации. Описанные положения Стратегии вполне релевантны положениям действующей Доктрины информационной безопасности. В качестве ключевой новеллы мы отмечаем выделение линии информационного противоборства. Представляется, что оно отражает понимание невозможности обеспечить безопасность только защитными мерами и потребность в проведении упреждающих и ответных мероприятий информационного воздействия на основные источники угроз информационной безопасности.

Дополнительные задачи обеспечения информационной безопасности

Помимо основного тематического подраздела Стратегии, положения об обеспечении информационной безопасности присутствуют и в других разделах документа, посвященных обороне страны (второй приоритет), государственной и общественной безопасности (третий приоритет), защите традиционных российских духовно-нравственных ценностей, культуры и исторической памяти (восьмой приоритет), стратегической стабильности и взаимовыгодному международному сотрудничеству (девятый приоритет). Их анализ позволяет выделить дополнительные задачи обеспечения информационной безопасности, а именно:

1) поддержание морально-политического и психологического состояния личного состава Вооруженных сил и других воинских формирований, военно-патриотическое воспитание;

2) недопущение вмешательства во внутренние дела Российской Федерации, пресечение разведывательной и иной деятельности иностранных государств и отдельных лиц против национальных интересов Российской Федерации;

3) профилактика радикализма и экстремизма, прежде всего среди детей и молодежи, недопущение распространения экстремистской продукции, пропаганды насилия и нетерпимости, межнациональной розни;

4) предупреждение и нейтрализация социальных, межконфессиональных и межнациональных конфликтов, сепаратизма, радикализма, деструктивных религиозных течений;

5) защита исторической правды, сохранение исторической памяти, противодействие фальсификации истории;

6) реализация государственной информационной политики по укреплению восприятия обществом традиционных российских духовно-нравственных и культурно-исторических ценностей, неприятию гражданами навязываемых извне деструктивных идей, стереотипов и моделей поведения;

7) укрепление культурного суверенитета РФ и сохранение ее единого культурного пространства, защита общества от внешней идейно-ценностной экспансии и внешнего деструктивного информационно-психологического воздействия;

8) духовно-нравственное и патриотическое воспитание граждан;

9) укрепление позиции российских средств массовой информации и коммуникации в глобальном информационном пространстве.

Как видно, перечисленные дополнительные направления обеспечения информационной безопасности отчасти перекликаются с основными, но во многом дополняют их. Почти все из них касаются обеспечения информационно-психологической безопасности.

Таким образом, включение информационной безопасности в число стратегических национальных приоритетов Российской Федерации в базовом документе стратегического планирования в области безопасности стало важным и своевременным шагом со стороны политического руководства России, отвечающим на возросшую опасность вызовов цифровой среды. Вкупе с четким и грамотным определением задач обеспечения информационной безопасности это способно послужить мощным импульсом для укрепления механизма защиты национальных интересов России в информационной сфере.

Библиографический список

Смирнов А. А. К вопросу о понятии, объекте и содержании информационно-психологической безопасности // Административное право и процесс. 2013. № 1. С. 34–39.

Смирнов А. А. Проблемы обеспечения информационно-психологической безопасности России на современном этапе // Национальная безопасность : научное и государственное управленческое содержание : материалы Всероссийской науч. конф. (Москва, 4 декабря 2009 г.). М. : Научный эксперт, 2010. С. 897–907.

References

Smirnov A. A. To the question about the concept, object and content of the information-psychological security // Administrative law and process. 2013. № 1. P. 34–39.

Smirnov A. A. The problem of providing information and psychological security of Russia at the present stage // national security: the state scientific and administrative content: proceedings of the science conf. 4 Dec. 2009, Moscow. M. : Scientific expert, 2010. P. 897–907.

Для цитирования:

Смирнов А. А. Четвертый приоритет : правовое закрепление задач обеспечения информационной безопасности в новой стратегии национальной безопасности Российской Федерации // Вестник Воронежского государственного университета. Серия: Право. 2021. № 3 (46). С. 222–228. DOI: https://doi.org/10.17308/vsu.proc.law.2021.3/3552

Recommended citation:

Smirnov A. A. Fourth priority : legal regulation of information security tasks in the new national security strategy of the Russian Federation // Proceedings of Voronezh State University. Series: Law. 2021. № 3 (46). P. 222–228. DOI: https://doi.org/10.17308/vsu.proc.law.2021.3/3552

Антитеррористический центр государств – участников СНГ

Смирнов А. А., кандидат юридических наук, доцент, ответственный секретарь Научно-консультативного совета

E-mail: smirnovsng@yandex.ru

Advisory Council the Commonwealth of Independent States Anti-Terrorism Center

Smirnov A. A., Candidate of Legal Sciences, Associate Professor, Executive Secretary of the Scientific

E-mail: smirnovsng@yandex.ru