DOI 10.35775/PSI.2023.33.3.001
УДК 32

А.К. ШАВЛОХОВ
кандидат юридических наук, доцент,
доцент кафедры государственно-правовых дисциплин
Института государственной службы и управления Российской
академии народного хозяйства
и государственной службы при Президенте РФ;
эксперт Комитета Государственной Думы
Российской Федерации по безопасности, Россия, г. Москва

Д.И. МАКСИМЕНКО
магистрант по направлению правовое обеспечение
государственного муниципального управления Высшей школы
правоведения Института государственной службы и управления
Российской академии народного хозяйства
и государственной службы
при Президенте РФ, Россия, г. Москва

АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАСЕЛЕНИЯ В УСЛОВИЯХ ВОЕННЫХ КОНФЛИКТОВ: ПРАВОВЫЕ АСПЕКТЫ

В статье рассматриваются некоторые аспекты организационно-правового обеспечения информационной безопасности Российской Федерации, как одного из приоритетных направлений обеспечения национальной безопасности государства. Проводится анализ некоторых законодательных актов Российской Федерации, правовое содержание которых направлено на регламентацию порядка и правил обеспечения информационной безопасности. Обосновывается актуальность исследований заданной проблематики, исходя из всесторонней оценки геополитической обстановки в мире и по отношению к Российской Федерации, в частности.

Ключевые слова: *государство, национальная безопасность, информационная безопасность.*

В настоящее время, всем известное выражение: «Кто владеет информацией, тот владеет всем миром», приобретает все большую и большую

актуальность. Действительно, жизнь современного человека в буквальном смысле окружена различного рода информационно-технологическими средствами, которые круглосуточно транслируют информацию всевозможного характера, что в свою очередь нередко создает проблемы с «отсеиванием» неправдоподобных, порой ничем необоснованных данных.

Особое развитие, преподнесение заведомо ложной информации наблюдается с начала проведения Российской Федерацией, специальной военной операции на территории Украины. Граждане нашего государства практически ежедневно подвергаются информационным атакам, в большей степени, осуществляющимся посредством социальных сетей и сетей сотовой связи. Как следствие этого, напрямую возникает угроза национальной безопасности государства, так как атаки такого рода, прежде всего направлены на: дестабилизацию государства и населения; подрыв государственного суверенитета; манипулирования общественным сознанием различных социальных групп населения; воздействия на политическую ориентацию активных гражданских слоев в интересах создания напряженности в политической обстановке; дестабилизации политических отношений между объединениями, движениями и партиями в целях провокации конфликтов, разжигания атмосферы недоверия и подозрительности; провоцирования репрессий и насильственных действий против оппозиции; дискредитации органов управления, подрыва их авторитета; дезинформации населения и инициирования забастовок, массовых беспорядков и других протестных акций; подрыва международного авторитета государства, нанесения ущерба его жизненно важным интересам в политической, экономической, оборонной, культурно-спортивной и других сферах; провоцирования социальных, политических, национальных и религиозных столкновений. В этой связи, проблемы организационно-правового обеспечения информационной безопасности государства, как одного из приоритетных направлений в рамках обеспечения его национальной безопасности, приобретают особую важность и требуют современного подхода к их решению.

Следует отметить, что актуальность вопросов обеспечения информационной безопасности, как элемента государственной политики в области обороны и национальной безопасности, неоднократно подчеркивались и высшим руководством нашей страны. Так, Министр иностранных дел Российской Федерации С.В. Лавров, в своей статье обратил внимание на отдельные вопросы по обеспечению информационной безопасности с учетом стратегических национальных приоритетов, говоря о том, что: «Россия продолжит работать над наращиванием двустороннего и многостороннего сотрудничества по всему комплексу актуальных вопросов обеспечения международной информационной безопасности, в том числе в интересах противодействия угрозам, возникающим в связи с масштабным использованием информационно-коммуникационных технологий

в военно-политических целях» [4]. Уже позднее, министром также было подчеркнуто, что: «Безусловно, мы сейчас наблюдаем информационную войну, я бы сказал, информационный терроризм. Вбрасываются миллионы фейков, мы их постоянно разоблачаем» [2]. Аналогичное по своему смыслу суждение высказывал постоянный представитель Российской Федерации при Организации Объединенных Наций (далее – ООН) и Совете Безопасности ООН В.А. Небензя: «Сейчас против России в соцсетях развязана информационная война. Поскольку свидетельств разрушения гражданской инфраструктуры российскими военными нет, за таковые выдаются украинские удары и ошибочные попадания, а также кадры и видеоролики из Донбасса, фиксирующие как раз преступления украинских националистов» [3]. Отметим также, что несколько ранее, об использовании информационного пространства, как одного из векторов развития современных военных конфликтов между государствами, писал Начальник Генерального штаба Вооруженных Сил Российской Федерации – первый заместитель министра обороны Российской Федерации, В.В. Герасимов. В своей статье он констатировал тот факт, что: «В концепциях применения армий ведущих государств завоевание информационного превосходства объявлено непременным условием боевых действий. Для решения данной задачи используются СМИ и социальные сети. Одновременно задействуются силы и средства информационно-психологического и информационно-технического воздействия. Так, в конфликтах на Ближнем Востоке впервые широко раскрылись мобилизационные возможности социальных сетей» [1].

В этом отношении, также следует обратить внимание на тот факт, что, руководствуясь вышеперечисленными тенденциями и особенностями использования информационных технологий, в контексте их современного воздействия на безопасность государства, российской общественной организацией, занимающейся созданием дружественной интернет-среды и популяризацией интернет-технологий – Региональный общественный центр интернет технологий (РОЦИТ), была предпринята попытка закрепить в международно-правовом порядке, нормы о цифровом нейтралитете в период вооруженных конфликтов, позволяющие регламентировать и детерминировать различные аспекты информационного освещения таких конфликтов. По мнению специалистов информационных технологий, данные правила смогли бы стабилизировать и укрепить мировое сообщество в условиях глобальной цифровизации и развития новых технологий [11]. Между тем, происходящие на данный момент события во внешнеполитической и военной сферах, позволяют констатировать, что западное мировое сообщество, активно противопоставляющее себя позиции Российской Федерации на международной арене, использует информационно противоборство, как одно из средств достижения своих целей, в том числе в военной сфере.

Необходимо пояснить, что в правовом отношении, российский законодатель в целом своевременно реагирует на тенденции новейших вызовов и угроз, связанных с обеспечением информационной безопасности государства. Так, реализация данного направления, получила свое отражение в Указе Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации». В частности, положения главы IV настоящей Стратегии, определили обеспечение информационной безопасности в числе приоритетов по достижению национальной безопасности государства. Важным решением, по нашему мнению, следует также считать закрепление норм Уголовного Кодекса Российской Федерации, предусматривающих уголовную ответственность за публичные действия, направленные на дискредитацию использования Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности или исполнения государственными органами Российской Федерации своих полномочий в указанных целях [5].

Между тем, по нашему мнению, не в полной мере реализованным остается вопрос организации четко скоординированного государственного механизма, выполняющего те задачи в сфере информационной безопасности, которые описывались нами ранее. В настоящее время деятельность по всем направлениям обеспечения информационной безопасности возложена на ряд министерств и ведомств, таких как: Министерство обороны РФ, Федеральная служба безопасности, Министерство внутренних дел РФ, Федеральная служба охраны РФ, Совет безопасности РФ, Комитет государственной думы по безопасности и некоторые другие.

В частности:

– Министерство обороны РФ, уполномочено на организацию деятельности по обеспечению информационной безопасности, защите государственной тайны в Вооруженных Силах [6];

– Министерство внутренних дел РФ, участвует в пределах своей компетенции в разработке и реализации основных направлений государственной политики Российской Федерации в области международной информационной безопасности [7];

– одной из задач Федеральной службы безопасности, также является формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности [8];

– Федеральная служба охраны принимает участие в пределах своих полномочий в обеспечении информационной безопасности Российской Федерации [9];

– формирование государственной политики в области обеспечения безопасности и контроль за ее реализацией, в том числе тех аспектов, которые

связаны с информационным пространством, также является одной из основных задач Совета безопасности РФ и Комитета государственной думы РФ по безопасности [10].

Тем не менее, краткий анализ законодательных актов РФ, регламентирующих компетенции ряда государственных органов и учреждений, вовлеченных в решение задач обеспечения информационной безопасности, позволяет констатировать тот факт, что вопросы обеспечения информационной безопасности населения, возникающие непосредственно в условиях военной конфронтации нашего государства, и направленные на преподнесение заведомо ложного контента в СМИ и социальных сетях, с целью дестабилизации общественного настроения, остаются не в полной мере решенными.

Подтверждением данных суждений, в некоторой степени может послужить недавнее решение, приятое главой МВД РФ, В.А. Колокольцевым [12], по поручению которого в структуре МВД России было создано управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК). Конечно, созданное подразделение в стенах МВД РФ, по информации предоставленной в СМИ, не будет профилировать лишь на тех аспектах информационной безопасности, которые обозначены в настоящей статье. Однако одним из направлений его деятельности, является в том числе сбор и обработка информации, содержащейся в информационно-коммуникационных сетях, в целях выявления запрещенного контента и пресечения преступности, что безусловно указывает на повышенное внимание руководства МВД РФ к вопросам, связанным с безопасностью информационного пространства.

Таким образом, в современных реалиях, угрозы информационной безопасности государства, представляют собой комплексное явление, реализуются различными способами и направлены на всестороннее овладевание информационным пространством противной стороны. Данные обстоятельства, безусловно, требуют от субъектов информационного противоборства наличия в полной мере скоординированного механизма обеспечения информационной безопасности, способного действовать во всех существующих направлениях информационных баталий. Кроме того, необходимо постоянное совершенствование материально-технической базы и подготовка высококвалифицированных специалистов IT-индустрии, а также наличие соответствующих правовых основ, в полной мере регламентирующих аспекты информационной безопасности государства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. *Герасимов В.В.* Мир на гранях войны // Военно-промышленный курьер. 2017.

2. Лавров: Россия сейчас наблюдает «информационный терроризм» со вбросом миллионов фейков // Интернет-издание «ТАСС». 02.03.2022 // https://tass.ru/politika/13936943.

3. Небензя заявил о развязывании против РФ информационной войны // Интернет-издание «Известия». 28.02.2022 // https://iz.ru/1297914/2022-02-28/nebenzia-zaiavil-orazviazyvanii-protiv-rf-informatcionnoi-voiny.

4. Статья Министра иностранных дел Российской Федерации С.В. Лаврова «Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью» для журнала «Внешнеэкономические связи» // Сайт МИД РФ // 28 сентября 2020 г. // https://www.mid. ru/foreign_policy/international_safety/regprla/-/asset_publisher/ YCxLFJnKuD1W/content/id/4350978).

5. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ. Ст. 280.3.

6. «Указ Президента РФ от 16.08.2004 № 1082 «Вопросы Министерства обороны Российской Федерации». П. 27 ст. 7.

7. «Указ Президента РФ от 21.12.2016 № 699 «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации». П. 9.1. ст. 11.

8. «Указ Президента РФ от 11.08.2003 № 960 «Вопросы Федеральной службы безопасности Российской Федерации». П. 14 ст. 8.

9. «Указ Президента РФ от 07.08.2004 № 1013 «Вопросы Федеральной службы охраны Российской Федерации». П. 8 ст. 4.

10. «Указ Президента Российской Федерации от 7 марта 2020 г. № 175 «Положение о Совете безопасности Российской Федерации» // «Положение о Комитете Государственной Думы Федерального Собрания Российской Федерации по безопасности и противодействию коррупции».

11. https://www.vedomosti.ru/society/articles/2022/03/08/912604-oon-tsifrovoi-neitralitet.

12. https://www.kommersant.ru/doc/5592758.

A.K. SHAVLOKHOV
Candidate of Law, Associate Professor, Associate Professor of the Department of State and Legal Disciplines of the MIGSU RANEPA; expert of the State Duma Committee on Security of the Russian Federation, Moscow, Russia

D.I. MAKSIMENKO
Master's student in the direction of legal support of state municipal administration, Higher School of Jurisprudence, Institute of Public Administration and Management, Russian Academy of National Economy and Public Administration, Moscow, Russia

TOPICAL ISSUES OF INFORMATION SECURITY OF THE POPULATION IN MILITARY CONFLICTS: LEGAL ASPECTS

The article deals with some aspects of organizational and legal provision of information security of the Russian Federation as one of the priority directions of national security of the state. An analysis of some legislative acts of the Russian Federation is carried out, the legal content of which is aimed at regulating the procedure and rules for ensuring information security. The urgency of research of the given problematics, proceeding from a comprehensive assessment of the geopolitical situation in the world and in relation to the Russian Federation in particular is substantiated.

Key words: *state, national security, information security.*