ВВЕДЕНИЕ

Масштабные и глубокие изменения современной системы международных отношений ведут к росту ее турбулентности, обострению внешне- и внутриполитических конфликтов. Так, в действующей Стратегии национальной безопасности Российской Федерации отмечается, что в настоящее время происходит изменение мирового порядка и формирование новой архитектуры, правил и принципов мироустройства; стремление стран западного мира удержать свою гегемонию приводит к усилению международных противоречий, обострению внутриполитических проблем, усилению нестабильности в мире, геополитической напряженности, росту радикальных и экстремистских настроений[1], что, в свою очередь, ведет к появлению новых вызовов и угроз национальной безопасности Российской Федерации. В этих условиях на передний план выдвигается вопрос об организации эффективной защиты личности, общества и государства, ключевым элементом которой становится государственная информационная политика.

Использование современными государствами в политической борьбе новейших форм, методов и технологий информационного противоборства ведет к возникновению новых вызовов и угроз в информационной сфере: согласно Доктрине информационной безопасности Российской Федерации, к ним относятся «увеличение масштаба применения спецслужбами некоторых государств методов и технологий информационно-психологического воздействия с целью дестабилизации внутриполитической обстановки, вмешательства во внутренние дела государства», что наносит ущерб суверенитету и представляет опасность для территориальной

[1] Российская Федерация. Законы. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 года № 400.

целостности государства, а также использование форм, методов и технологий информационного влияния в военно-политических целях и деятельности, противоречащей международному праву[2].

В информационной сфере такими угрозами становятся новейшие формы и методы ведения информационной войны и организации цветных революций, кибернетические операции и идеологические диверсии. Новые угрозы выглядят структурно более сложными, многокомпонентными (гибридными), использующими новейшие достижения в сфере технологий дестабилизации общества, что, в свою очередь, требует выработки мер противодействия, адекватных уровню угрозы. При этом эффективное и системное противодействие данным вызовам и угрозам может быть обеспечено только на уровне государственной политики.

Россия и страны Запада сегодня находятся в состоянии информационной борьбы, которая демонстрирует тенденцию к еще большему обострению. Дополнительную угрозу создает лидерство коллективного Запада в информационно-коммуникационной сфере и практически монопольное глобальное влияние западных СМИ и социальных сетей, которые транслируют недружественную по отношению к России повестку и вводят правила, ограничивающие деятельность России в информационном пространстве. В Стратегии национальной безопасности Российской Федерации отмечается, что ряд недружественных стран проводит информационные кампании для формирования враждебного образа России, в том числе путем запрещения деятельности российских средств массовой информации и использованием информационных ресурсов[3]. В этих условиях основным инструментом противодействия данным угрозам также становится выверенная государственная информационная политика.

---

[2] Российская Федерация. Законы. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 5 декабря 2016 года № 646.

[3] Российская Федерация. Законы. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 года № 400.

В условиях проведения Российской Федерацией специальной военной операции на Украине одним из главных направлений боевых действий стало информационное противоборство, которое ведется в виде информационных диверсий и других видов информационных операций, фейковых новостей и дезинформации и других методов манипуляции общественным мнением на фронте и в тылу. Кроме того, в ходе самой СВО происходит изменение форм, методов и подходов к организации информационной борьбы, что также создает новые вызовы и угрозы безопасности и актуализирует поиск и разработку инструментов противодействия им.

Реакцией на появление новых вызовов и угроз становится изменение государственной информационной политики России. В новой редакции Конституции Российской Федерации к сфере ведения федеральных органов власти добавлено обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных (ст. 71, п. «м»)[4]. В 2021 г. принята новая Стратегия национальной безопасности, в которой, в отличие от предыдущей редакции документа, среди приоритетов обеспечения национальной безопасности в отдельный блок выделены основные риски и угрозы информационной безопасности, а также цели, задачи, формы и методы противодействия им (пп. 48–57)[5]. Также в 2021 г. утверждены новые основы государственной политики в области международной информационной безопасности, в которых изменен перечень вызовов и угроз, основных направлений и механизмов реализации государственной политики в данной области[6]. Кроме того, трансформировалась и практика государственной информационной политики Российской Федерации: приняты

[4] Российская Федерация. Законы. Конституция Российской Федерации (ред. от 01.07.2020).

[5] Российская Федерация. Законы. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 года № 400.

[6] Российская Федерация. Законы. Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности: Указ Президента Российской Федерации от 12 апреля 2021 года № 213.

новые нормативно-правовые акты, регулирующие информационную сферу (о «суверенном Интернете», «оскорблении власти», «иностранных агентах и нежелательных организациях», открытии филиалов иностранных IT-компаний в России, дискредитации армии и др.), созданы новые подразделения в органах государственной власти (42-й Департамент МИД международной информационной безопасности) и расширяются полномочия действующих контрольно-надзорных структур (Роскомнадзор, Генпрокуратура, МВД и др.), заблокированы ряд соцсетей и мессенджеров (*Facebook*, *Instagram*, *Tweeter* и др.), крупных СМИ и цифровых ресурсов (BBC, «Голос Америки», *Deutsche Welle, Bellingcat, Paper, Meduza, Mediazona*, «Собеседник», «Радио», «Свободная Европа / Радио Свобода (РСЕ/РС)»), растет количество заблокированных сайтов с нежелательной и ложной информацией[7]. Появление новых концептуальных основ, форм и методов реализации государственной информационной политики Российской Федерации в области обеспечения национальной безопасности в ответ на возникающие вызовы и угрозы свидетельствует о важности изучения особенностей изменения форм и методов деятельности государства в информационной сфере в условиях «неожиданных вводных» (факторов, появление которых до начала СВО вряд ли можно было предсказать).

Результаты данного исследования могут быть использованы при оценке состояния информационной безопасности Российской Федерации, дальнейших эмпирических исследованиях по отдельным вопросам государственной информационной политики и национальной безопасности Российской Федерации. Результаты работы наряду с другими исследованиями данной проблематики могут быть использованы для обучения специалистов и выработке практических рекомендаций для совершенствования государственной информационной политики в сфере противодействия новым вызовам и угрозам в информационно-коммуникационном пространстве.

[7] Роскомнадзор в 2022 г. внес более 384 тыс. ссылок в Единый реестр запрещенной информации // ТАСС [Электронный ресурс]. URL: https://tass.ru/obschestvo/17071733 (дата обращения: 28.02.2023).