

Секция «Политическое развитие России в условиях новых геополитических вызовов»

## Особенности формирования политики информационной безопасности Российской Федерации

Научный руководитель – Кучерявый Михаил Михайлович

*Вовенда Юлия Владимировна*

*Аспирант*

Северо-Западный институт управления - филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Факультет государственного и муниципального управления, Санкт-Петербург, Россия

*E-mail: Vovenda-yv@sziu.ru*

В настоящее время странами Запада проводится беспрецедентная деятельность, направленная на формирование негативного образа Российской Федерации на международной арене. При этом определяющим фронтом борьбы становится информационная сфера, где решаются важнейшие геополитические задачи по реализации национальных интересов крупнейших мировых держав. В данной связи актуальным является организация системы информационного противоборства на федеральном и региональном уровнях.

Геополитическая ситуация вокруг Российской Федерации становится все более сложной и напряженной, что вызвано еще и агрессивной деятельностью международных террористических организаций «Исламского государства», «Джабхат ан-Нусра», запрещенных в России, а также политикой США и стран НАТО по дестабилизации ситуации на Ближнем Востоке. Международная обстановка, сложившаяся в начале XXI века, потребовала переосмысления содержания понятия «национальная безопасность» и смены приоритетов в сфере ее обеспечения.

Необходимо отметить, что в сегодняшнем глобальном мире одним из основных приоритетов обеспечения национальной безопасности Российской Федерации является информационная сфера [2]. В данной связи необходимо выделить угрозы, которые действуют через компоненты информационной сферы, и провести их классификацию. В качестве компонентов информационной сферы выделяются: информационно-политическая, информационно-психологическая, информационно-технологическая сферы. Предлагается классификация **угроз безопасности** в глобальном информационном пространстве по следующим признакам: по происхождению угроз, по расположению источника угроз, по компонентам информационной сферы, по характеру деструктивного воздействия, по цели воздействия, по масштабу проявления.

Среди них, в первую очередь следует выделить **угрозы, которые воздействуют через компоненты информационной сферы:**

- информационные войны;
- военные конфликты всех масштабов - от локальных и региональных до международных;
- информационный терроризм;
- борьба за энергоресурсы;
- политическая пропаганда чуждых российскому менталитету идей;
- деструктивное воздействие Интернета, СМИ на общественное сознание граждан, на систему политического управления государством и др [4].

Поддержание статуса России как великой мировой державы требует от нашей страны обеспечения темпов инновационного развития, не уступающим другим высокоразвитым государствам. Особенностью формирования политики информационной безопасности будет являться развитие передовых информационных технологий

с темпами инновационного развития, не уступающим другим высокоразвитым государствам, на трех главных уровнях: отраслевом, национальном и международном.

На **отраслевом уровне** обеспечивается устойчивое функционирование информационной структуры, включающее в себя надежность информационных аппаратных средств, предотвращение действий злоумышленников и т.д. **Национальный** - связывает между собой виды системы национальной безопасности страны. **Международный** - предотвращаются угрозы из глобального информационного пространства и обеспечивается национальная безопасность в информационно-политической, информационно-технологической и информационно-психологической сферах.

Современные угрозы информационной безопасности в настоящее время ориентированы подорвать деятельность органов государственной власти и управления всех регионов Российской Федерации. Источниками угроз безопасности информации для объектов защиты являются все виды разведок (наземная, морская, воздушная и космическая). Особую угрозу для органов власти представляют системы глобальной радиоэлектронной разведки «Эшелон» и электронного наблюдения «ПРИЗМ».

В этой связи актуальным является организация и ведение информационного противоборства с целью, прежде всего:

противодействия пропагандистской деятельности иностранных государств и неправительственных организаций, направленной на дестабилизацию общественно-политической обстановки в Российской Федерации;

разоблачения и дискредитации организаций и информационных центров, осуществляющих подрывную информационную деятельность против Российской Федерации;

противодействия информационно-пропагандистской деятельности террористических организаций и радикально настроенных политических движений и группировок;

предотвращения деструктивных информационных воздействий на государственные информационные системы, информационные системы оборонно-промышленного комплекса, научно-исследовательских учреждений и образовательных организаций.

**Информационно-политическое противоборство** направлено на повышение эффективности реализации государственной информационной политики Российской Федерации, в т.ч. в информационном пространстве зарубежных государств.

В настоящее время общество обладает различными способами информационного противоборства:

- контроль и управление потоками информации;
- информационная асимметрия;
- информационное доминирование;
- информационное сдерживание;
- информационная агрессия;
- информационная война [3].

В настоящее время в Российской Федерации достаточно активно идет процесс формирования нормативно-правовой базы обеспечения информационной безопасности, тому свидетельство обновление Доктрины информационной безопасности в декабре 2016 года в соответствии с новыми существующими вызовами и угрозами в глобальном информационном пространстве [1].

Таким образом, политика информационной безопасности России и ее союзников в условиях современных угроз в глобальном мире будет определяться не только традиционными формами и способами применения вооруженных сил, но и комплексным использованием сил и средств информационного противоборства и действий государств в глобальном информационном пространстве.

### Источники и литература

- 1) Доктрина информационной безопасности Российской Федерации / Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. // Российская газета. 2016. 06 декабря
- 2) Стратегия национальной безопасности Российской Федерации / Утверждена Указом Президента Российской Федерации от 31 декабря 2015 г. № 683 // Российская газета. 2015. 31 декабря
- 3) Кучерявый М.М. К пониманию политики модернизации национальной безопасности // Управленческое консультирование. 2015. №11 (83). С. 19-32
- 4) Кучерявый М. М. Проблема информационной безопасности в современном обществе // Информационная безопасность. Невский диалог — 2012: матер. 4-й науч.-практ. конф., Санкт-Петербург, 23–24 октября 2012 г. СПб. : ЛЕНЭКСПО, 2012. С. 5–6