

Меньшиков Пётр Витальевич

МГИМО МИД России, и.о. заведующего кафедрой «Реклама и связи с общественностью», к.и.н., доцент

**Информационная безопасность и информационный суверенитет
и «гибридные войны» в современных международных отношениях**

1. Проблематика информационной безопасности занимает центральное место в стратегии государственной информационной политики современного государства. Прогнозируется дальнейшее нарастание в этой сфере угроз и вызовов, как во всем мировом сообществе, так и в России.
2. Недостаточная защищенность информационных ресурсов создает угрозы национальной и международной безопасности в целом, ведет к частичной или полной потере государственного информационного суверенитета.
3. С целью действенной защиты информационной инфраструктуры в России на протяжении всех последних десятилетий в рамках государственной стратегии последовательно создается система обнаружения, предупреждения и ликвидации угроз информационной безопасности России.
4. Информационная безопасность, как приоритетный компонент информационного суверенитета государства, включает в себя два главных компонента – технико-технологический и политико-идеологический, информационный, то есть имеют техническое и политическое измерения.
5. НАТО, США, ведущие страны ЕС активно расширяют усилия по созданию масштабной системы информационного противоборства на международной арене, что придает задаче деидеологизации международных отношений все более отдаленную и иллюзорную перспективу.
6. Нарращивание внешнеполитического информационно-пропагандистского потенциала США, НАТО, ЕС идет по нескольким направлениям со

смещением активности главным образом в сторону усиления коммуникационного присутствия в глобальной сети Интернет.

7. В структуре НАТО информационно-психологические операции как часть общей информационно политико-идеологической активности Альянса координируются Атлантическим Советом. Создана единая организационная система как организационно-тактического, так и стратегического уровней на основе долгосрочных доктрин НАТО, предусматривающих, в частности, задействование потенциала кибератак как средств цифровой пропаганды, кампаний DDoS-атак, дефейсы web-сайтов, утечку информации за счет хакерских кибератак, использование вредоносного программного обеспечения.
8. Активно привлекаются к разработке операций психологической войны неправительственные коммерческие организации.
9. Усиление русофобского дискурса за рубежом представляет собой реакцию со стороны правящих военных и части гражданских элит западных стран на объективно наступивший исторический этап российского национального возрождения. Последовательное отстаивание Россией своих национальных интересов, активное противодействие киберпреступности и идеологическим диверсиям является ответом на ужесточающееся идеологическое противостояние и усиление русофобского контента глобальных информационных потоков.