МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
ФАКУЛЬТЕТ ПОЛИТОЛОГИИ
КАФЕДРА РОССИЙСКОЙ ПОЛИТИКИ

На правах рукописи

Го Фэнли

Особенности противодействия современным гибридным войнам в сфере внешней политики Российской Федерации

Специальность 5.5.4. Международные отношения,
глобальные и региональные исследования

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата политических наук

Научный руководитель
доктор политических наук, с.н.с.
МАНОЙЛО АНДРЕЙ ВИКТОРОВИЧ

Москва – 2024

Оглавление

Введение

Тема диссертационного исследования – гибридные войны, которые ведутся в сфере, в которой Российской Федерация осуществляет свою внешнеполитическую деятельность. Применительно к гибридным войнам данная сфера очерчивается автором как пространство международных отношений, внешнеполитической деятельности основных акторов, обладающих собственными концепциями гибридных войн – России, США, Китая. Современные гибридные войны носят агрессивный характер и представляют угрозу национальной безопасности Российской Федерации. Неслучайно в пункте 13 Концепции внешней политики Российской Федерации 2023 года отмечается, что Соединенные Штаты Америки и их союзники «развязали гибридную войну нового типа», направленную на «всемерное ослабление России, включая подрыв ее созидательной цивилизационной роли, …, ограничение ее суверенитета во внешней и внутренней политике, разрушение территориальной целостности»; такой курс Запада приобрел всеобъемлющий характер и закреплен на доктринальном уровне»[1]. Россия в ответ на недружественные действия Запада (в том числе, в форме ведущихся против нее гибридных войн) «намерена отстаивать свое право на существование и свободное развитие всеми имеющимися средствами»[2]. Вместе с тем организация противодействия со стороны Российской Федерации гибридным войнам на системном уровне осложняется недостаточностью научного осмысления сущности, содержания и природы современных гибридных войн, которые, уже став частью объективной реальности, в научном сообществе все еще остаются предметом оживленных дискуссий.

[1] Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В.В. Путиным 31 марта 2023 г.). / МИД России, 31.03.2023. URL: https://mid.ru/ru/foreign_policy/official_documents/1860586/ (дата обращения: 02.01.2024).
[2] Там же.

Актуальность темы исследования определяется тем, что в настоящее время в военной сфере происходят значительные изменения, связанные с появлением войн нового поколения – гибридных войн. В современной политической науке гибридная война – это полноценная военная стратегия, ставшая «точкой сборки» и «зонтичным брендом» для различных видов вооруженного и невооруженного противоборства – традиционных военных действий, информационной, когнитивной, кибернетической, экономической, дипломатической, торговой и санкционной войн. Современная гибридная война предполагает комбинированное использование данных форм ведения войны, что делает ее чрезвычайно опасной, особенно в условиях глобальной нестабильности и нарастающей дестабилизации системы международных отношений. Ведущие страны мира, в числе которых Россия, США, КНР, уже имеют собственные концепции гибридных войн. У США первая концепция гибридных войн появилась в 2007 году[3] и получила распространение в начале 2010-х годов[4], у Российской Федерации собственная концепция гибридной войны возникла в 2013 году (в США и НАТО она получила название «Доктрина Герасимова»). В 1999 году Китай разработал концепцию «неограниченной войны», что стимулировало военную мысль США и стран Запада в направлении поиска новых форм «гибридного противостояния» во внешней политике и в военной области.

США и другие ведущие страны Запада в разработке глобальных стратегий все больше принимают во внимание фактор трансформации форм и методов ведения современных войн, активно пополняя свой арсенал технологиями гибридных войн. Так, еще в 2016 году на Варшавском саммите НАТО руководство этого военно-политического блока сделало тему гибридных войн одной из центральных в своей повестке и утвердило стратегию и план совместных действий по обеспечению собственной боеспособности в условиях современных гибридных

[3] Hoffman F.G. Conflict in the 21-st century. The rise of hybrid wars. Arlington: Potomac Institute for policy studies, 2007. – 72 p.; Mattis J.N., Hoffman F.G. Future Warfare: The Rise of Hybrid Wars // US Naval Institute Proceedings Magazine. – 2005. – Vol. 132/11/1,233. – P. 18-19. URL: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf (accessed: 01.03.2023).

[4] United States Government Accountability Office: Hybrid Warfare, GAO-10-1036R. Washington, DC, USA: USGAO, 10.09.2010. – 26 p. URL: http://www.globalsecurity.org/military/library/report/gao/d101036r.pdf (accessed: 01.03.2023).

войн[5]. С этого момента концепт «гибридная война» стал еще и идеологическим оружием, используемым США для дискредитации соперников.

Гибридная война, ведущаяся США и их союзниками против России, уже стала важнейшим фактором трансформации системы международных отношений и мировой политики, в ходе которой «происходит становление новой, более справедливой и демократической системы международных отношений, отвечающей потребностям мирового большинства»[6]. Неслучайно Президент Российской Федерации В.В. Путин, выступая 19 декабря 2023 года на расширенном заседании коллегии Министерства обороны Российской Федерации, заявил, что «Запад продолжает вести против России гибридную войну»[7], видя в России основную причину происходящих в мире изменений. В рамках этой гибридной войны США активизируют очаги локальных войн и вооруженных конфликтов, прежде всего у российских границ, а западные средства массовой информации (СМИ) ведут антироссийскую пропаганду, массово фабрикуют и вбрасывают в российское и мировое информационное пространство «фейковые новости», касающиеся целей, задач и хода специальной военной операции России на Украине, российского политического руководства, выборов в Российской Федерации.

В этих условиях возможность противостоять гибридным войнам прямо зависит от способности российского государства и научного сообщества вырабатывать и систематизировать научные знания о формах и методах ведения современных гибридных войн и на их основе разрабатывать эффективную стратегию противодействия гибридным войнам. Это, в свою очередь, делает исследование проблематики современных гибридных войн актуальным как в теоретическом, так и в практическом плане.

---

[5] Warsaw Summit Communiqué // NATO, 2016. URL: http://www.nato.int/cps/en/natohq/official_texts_133169.htm (accessed: 02.01.2024).

[6] Путин заявил о становлении новой системы международных отношений // РИА Новости, 27.11.2023. URL: https://ria.ru/20231127/otnosheniya-1912037256.html (дата обращения: 21.01.2024).

[7] Путин заявил о продолжении Западом гибридной войны против России // ТАСС, 19.12.2023. URL: https://tass.ru/politika/19578029 (дата обращения: 21.01.2024).

Степень научной разработанности темы исследования. Научные труды по тематике гибридных войн как российских, так и зарубежных авторов можно разделить на три основные группы.

Первая группа исследований содержит комплексный анализ сущности и содержания современных гибридных войны. В этих трудах особое внимание уделяется подходам военно-политического руководства России, коллективного Запада (прежде всего, США, НАТО) и Китая, имеющих собственные концепции гибридных войн. В США и других странах Запада проблематику гибридных войн разрабатывают как отдельные ученые-исследователи, так и крупные аналитические центры. К наиболее известным работам в данной области можно отнести труды Т. Мокайтиса[8], Дж. Немета[9], Ф. Хоффмана[10], Дж. МакКуина[11], М. Галеóтти[12], М. Кофмана[13], М. Кларка[14], К. Джайлза[15], М. Горанссона[16].

Со второй половины 2000-х годов теория гибридной войны получила широкое распространение в оборонной сфере США. Из научных и экспертных статей понятие «гибридная война» перешло в официальные документы (концепции,

---

[8] Buţa V., Vasile V. Persectives on the evolution and influence of the hybrid warfare concept // Romanian Military Thinking. – 2015. – № 3. – P. 11-32; Popescu N. Hybrid tactics: Russia and the West // European Union Institute for Security Studies, Alert. – 2015. – T. 46. – № 46. URL: http://www.iss.europa.eu/publications/detail/article/hybrid-tactics-russia-and-the-west (accessed: 05.02.2024); Solmaz T. 'Hybrid Warfare': One Term, Many Meanings // Small Wars Journal, 2022. URL: https://smallwarsjournal.com/jrnl/art/hybrid-warfare-one-term-many-meanings (accessed: 20.02.2022).

[9] Бурило Е.А. «Цветные революции» как разновидность политического конфликта // Будущее науки. Сборник научных статей 7-й Международной молодежной научной конференции, Курск: Юго-Западный государственный университет, 2019; Dominioni S., Tafuro Ambrosetti E. Russia's Hybrid Strategy: Myth or Reality? // Italian Institute for International Political Studies (ISPI), 2020. URL: https://www.ispionline.it/en/pubblicazione/russias–hybrid–strategy–myth–or–reality–26805 (accessed: 05.04.2022); Królikowski H. Hybrid Threats and Warfare, Are We Really Facing Something New? // Internal Security. – 2017. – Vol. 9. – № 2. – P. 9-21.

[10] Hoffman F.G. Conflict in the 21– st century. The rise of hybrid wars. – Arlington: Potomac Institute for policy studies, 2007. – 72 p.

[11] McCuen J.J. Hybrid Wars // Military Review. – Fort Leavenworth, Ks: Combined Arms Center, 2008. – P. 107-113.

[12] Galeotti M. I'm Sorry for Creating the 'Gerasimov Doctrine' // Foreign Policy, 2018. URL: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ (accessed: 15.12.2023); Mark Galeotti. Russian Political War: moving beyond the hybrid. – London: Routledge, 2019. – 136 p.

[13] Kofman M. Russia's Armed Forces under Gerasimov, the Man without a Doctrina // Russian Military Analysis, 2020. URL: https://www.ridl.io/en/russia-s-armed-forces-under-gerasimov-the-man-without-a-doctrine/ (accessed: 10.12.2021); Michael Kofman, Matthew Rojansky. A Closer Look at Russia's Hybrid War // Kennan Cable. – 2015. – № 7. – P. 1-8; Mark Galeotti.Russian hybrid warfare and other dark arts // War on the rocks, 2016. URL: https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/ (accessed: 10.12.2023).

[14] Clark M. Russian Hybrid Warfare // The Institute for the Study of War, 2020. URL: http://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf (accessed: 01.03.2022).

[15] Giles K. Handbook of Russian Information Warfare. – Rome, Italy: NATO Defense College, 2016. – 90 p.

[16] Göransson M.B. Russian scholarly discussions of nonmilitary warfare as securitizing acts // Comparative Strategy. – 2022. – Vol. 41. – № 6. – P. 526-542.

доктрины, стратегии) США и НАТО[17]. Так, в Стратегии национальной обороны США 2005 года[18] фактически была пересмотрена модель ведения войны, расширено понимание военных угроз, а в Четырехлетнем обзоре оборонной политики (QDR) США 2010 года теория гибридных войн была официально признана частью военной стратегии США[19]. В Итоговой декларации саммита НАТО 2016 года впервые на столь высоком официальном уровне говорилось о необходимости готовить Организацию Североатлантического договора к участию в гибридных войнах. По мнению руководства НАТО, такие войны включают в себя «проведение широкого спектра прямых боевых действий и тайных операций, осуществляемых по единому плану вооруженными силами, партизанскими и иными иррегулярными формированиями при участии различных гражданских компонентов»[20]. О подготовке к конфликтам в новых условиях, к которым НАТО относит и гибридную войну, говорилось в ежегодном докладе Генерального секретаря НАТО Й. Столтенберга 2015 года: «НАТО разрабатывает стратегию противостояния гибридным угрозам и действиям в условиях гибридной войны, которая охватывает широкий диапазон прямых и непрямых (скрытных) военных, полувоенных и гражданских акций, призванных разрушать, повреждать или принуждать»[21].

Важными документами для анализа гибридных угроз, возникающих в сфере внешнеполитической деятельности России, служат отчеты ряда американских аналитических центров, тесно сотрудничающих с военными ведомствами США и НАТО, в частности, корпорации RAND[22], Института изучения войны (ISW)[23],

---

[17] Данюк Н.С. Внешняя политика Российской Федерации (2000-2016 гг.) и феномен «цветных революций»: дисс. ... канд. истор. наук: 07.00.15. – М., 2018. – 312 с.

[18] The National Defense Strategy of the United States of America. – Washington, D.C.: U.S. Department of Defense, 2005. – 24 p.

[19] Quadrennial Defense Review Report // U. S. Department of Defense, 2010. – 128 p.

[20] Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales // NATO. 2016. URL: http://www.nato.int/cps/en/natohq/official_texts_112964.htm (accessed: 20.01.2021).

[21] Secretary General's Annual Report 2015 // NATO, 2016. URL: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160128_SG_AnnualReport_2015_en.pdf (accessed: 20.01.2021); Данюк Н.С. Внешняя политика Российской Федерации (2000-2016 гг.) и феномен «цветных революций»: дисс. ... канд. истор. наук: 07.00.15. – М., 2018. – 312 с.

[22] Dobbins J., Cohen R.S., Chandler N. et al. Overextending and Unbalancing Russia: Assessing the Impact of Cost– Imposing Options. Santa Monica, CA: RAND Corporation // RAND Corporation, 2019. URL: https://www.rand.org/pubs/research_briefs/RB10014.html (accessed: 10.02.2021).

Центра анализа европейской политики (CEPA)[24]. В трудах данных центров, посвященных тематике гибридных угроз, отдельное место отводится Российской Федерации. Так, в 2019 году RAND выпустил отчет, в котором были систематизированы технологии ведения гибридных войн, а также дана оценка преимуществ применения Государственным департаментом, Министерством обороны и Разведывательным сообществом США инструментария гибридных войн в сфере внешней политики США и в зонах вооруженных конфликтов[25].

В свою очередь, китайские научные труды по гибридным войнам можно разделить на две категории. Первая категория работ китайских ученых фактически содержит пересказ и поверхностные интерпретации результатов исследований гибридных войн российскими и западными экспертами[26]. Вторая категория трудов рассматривает гибридные войны как инструмент трансформации современных международных отношений[27]. Стоит отметить, что, несмотря на возрастающую популярность термина «гибридные войны» в научной сфере и в СМИ, исследования китайских авторов по тематике гибридных войн носят преимущественно фрагментарный характер. Это обусловлено тем, что в Китае практически полностью отсутствуют фундаментальные научные работы по тематике гибрид-

---

[23] Snegovaya M. Russia report Ⅰ. Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare // The Institute for the Study of War, 2015. URL: https://www.understanding war.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf (accessed: 10.11.2021); Clark M. Russian Hybrid Warfare // The Institute for the Study of War, 2020. URL: http://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf (accessed: 05.02.2023).

[24] Boulègue M., Chatterjee-Doody N., Polyakova A. et al. The Evolution of Russian Hybrid Warfare // The Center for European Policy Analysis, 2020. URL: https://cepa.org/wp-content/uploads/2021/01/CEPA-HybridWarfare-1.28.21.pdf (accessed: 05.02.2023).

[25] Dobbins J., Cohen R.S., Chandler N. et al. Overextending and Unbalancing Russia: Assessing the Impact of Cost–Imposing Options. Santa Monica, CA: RAND Corporation // RAND Corporation, 2019. URL: https://www.rand.org/pubs/research_briefs/RB10014.html (accessed: 10.02.2021).

[26] Ма Цзяньгуан, Ли Юаньбин. Гибридная война и ее характеристики: анализ с точки зрения российских учёных // Исследования по России, Восточной Европе и Центральной Азии. – 2021. – № 5. – С. 21-36. （马建光、李元斌.《"混合战争"及其特点：俄罗斯学者视角的解析》，载《俄罗斯东欧中亚研究》2021 年第 5 期，第 21–36 页.）; переводчик статьи: Сюй Дэцзюнь. Гибридная война в будущих конфликтах // StrategicFrontierTechnologies. 2021. URL: https://mp.weixin.qq.com/s/_vxEPz5tsmwJaQ4vcILHww (accessed: 10.02.2021). (许得君(编译).《未来冲突中的混合战争》战略前沿技术 2021 年 3 月 26 日)；переводчики статьи: Ли Шуйинь, У Имин. Стратегии и контрстратегии гибридной войны // RussianStudy. – 2020. – № 2. – С. 121-136. (李抒音、吴一鸣（译）.《混合战争战略和反战略》，俄罗斯研究，2020 年第 2 期，第 121– 136 页).

[27] Хан Кеди. «Гибридная война» России в Украине // Исследование стратегических решений. – 2021. – № 6. – С. 51– 80. (韩克敌. 俄罗斯在乌克兰的"混合战争",载《战略决策研究》2021 年第 6 期，第 51 至 80 页.); Шэнь Вэнькэ. Взгляд на современную войну из конфликта в Нагорном Карабахе // PLADaily. – 2020. – № 7. (沈文科：《从纳卡冲突管窥现代战争》, 解放军报, 2020 年 10 月, 第 007 版.).

ных войн. Исключением является единственная монография, посвященная гибридному вооруженному конфликту 2011 – 2017 годов в Сирии – «Откровение сирийской войны»[28], в которой ее автор Ма Цзяньгуан проанализировал военную операцию России в Сирии с точки зрения концепции гибридной войны, разработанной Ф. Хоффманом, и так называемой российской «Доктрины Герасимова» – о невоенных способах достижения политических и стратегических целей, изложенных в статье В.В. Герасимова в газете «Военно-промышленный курьер»[29], которую на Западе (в США и НАТО) считают российской концепцией ведения гибридных войн[30].

Среди российских исследований, посвященных всестороннему анализу гибридных войн, стоит выделить работы П.А. Цыганкова[31], А.В. Манойло[32], А.А. Бартоша[33], И.Н. Панарина[34], И.А. Николайчука[35], В.С. Котляра[36], А.Е. Шагова[37], В.Э. Багдасаряна[38], В.М. Буренка[39], С.М. Иншакова[40], И.С. Прокопенко[41],

---

[28] Ма Цзяньгуан. Откровение сирийской войны. – У Хань: Издательство литературы и искусства Чанцзян, 2017. – 272 с. (马建光. 《叙利亚战争启示录》，长江文艺出版社，2017 年，272 页).

[29] Герасимов В.В. Ценность науки в предвидении // Военно-промышленный курьер. – 2013. – № 8 (476). – С. 2.

[30] McKew Molly K. The Gerasimov Doctrine // Politico Magazine, 2017. URL: https://web.archive.org/web/20211111122402/https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/ (accessed: 20.01.2024).

[31] Цыганков П.А., Слуцкий Л.Э. Западный дискурс о «гибридной войне России против демократии»: новое вино в ветхие мехи // Вопросы политологии. – 2022. – № 12. – С. 4227-4238; Цыганков П.А. Гибридная война: политический дискурс и международная практика // Вестник Московского университета. Серия 18. Социология и политология. – 2015. – № 4. – С. 253-258.

[32] Манойло А.В., Стригунов К.С. Технологии неклассической войны. – М.: Генезис. Эволюция. Практика. Горячая линия – Телеком, 2020. – 378 с.; Евстафьев Д.Г., Манойло А.В. Гибридные войны в контексте постглобализации // Контуры глобальных трансформаций: политика, экономика, право. – 2021. – Т. 14. – № 4. – С. 332-347; Манойло А.В. Гибридизация современной мировой политики и национальная безопасность Российской Федерации // Геополитический журнал. – 2017. – № 1 (17). – С. 3-20.

[33] Бартош А.А. Вопросы теории гибридной войны. – М: Горячая линия – Телеком, 2023. – 324 с.; Бартош А.А. Театры гибридной войны. – М: Горячая линия – Телеком, 2022. – 356 с.

[34] Панарин И.Н. Гибридная война. Теория и практика. – М.: Горячая линия – Телеком, 2022. – 402 с.; Панарин И.Н. Гибридная война и передел мира. – М.: Горячая линия –Телеком, 2022. – 274 с.

[35] Николайчук И.А. О сущности гибридной войны в контексте современной военно-политической ситуации // Проблемы национальной стратегии (РИСИ). – 2016. – № 3 (36). – С. 85-104.

[36] Котляр В.С. К вопросу о «гибридной войне» и о том, кто же ее ведёт на Украине // Международная жизнь. – 2015. – № 8. – С. 57-72.

[37] Шагов А.Е. История происхождения и эволюция концепции и методов ведения гибридной войны. – М.: Мир науки, 2022. – Сетевое издание. – 155 с.; Шагов А.Е. «Гибридная война» и «Гибридные угрозы» в зарубежной военно-исторической науке. – М.: Мир науки, 2023. – 147 с.

[38] Багдасарян В.Э. Россия – Запад: цивилизационная война. – М.: Форум, 2017. – 410 с.

[39] Буренок В.М., Горгола Е.В., Викулов С.Ф. Национальная безопасность России в эпоху сетевых войн. – М.: Граница, 2015. – 190 с.

[40] Иншаков С.М. Гибридная война в системе военных угроз национальной безопасности. – М.: КноРус, 2018. – 312 с.

[41] Прокопенко И.С. Злые мифы о России. Что о нас говорят на Западе? – М.: Эксмо, 2016. – 288 с.

Н.С. Данюка[42]. Стоит отметить, что большой вклад в комплексное осмысление проблематики гибридных войн в современных международных отношениях внесла коллективная монография «Гибридные войны в хаотизирующемся мире XXI века» под редакцией П.А. Цыганкова[43]. В данной монографии отмечается, что гибридная война – это понятие, содержание которого «наполнено многими знакомыми элементами, придающими при их соединении новый смысл современной среде международной безопасности»[44]. По мнению П.А. Цыганкова, «гибридные войны уже стали объективной реальностью современных международных отношений» и «являются наиболее часто используемым инструментом внешней политики США»[45], создающим угрозу национальным интересам и национальной безопасности Российской Федерации.

Вторая группа научных трудов посвящена исследованию концепций, схожих с концепциями гибридных войн или являющихся по отношению к ним родственными. Так, помимо концепта «гибридные войны», в современной политической науке присутствуют такие понятия, как «управляемый хаос», «операции, основанные на достижении эффектов» (effects-based operations, EBO)[46], «неограниченная война»[47], «новая война»[48], «прокси-война»[49]. Эти понятия по своей сути очень близки к современному американскому пониманию гибридной войны, благодаря чему они и легли в основу более широкой научной дискуссии о природе, формах и методах гибридных войн.

---

[42] Егорченков Д.А., Данюк Н.С. Теоретико-идеологические подходы к исследованию феномена «гибридных войн» и «гибридных угроз»: взгляд из России // Вестник Московского университета. Серия 12: Политические науки. – 2018. – № 1. – С. 26-48; Филимонов Г.Ю., Данюк Н.С. «Гибридная война»: интерпретация и реальность // Свободная мысль. – 2017. – № 3. – С. 17-24.

[43] Гибридные войны в хаотизирующемся мире XXI века: коллективная монография / под ред. П.А. Цыганкова. – М.: Изд-во Московского ун-та, 2015. – 384 с.

[44] Там же.

[45] Цыганков П.А. «Гибридные войны»: понятие, интерпретации и реальность // «Гибридные войны» в хаотизирующемся мире XXI века / под. ред. П.А. Цыганкова. – М.: Изд-во МГУ, 2015. – С. 5-28.

[46] Манойло А.В., Стригунов К.С. Технологии неклассической войны: Генезис. Эволюция. Практика. – М.: Горячая линия – Телеком, 2023. – 378 с.

[47] Liang Q., Xiangsui W. Unrestricted warfare. – Beijing: PLA Literature and Arts Publishing House Arts, 1999. – FBIS Translated Text. – 228 p.

[48] Калдор М. Культура новых войн // Логос. – 2019. – Т. 29. – № 3 (130). – С. 1-21.

[49] Капицын В.М. Состоятельность современного государства в условиях нарастающих прокси-войн // Социально-гуманитарные знания. – 2019. – № 4. – С. 117-120; Столетов О.В. Концепт «прокси-война» в международно-политическом дискурсе «Новой Холодной войны» // Социально-гуманитарные знания. – 2019. – № 4. – С. 122-124.

Среди основных разработчиков теории «управляемого хаоса» часто называют имена Дж. Шарпа[50], Ст. Манна[51] и Зб. Бжезинского[52]. Изучению теории «управляемого хаоса» также посвящены работы ряда российских исследователей, в числе которых А.А. Бартош [53], В.Е. Лепский [54], С.А. Батчиков[55], И.А. Василенко[56] , Е.Г. Пономарева, Е.В. Рябинин[57]. Исследованию «операций, основанных на достижении эффектов», посвящены работы Д.А. Депутула [58], Д.Р. Леонарда [59], П.К. Дэвиса[60]. Данные теории в совокупности представляют собой базис исследований современных гибридных войн.

Третья группа работ посвящена изучению основных составляющих гибридных войн, среди которых особое место занимают цветные революции и информационные операции[61]. В этих исследованиях раскрывается эволюция форм и методов проведения современных психологических, информационных и кибероперациий, направленных на высшее военно-политическое руководство, население и критически значимую инфраструктуру «стран-мишеней»[62].

Вместе с тем перечисленные выше труды российских и зарубежных ученых, наряду с явными достоинствами, имеют и определенные недостатки – большинству из них не хватает системности. В научной литературе описание

[50] Sharp G. Exploring Nonviolent Alternatives. – Boston: Porter Sargent, 1970. – 162 p.; The Politics of Nonviolent Action. – Boston: Porter Sargent, 1973. – 913 p.; Social Power and Political Freedom. – Boston, 1980.– 440 p.; Шарп Дж. От диктатуры к демократии: Стратегия и тактика освобождения. – М.: Новое издательство, 2005. – 84 с.

[51] Mann S.R. The Reaction to Chaos // Complexity, Global Politics, and National Security. – 1997. – P. 62-68; Mann S.R. Chaos Theory in Strategic Thought // Parametes. – 1992. – Vol. 22. – № 1. – P. 54-68.

[52] Brzezinski Zb. Out of Control: Global Turmoil on the Eve of the 21st Century. – New York: Scribner Cop., 1993. – 240 c.

[53] Бартош А.А. Модель управляемого хаоса в культурно-мировоззренческой сфере // Вестник Московского государственного лингвистического университета. – 2014. – № 39. – С. 9-27.

[54] Лепский В.Е. Методологический и философский анализ проблематики управления. – М.: Когито-Центр, 2019. – 340 с.; Лепский В.Е. Технологии управляемого хаоса – оружие разрушения субъектности развития // Информационная война. – 2010. – № 4 (16). – С. 69-78.

[55] Батчиков С.А. Глобализация-управляемый хаос // Экономические стратегии. – 2008. – Т. 10. – № 5-6. – С. 38-45.

[56] Василенко И.А. Модель управляемого хаоса // Наш Современник. – 2003. – № 6. – С. 3-9.

[57] Пономарева Е.Г., Рябинин Е.В. «Цветные революции» в контексте стратегии управляемого хаоса // Обозреватель. – 2015. – № 12. – С. 38-51.

[58] Deptula D.A. Effects – Based Operations: Change in the Nature of Warfare. – Arlington VA: Aerospace Education Foundation. Defense and Airpower Series, 2001. – 41 p.

[59] Leonard D.R. Effects–Based Operations: A New Way of Thinking and Fighting. – Fort Leavenworth, KS: School of Advanced Military Studies, Army Command and General Staff College, 2003. – 48 p.

[60] Davis K.P. Effects – Based Operations. – RAND, 2001. – 117 p.

[61] Clark M. Russian Hybrid Warfare // The Institute for the Study of War, 2020. URL: http://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf (accessed: 10.02.2022).

[62] Курилкин А.В. Информационные и кибернетические операции как инструмент реализации внешней политики: формы, методы, технологии: дисс. ... канд. полит. наук: 23.00.04. – М., 2021. – 207 с.

гибридных войн носит фрагментарный характер, представляющий гибридные войны в виде набора частных кейсов.

Причем расхождения в мнениях у различных авторов начинаются уже на стадии определения того, что такое гибридная война – феномен, конфликт или конструкция. На этой стадии понятие «гибридные войны» часто пытаются определить через смежные категории, в числе которых управляемый хаос, цветные революции, ментальные и когнитивные войны, войны смыслов, которые сами еще являются дискуссионными и не получили общепризнанной интерпретации в мировом научном сообществе.

Кроме того, анализ научной литературы по проблематике гибридных войн показывает, что ведущие мировые державы, такие как Россия, Китай и США, уже имеют собственные концепции ведения гибридных войн, но при этом в развитии этих концепций идут собственным путем. При этом сравнительный анализ этих концепций в научной литературе отсутствует практически полностью.

Наконец, определенно не хватает исследований по практическому применению с практически отсутствуют научные труды, в которых дается объективная оценка эффективности мер, предпринимаемых Российской Федерацией, в целях противодействия гибридным войнам, развернутым против нее коллективным Западом, в том числе в контексте продолжающейся специальной военной операции России на Украине.

Цель исследования – выявить формы и методы организации противодействия Российской Федерации гибридным войнам, ведущимся США и его военно-политическими союзниками в пространстве реализации Российской Федерацией своей внешней политики.

Задачи исследования:

- выявить и классифицировать современные научные подходы к исследованию гибридных войн в России, США и КНР;

- установить основные закономерности эволюции форм и методов ведения современных гибридных войн;

- выявить и классифицировать формы и методы ведения гибридных войн;

- выявить современные подходы к организации системного противодействия гибридным войнам, а также сходства и различия данных подходов у России, США и Китая;

- оценить эффективность российского противодействия гибридным войнам, ведущимся США против России в информационном пространстве внешней политики Российской Федерации;

- предложить практические рекомендации по совершенствованию системы противодействия информационным и гибридным войнам в Российской Федерации.

Объект исследования – современные гибридные войны, представляющие собой комбинацию конвенционных и неконвенционных форм вооруженной и невооруженной борьбы, и воздействующие на Российскую Федерацию в процессе реализации ее внешней политики.

Предмет исследования – современные формы и методы противодействия гибридным войнам в пространстве реализации Российской Федерацией внешней политики.

Хронологические рамки исследования охватывают период с 2007 по 2024 год, что обусловлено целью и задачами диссертационной работы. Именно в этот период ведущие страны мира, такие как Россия, США и Китай, разрабатывают собственные концепции гибридных войн, включающие в себя опыт противодействия гибридным войнам со стороны вероятных противников. В США первые научные исследования гибридных войн появляются в 2007 году, в России – в 2013 году (так называемая «Доктрина Герасимова»), в КНР – в 1999 году (концепция «неограниченной войны»); в 2016 году Варшавский саммит НАТО утвердил план совместных действий по обеспечению собственной боеспособности в условиях современных гибридных войн. 31 марта 2023 года гибридные войны появляются в Концепции внешней политики Российской Федерации как «гибридные войны нового типа».

Научная новизна исследования выражается в следующем. Во-первых, диссертация является одним из первых научных исследований в России и первой

в КНР, посвященных системному исследованию форм и методов противодействия гибридным войнам, анализу эффективности данных методов, что имеет большое значение в контексте обострения противоречий между США и Российской Федерацией.

Во-вторых, в диссертации выявлены и классифицированы современные научные подходы к исследованию гибридных войн; установлены сходства и различия в российских, китайских, американских подходах к ведению гибридной войны; установлены основные закономерности эволюции гибридных войн; раскрыты основные формы и методы ведения гибридных войн Соединенными Штатами Америки против Российской Федерации; обобщен и систематизирован опыт НАТО и Китая по противодействию гибридным войнам, ведущимся их геополитическими противниками (для США и НАТО таким противником является Россия и, в определенной мере, Китай; для Китая – США, использующие методы гибридной войны для эскалации ситуации вокруг Тайваня и островов в Южно-Китайском море); предложены практические рекомендации по совершенствованию деятельности Российской Федерации в области противодействия гибридным войнам.

Установлено, что современные гибридные войны представляют собой полноценную военную стратегию, основанную на комбинированном использовании различных видов вооруженной и невооруженной борьбы, с широким привлечением к решению боевых задач нелегитимных акторов мировой политики – международных террористических, повстанческих группировок, приобретающих в гибридных войнах США и их союзников ограниченную, характерную для «акторов вне суверенитета», правосубъектность. При этом одним из ключевых результатов исследования стали полученные автором диссертации характеристика и классификация современных западных подходов к гибридной войне, которые в зарубежной научной литературе представлены двумя крупными направлениями: консервативным и новаторским, каждое из которых, в свою очередь, включает две платформы: «умеренную» и «радикальную».

Примененный автором диссертации сравнительный анализ подходов США, КНР и Российской Федерации к ведению гибридных войн позволил выявить сходства и различия во взглядах политической и военной элит этих стран на формы и методы ведения гибридных войн. Это также один из новых результатов данного исследования. Выявлено, что в плане философско-теоретического осмысления природы гибридных войн Россия ушла вперед и опередила США. Однако в плане практического применения форм и методов ведения гибридных войн США лидируют, перейдя от философского осмысления феномена гибридных войн непосредственно к практике применения конкретных методов и технологий ведения гибридных войн. Также в ходе исследования установлено, что в КНР теория и практика гибридной войны развиваются в форме собственного эндемичного направления – концепции «неограниченной войны», которая многое заимствовала из концепций гибридных войн России и Запада, но при этом в целом не повторяет их.

В ходе исследования также выявлено, что российский подход к ведению гибридных войн отличается определенной двойственностью. Несмотря на наличие собственной концепции ведения гибридных войн – так называемой «Доктрины Герасимова», российские ученые и военные специалисты еще не определились с тем, как относиться к гибридным войнам – как к эффективному инструменту воздействия или как к угрозе национальной безопасности. Такая двойственность, с одной стороны, вносит в российскую стратегию ведения гибридных войн элементы неопределенности (то есть, какой эта стратегия должна быть – сугубо наступательной или сугубо оборонительной); с другой стороны, данная двойственность уже привела к появлению уникального феномена – особой оборонительной по своему характеру стратегии, выражающейся в преимущественных наступательных действиях (то есть в так называемой активной обороне).

Теоретическая значимость исследования состоит в систематизации современных научных подходов к исследованию гибридных войн, опыта России, Китая и США по противодействию гибридным войнам. Благодаря систематизации форм и методов ведения США и их союзниками гибридных войн в исследо-

вании удалось выявить стратегию ведения США гибридных войн против России и Китая. В работе проанализированы меры противодействия гибридным войнам, предпринимаемые Российской Федерацией, и дана оценка эффективности данных мер. Полученные автором теоретические результаты могут быть использованы в деятельности федеральных органов исполнительной власти Российской Федерации по обеспечению национальной безопасности Российской Федерации и выработке приоритетных направлений противодействия гибридным угрозам в сфере реализации Россией своей внешней политики.

Практическая значимость исследования. Результаты исследования могут быть использованы в своей деятельности федеральными органами власти Российской Федерации, отвечающими за реализацию внешней политики России и обеспечение национальной безопасности государства, а также в учебном процессе по направлениям подготовки «Политология», «Конфликтология», «Международные отношения», при разработке учебных пособий для высших учебных заведений.

Теоретическую основу исследования составляет политический неореализм в теории международных отношений, а также знания и представления о природе современных войн и вооруженных конфликтов, нашедшие свое выражение в трудах Ф. Хоффмана, относившего к гибридным войнам внешнеполитическую деятельность России и Ирана[63]; Б. Родала и П. Акермана, утверждающих, что гибридные войны представляют собой комбинации действий регулярных войск и иррегулярных формирований, в том числе террористических группировок и транснациональных трансграничных сообществ организованной преступности, объединяющих свои усилия ради достижения общих целей [64]; Дж. Альманга, исследовавшего гибридные войны и гибридные вооруженные конфликты в так называемых «серых зонах» между миром и войной [65], и Дж. Чэмберса, исследовавшего гибридные войны в «серых зонах» с точки зрения

[63] Hoffman F. 'Hybrid Threats': Neither Omnipotent Nor Unbeatable // Orbis. – 2010. – № 54 (3). – P. 441-455.
[64] Ackerman P., Rodal B. The Strategic Dimensions of Civil Resistance // Survival. – 2008. – № 50 (3). – P. 111-126.
[65] Almäng J. War, vagueness and hybrid war // Defence Studies. – 2019. – № 19 (2). – P. 189-204.

возможностей сокрытия участия в них агрессора[66]; труды по теории сетецентрических войн, близких по своей природе к гибридным войнам, ведущимся США против Российской Федерации[67]. В теоретическом плане исследование также опирается на такие теории и концепции, разработанные китайскими учеными, как «неограниченная война»[68] и «квазивойна»[69], близкие по смыслу к западным ториям «войн в серой зоне».

Методологическая основа исследования включает в себя системный, компаративистский подходы, методы дискурс-анализа и «case study». Системный подход позволил выявить и классифицировать основные структурные составляющие гибридных войн, а также подходы различных государств к планированию и проведению информационно-психологических операций оборонительного и наступательного характера.

Метод «case study» использовался для анализа информационных операций, проводимых США против России. Дискурс-анализ использовался для исследования российской концепции ведения гибридных войн, представленной в выступлениях политического и военного руководства Российской Федерации (Президента Российской Федерации В.В. Путина, министра обороны Российской Федерации С.К. Шойгу, начальника Генерального штаба Вооруженных Сил Российской Федерации В.В. Герасимова).

Компаративистский подход позволил сравнить концепции ведения гибридных войн России, США и Китая, применяемые данными странами формы и методы противодействия гибридным войнам, выявить сходства и различия данных подходов.

Положения, выносимые на защиту:

---

[66] Chambers J. Countering Gray-Zone Hybrid Threats. An Analysis of Russia's «New Generation Warfare» and Implications for the US Army // Modern War Institute at West Point, 18.10.2016. URL: https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf (accessed: 13.03.2022).

[67] Cebrowski A., Garstka J. Network Centric Warfare: Its Origin and Future // Proceedings of the Naval Institute. – 1998. – № 124 (1). – P. 28-35.

[68] Liang Q., Xiangsui W. Unrestricted warfare. – Beijing: PLA Literature and Arts Publishing House Arts, 1999. – FBIS Translated Text. – 228 p.

[69] Zhao Z., Zhao J. On Control and Management of Military Crises (论军事危机的管控) // China Military Science (中国军事科学). – 2013. – № 4. – P. 62-71.

1. Основываясь на переоценке международной обстановки и условий обеспечения национальной безопасности Российской Федерации, российское руководство внесло существенные коррективы в стратегию реализации внешней политики Российской Федерации, вызванные окончательной утратой иллюзии о возможности возвращения в «лоно западной цивилизации», осознало самобытность и самодостаточность российского государства-цивилизации и собственную роль России в мировой истории. При этом в Концепцию внешней политики Российской Федерации 2023 года, важнейший документ стратегического планирования, впервые был введен термин «гибридная война нового типа», определяемый как внешнеполитическое направление деятельности коллективного Запада, нацеленное на всемерное ослабление России, что показывает повышенное внимание руководства Российской Федерации к гибридным войнам, ведущимся США и их военно-политическими союзниками, и в среднесрочной перспективе может стать основой для разработки Россией эффективной стратегии противодействия гибридным войнам.

2. Обновленная Концепция внешней политики России 2023 года демонстрирует стремление к минимизации издержек при одновременном обеспечении национальных интересов Российской Федерации за счет накопления и концентрации стратегических ресурсов на указанных в данной концепции приоритетных направлениях внешнеполитической деятельности. С одной стороны, в ответ на недружественные действия коллективного Запада Россия намерена наращивать внешнеполитическую активность на азиатском, африканском и латиноамериканском направлениях, которые имеют очевидные перспективы с точки зрения расширения взаимовыгодного международного сотрудничества с «незападным миром». С другой стороны, хотя Россия не испытывает оптимизма по поводу перспектив развития отношений с США и другими западными странами, она все же готова вернуться к сотрудничеству с Западом на равных и взаимовыгодных условиях, но не в формате гибридных войн.

3. Современные гибридные войны представляют собой полноценную военную стратегию, основанную на принципе комбинированного использования

различных видов классической (конвенционной) и неклассической (неконвенционной) вооруженной борьбы. В гибридной войне, наряду с традиционными вооруженными силами, активно используются операции информационной войны, инструментарий экономических, торговых и санкционных войн, а также различные виды разведывательно-диверсионной деятельности (в том числе, в идеологической сфере и сфере исторической памяти), для осуществления которых привлекаются трансграничные преступные сообщества, международные террористические организации, наркокартели, разнообразные «повстанческие» и «освободительные» движения. В этом плане гибридные войны представляют собой «зонтичный бренд» и «точку сборки» для различных методов ведения вооруженной (силовой) и невооруженной (несиловой) борьбы, применяющихся как в военное, так и в мирное время. При этом основные научные дискуссии ведутся вокруг двух основных вопросов: 1) в какой мере появление гибридных войн стало революцией в военном деле, какова связь между современными концепциями гибридных войн и традиционными представлениями о войне; 2) как гибридные войны влияют на международную политику и находят свое практическое применение в международных конфликтах. При этом по отношению к самому феномену гибридных войн современные научные подходы представлены двумя основными направлениями: консервативным и новаторским, каждое из которых включает в себя две платформы: «умеренную» и «радикальную».

4. Сторонники консервативного направления считают, что гибридные войны – это давно известное явление, так как все без исключения войны всегда были гибридными; новаторы, напротив, рассматривают гибридные войны как принципиально новое явление. Сторонники радикально-консервативной платформы, отрицающей новизну гибридных войн, утверждают, что понятие «гибридные войны» лишено смысла и навеяно модными политическими предпочтениями. В отличие от них, сторонники умеренно-консервативной платформы не видят инновационного прорыва в содержании гибридных войн, однако не отрицают разумность и ценность их исследования. Стоит отметить, что данная точка зрения разделяется большинством исследователей современных войн и локальных воору-

женных конфликтов. Сторонники новаторского направления, напротив, подчеркивают необходимость и актуальность исследования гибридных войн, а также форм и методов противодействиям им, признавая гибридные войны новым явлением. При этом «радикальные» сторонники новаторского направления рассматривают гибридные войны как некое новое явление, принципиально отличающееся от «классических» войн, а умеренные новаторы считают, что гибридные войны представляют собой новый этап эволюции классических форм и методов ведения войны, вобравших в себя неклассические («гибридные») методы и подходы ведения современных войн.

5. Проведенный сравнительный анализ подходов Запада (прежде всего, США и НАТО) и России к феномену гибридной войны позволил выяснить, что США и их военно-политические союзники уделяют повышенное внимание технологиям гибридных войн, рассматривая гибридные войны как часть стратегии соперничества великих держав. При этом подходы США и России заметно отличаются. Так, концепция гибридных войн России опирается на более глубоко и основательно разработанную теоретико-философскую базу, чем концепция гибридных войн США, которые рассматривают гибридные войны преимущественно с инструментальной точки зрения. При этом США и их главные союзники в Европе уже перешли от абстрактных дискуссий о природе гибридных войн к практическому применению данного инструментария во внешнеполитических целях. Для США гибридные войны, с одной стороны, стали поводом для выдвижения обвинений в отношении других стран (в том числе, России и Китая) в ведении гибридных войн, с другой стороны, США сами активно разрабатывают и используют широкий спектр технологий гибридных войн для нанесения военного и экономического ущерба своим геополитическим соперникам, к числу которых относятся Китай и Россия.

6. Китайский подход к гибридным войнам обладает определенной спецификой. Китай внимательно следит за научной дискуссией России и Запада о сущности и содержании феномена гибридных войн, фокусируя внимание на практическом использовании технологий ведения гибридных войн. При этом са-

ми концепции гибридных войн, разработанные Россией и США, в Китае в настоящее время не получили такого же широкого распространения, так как в Китае уже сформировалась и развивается собственная теоретическая концепция «неограниченной войны», возникшая в процессе осмысления новых изменений в сфере международных конфликтов и безопасности, которая выходит за рамки российской и западной концепций гибридных войн. В отличие от российской и западной концепций гибридных войн, рассматривающих «внешние силы» и «угрозы», китайский подход сосредоточен на внутреннем управлении состоянием национальной безопасности. В рамках концепции «неограниченной войны» границы между войной и миром, конвенционными и неконвенционными формами и методами борьбы становятся размытыми, транспарентными, а в некоторых случаях исчезают вообще. В свою очередь, российский подход к гибридным войнам отличается определенной «двойственностью» – гибридные войны рассматриваются военным и политическим руководством Российской Федерации одновременно и как угроза внутренней безопасности (если эти войны ведет Запад с целью дестабилизировать политическую ситуацию внутри России), и как эффективный способ борьбы с противниками России, позволяющий устранить дисбаланс в военных возможностях.

Достоверность полученных результатов исследования обеспечивается обоснованностью и выверенностью методологической базы исследования; использованием методов, адекватных объекту, предмету, цели и задачам исследования; опорой на верифицируемые научные источники.

Соответствие содержания диссертации паспорту научной специальности. Диссертация соответствует следующим направлениям исследований, указанным в паспорте научной специальности 5.5.4 Международные отношения, глобальные и региональные исследования: 2. Субъекты международных отношений. Деятельность государственных и негосударственных акторов. Формальные и неформальные институты в международных отношениях и в мировой политике. Формирование и реализация внешнеполитических стратегий, концепций и доктрин. 3. Мировая политика. Субъекты мировой политики. Современный мировой

политический процесс. Глобальная система и региональные подсистемы международных отношений и мировой политики. 7. Международная безопасность. Системы глобальной и региональной безопасности. Военная сила в международных отношениях. Международный терроризм и борьба с ним. Разоружение и контроль над вооружениями. Вызовы, риски, опасности и угрозы. 8. Международные кризисы и конфликты. Этнический и религиозный факторы в международных отношениях. Миротворческая деятельность. 17. Информационные, когнитивные, био- и другие новые технологии в международных отношениях и мировой политике. 19. Российская Федерация в системе международных отношений.

Апробация результатов исследования. Основные положения диссертации и полученные научные результаты изложены в 9 научных публикациях, в том числе в 7 журналах, включенных в перечень научных изданий, рекомендованных для защиты в диссертационном совете МГУ имени М.В. Ломоносова по специальности и отрасли наук, в 1 журнале из Перечня ВАК при Минобрнауки России, а также в 1 монографии. Общий объем статей и монографии, опубликованных по теме диссертационного исследования, – 14,04 п.л. (доля соискателя – 11,36 п.л.).

Глава I. Теоретико-методологические аспекты исследования современных гибридных войн[70]

1.1. Внешняя политика России в условиях новых вызовов и угроз

31 марта 2023 года президент РФ В. В. Путин подписал Указ об утверждении обновлённой Концепции внешней политики (далее – «Концепция-2023»), которая стала руководящим документом для реализации внешней политики России в условиях новых вызовов и угроз.

Основываясь на переоценке Россией международной обстановки и условий собственной безопасности, новая редакция Концепции определяет национальные интересы, стратегические цели и приоритеты российской внешней политики. Прежде всего, в ней учитываются происходящие глубокие трансформации и долгосрочные тенденции в современном мире, в частности, становление новых мощных центров экономического роста (прежде всего в Восточной и Южной Азии), формирование многополярного мироустройства, увеличение значения

[70] При подготовке данного раздела диссертации использованы следующие публикации, выполненные автором лично или в соавторстве, в которых, согласно Положению о присуждении ученых степеней в МГУ, отражены основные результаты, положения и выводы исследования: Го, Фэнли. Гибридная война в исследованиях ученых китайской народной республики / Ф. Го // Гражданин. Выборы. Власть .– 2022. – № 1(23). – С. 140-152; Го, Фэнли. Особенность противодействия информационным операциям со стороны Российской Федерации / Ф. Го // Вопросы национальных и федеративных отношений. – 2023. – Т. 13. – № 6 (99). – С. 2554-2560; Го Фэнли. Российский подход к информационному противоборству / Ф. Го // Вопросы политологии. – 2023. – Т. 13. – № 3 (91). – С. 1253-1260; Го, Фэнли. Гибридная война США и их союзников против России в контексте специальной военной операции / Ф. Го // Гражданин. Выборы. Власть. – 2023. – № 2 (28). – С. 146-155; Го, Фэнли. Гибридная война США и их союзников против России в контексте специальной военной операции / Ф. Го // Гражданин. Выборы. Власть. – 2023. – № 2 (28). – С. 146-155; Го, Фэнли, Манойло, А.В. Торговая война США против Китая в период президентского правления Д. Трампа как составляющая современных гибридных войн / Ф. Го, А.В. Манойло // Вестник Московского университета. Серия 12. Политические науки. –2022. – № 5. – С. 81-92.

фактора силы в международных делах и наращивание влияния культурно-цивилизационного фактора на мировую политику[71]. Вместе с тем в своём внешнеполитическом планировании Российская Федерация также принимает во внимание вызовы текущего момента, основным из которых является эскалация напряжённости в отношениях между Россией и Западом. Это выражается, прежде всего, в европейском направлении, где оппоненты развязали против России гибридные войны нового типа с использованием Украины как плацдарма. К тому же, в Азиатско-Тихоокеанском театре действия США и их союзников, направленные на системное «сдерживание» Китая, также представляют непосредственный вызов интересам и безопасности Москвы.

По сравнению с предыдущей редакцией 2016 года, а также действовавшей до него Концепцией 2013 года, «Концепция-2023» отличается следующими основными особенностями.

1. Подчёркивается самобытность российской цивилизации. В новой редакции Концепции неоднократно подчёркивается особое положение России, которое определяется как «самобытное государство-цивилизация», «обширная евразийская и евро-тихоокеанская держава, сплотившая русский народ и другие народы, составляющие культурно-цивилизационную общность Русского мира», «один из суверенных центров мирового развития, выполняющий исторически сложившуюся уникальную миссию по поддержанию глобального баланса сил и выстраиванию многополярной международной системы»[72]. Стоит отметить, что это впервые в стратегическом документе Россия назвала себя отдельной цивилизацией. В редакции 2013 года страна была «неотъемлемой, органичной частью европейской цивилизации», а в документе 2016 года термин «цивилизация» был употреблен в отношении кого угодно, но не самих себя. Теперь Россия закрепляется «ядром цивилизационной общности Русского мира». Все это показывает, что в российском обществе, экспертной среде и высоких кабинетах происходило

[71]Дробинин А. Ю. Основные тенденции мирового развития и внешняя политика Российской Федерации // Дипломатическая служба. – 2023. – №1. – С. 7– 8.

[72] Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В.В. Путиным 31 марта 2023 г.) [Электронный ресурс] // МИД РФ. 2023. URL: https://www.mid.ru/ru/detail-material- page/1860586/ (дата обращения: 20.04.2023).

переосмысление собственной роли в мировой истории и формально прописалась своя самобытность.

2.Стоит отметить, что в «Концепции-2023» привлекает особое внимание упоминание трёх новых терминов, которые отсутствовали в предыдущих концепциях внешней политики. Во-первых, относительно новый термин «ближнее зарубежье». Он активно использовался в России в 1990-е годы, но затем почти вышел из употребления из официального оборота в связи с тем, что его использование стало раздражать партнёров России в СНГ, по мнению которых, в этот термин вкладывали семантические коннотации об их неполноценности в качестве суверенных государств. С учетом того, что, по умолчанию, «в такого рода документах ничего не меняется случайно»[73], активизирование данного термина в официальном документе, безусловно, было осознанным и может быть рассмотрено как некий сигнал или намёк со стороны российского руководства для других стран. Аналогично, не меньше внимания вызывает и появление двух совершено новых терминов, которые никогда не упоминались в предыдущих концепциях: «англосаксонские государства» и «гибридная война». Первое, «англосаксонские государства», представляет собой «ядро» Коллективного Запада под руководством США. Другой новый термин – это «гибридная война», который впервые появился в официальном документе России. После начала СВО оба термина всё чаще используются в заявлениях официальных представителей РФ[74]. В «Концепции-2023» признается «экзистенциальный характер угроз безопасности и развитию России, создаваемых действиями недружественных государств» во главе США, которые выступают «главным инициатором и проводником антироссийской линии», при этом «политика Запада, направленная на всемерное ослабление России, охарактеризована как гибридная война нового типа»[75].Так, в доку-

[73] Барабанов О.Н. Новая Концепция внешней политики РФ: структура и семантика [Электронный ресурс] // Валдай. 2023. URL: https://ru.valdaiclub.com/a/highlights/novaya-kontseptsiya-vneshney-politiki-rf-semantika/?sphrase_id =645683 (дата обращения: 20.04.2023).

[74] Посол США в России назвала странным и средневековым понятие «англосаксы» [Электронный ресурс] // РБК. 2023. URL: https://www.rbc.ru/rbcfreenews/644ac8469a7947383e0ff8b0 (дата обращения: 20.04.2023).

[75] Выступление Министра иностранных дел Российской Федерации С. В. Лаврова на Совещании с постоянными членами Совета Безопасности Российской Федерации [Электронный ресурс] // МИД РФ. 2023. URL: https://www.mid.ru/tv/?id=1861005&lang-ru (дата обращения: 20.04.2023).

менте указывается следующее: рассматривая Россию угрозой западной гегемонии, «США и их сателлиты развязали гибридную войну нового типа. Она направлена на всемерное ослабление России, включая подрыв ее созидательной цивилизационной роли, силовых, экономических и технологических возможностей, ограничение ее суверенитета во внешней и внутренней политике, разрушение территориальной целостности»[76]. Это отражает тот факт, что руководство России по-настоящему утратило иллюзию о вступлении в «семью западной цивилизации», осознав долгосрочное стремление Запада уничтожить Россию и непримиримые противоречия между двумя сторонами. При этом оно также осознает, что такой курс Запада приобрёл всеобъемлющий характер и закреплён на доктринальном уровне – в том числе, в форме концепции гибридных войн. Это также можно рассматривать как официальное признание российской стороны существования гибридных войн, хотя в контексте Концепции внешней политики РФ данный термин употребляется скорее как главная стратегия Запада для уничтожения России. Вместе с тем это создет предпосылки для применения Россией технологии гибридных войн для противодействия угрозам со стороны противника. Ведь, как указал начальник Генштаба В. В. Герасимов на общем собрании Академии военных наук 2016 года, на гибридные войны следует отвечать гибридными методами[77].Тем более, в «Концепции-2023» предусматривается возможность принятия симметричных и асимметричных мер в ответ на такие действия. В частности, тезис о превентивном ударе также включен в новую концепцию внешней политики России из-за «агрессивного развития событий», согласно которой «Вооруженные силы РФ могут быть задействованы, чтобы отразить или предотвратить нападение на страну или ее союзников»[78].

---

[76]Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерацииот 31 марта 2023 года № 229 [Электронный ресурс] // МИД РФ. 2023. URL: https://www.mid.ru/ru/detail-material-page/1860586/?lang-ru (дата обращения: 20.04.2023).

[77] На гибридные войны следует отвечать гибридными методами [Электронный ресурс] // Центр анализ террористических угроз. 2023. URL: https://catu.su/analytics/1256-na-gibridnye-vojny-sleduet-otvechat-gibridnymi-metodami (дата обращения: 20.04.2023).

[78]Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации от 31 марта 2023 года №229 [Электронный ресурс] // МИД РФ [Официальный сайт]. 2023. URL:https://www.mid.ru/ru/detail-material-page/1860586/?lang=ru(дата обращения: 20.04.2023).

3.Более показательны отличия нынешней Концепции от предыдущих в разделе региональных приоритетов внешней политики РФ. Прежде всего, региональные приоритеты выделялись в качестве отдельных подразделов. Стоит отметить, что в Концепциях 2013 и 2016 годов региональные приоритеты шли сплошным текстом в перечислении абзацев друг за другом, не выделяясь отдельно. Их порядок в этих концепциях также аналогичен: СНГ, Евро-Атлантический регион, Арктика, Антарктика, Азиатско-Тихоокеанский регион, Ближний Восток и Северная Африка, Латинская Америка и Карибский бассейн, Африка. Значит, событие в Крыму и первые санкции не понизили Евроатлантику в её месте региональных приоритетов. В «Концепции-2023» отдельные регионы мира структурно поделены на несколько подразделов, при этом их названия и порядок следования следующие: «Ближнее зарубежье», «Арктика», «Евразийский континент. Китайская Народная Республика, Республика Индия», «Азиатско-Тихоокеанский регион», «Исламский мир», «Африка», «Латинская Америка и Карибский бассейн», «Европейский регион», «США и другие англосаксонские государства», «Антарктика». Как видно из этого документа, изменились некоторые формировки и порядок перечисления приоритетных регионов. Считается, что, «чем выше стоит тот или иной регион в этом перечислении, тем более он значим в реальной политике»[79]. В текущей геополитике вместо «Евро-Атлантического региона» выделились Европа и англосаксонские государства, в первую очередь, благодаря тому, что они из верхней части списка опустились практически на самое дно списка. Вместе с тем отдельно из Азиатско-Тихоокеанского региона выделен Евразийский континент с Китаем и Индией и помещён впереди него. Здесь также надо обратить внимание на то, какие страны упоминаются особо. В тексте подобных Концепций, по умолчанию, «если то или иное государство упоминалось особо, значит, оно действительно первостепенно важно для политики РФ. Если же оно исчезало или же появлялось новое, то это воспринималось как семанти-

[79]Барабанов О. Н. Новая Концепция внешней политики РФ：структура и семантика [Электронный ресурс] // Валдай. 2023. URL: https://ru.valdaiclub.com/a/highlights/novaya-kontseptsiya-vneshney-politiki-rf-semantika/?sphrase_id -645683 (дата обращения: 20.04.2023).

ческий сигнал»[80]. По сравнению с двумя предыдущими версиями, в нынешней Концепции список отдельно упомянутых стран изменились значительно. В частности, бросается в глазато, что из него удалены все европейские и «другие англосаксонские» страны, при этом, из стран СНГ отдельно упоминается только Белоруссия.

4.Взаимодействие между внешней политикой России и безопасностью страны возросло на небывалый уровень. «Концепция-2023» характеризуется яркими оттенками безопасности с заметным умножением использования таких терминов, как «враждебный», «угроза», «русофобия». С точки зрения внутренней безопасности Россия подчеркивает легитимность применения силы в целях самообороны, считая, что в ответ на недружественные действия Запада она может использовать все имеющиеся средства для защиты своего права на существование и развитие. В области международной безопасности, выступая за создание новой архитектуры международной безопасности, Москва призывает обеспечивать безопасность всех стран равномерно на основе принципа неделимости безопасности, и тем самым сокращать злоупотребление доминирующим положением в мировой экономике со стороны недружественных стран. Что касается периферийной безопасности, все эти годы постсоветское пространство сохраняется в первом приоритете российской внешнеполитической линии, однако в тексте «Концепции-2023» оно выглядят иначе. Прежде всего, впервые оно упомянуто отдельным пунктом, в частности, явно выделена роль Союзного государства, которое стало вторым приоритетом в разделе «Ближнее зарубежье». Кроме Белоруссии, из республик бывшего СССР упомянуты лишь Абхазия и Южная Осетия. Исчезновение в новой Концепции неких членов этого региона, признавшихся Москве в своей серьёзной озабоченности в предыдущих документах. В частности, речь идет об Украине, Грузии и Молдавии, что заставляет призадуматься. Так, в Концепции 2013 года в разделе региональных приоритетов отдельно были упомянуты Украина (как приоритетный партнёр в СНГ), в Концепции 2016 года в данном разделе списка формулировка об Украине изменена на то, что Россия

[80] Там же.

«заинтересована в развитии всего многообразия политических, экономических, культурных и духовных связей с Украиной». А в Концепции 2023 года о связи с Украиной уже не упоминается. Говорится лишь о том, что «США и их саттелиты использовали принятые РФ меры по защите своих интересов на украинском направлении как предлог для обострения многолетней антироссийской политики и развязали гибридную войну нового типа»[81].

В новой концепции также не упомянута Грузия, хотя в прошлой редакции (пункт №59) говорилось о заинтересованности Москвы в нормализации отношений с Тбилиси[82], однако, остались пункты, касающиеся Абхазии и Южной Осетии: «Российская Федерация намерена уделять приоритетное внимание всеобъемлющей поддержке Республики Абхазия и Республики Южная Осетия, содействию добровольного выбора народов этих государств в пользу углубления интеграции с Россией»[83].

Восприятие Приднестровского конфликта долгие годы на бумаге не менялось. Для его решения Россия сначала руководствовалась принципами территориальной целостности и нейтралитета Молдавии, позже – «определением особого статуса Приднестровья», что звучало примерно так: «Молдавия не должна вступать в НАТО, тогда при учёте автономии ПМР может вернуться в состав государства»[84]. Именно такие принципы прописывались в текстах 2013 и 2016 годов. А в новой Концепции удалена привычная формулировка об уважении суверенитета и нейтралитета Молдавии. Пусть и это не означает, что Кремль хочет силой забрать Приднестровье, которое годами стремилось войти в состав России, стоит рассматривать это как некий тревожный сигнал для Кишинёва. В этом

[81]Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В. В. Путиным 31 марта 2023 г.) [Электронный ресурс] // МИД РФ [Официальный сайт]. 2023. URL: https://www.mid.ru/ru/detail-material-page/1860586/ (дата обращения: 20.04.2023).

[82] Указ президента Российской Федерации об утверждении Концепции внешней политики Российской Федерации [Электронный ресурс] // Президент России [Официальный сайт]. 2016. http://www.kremlin.ru/acts/bank/41451/print(дата обращения: 25.05.2023).

[83] Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В. В. Путиным 31 марта 2023 г.) [Электронный ресурс] // МИД РФ [Официальный сайт]. 2023. URL: https://www.mid.ru/ru/detail-material-page/1860586/ (дата обращения: 20.04.2023).

[84] Токарев Андрей. С Белоруссией, без Молдавии и Грузии: постсоветское пространство в новой концепции внешней политики [Электронный ресурс] // Российский совет по международным делам [Официальный сайт]. 2023. URL: https://russiancouncil.ru/analytics-and-comments/analytics/s-belorussiey-bez-moldavii-i-gruzii-postsovetskoe-prostranstvo-v-novoy-kvp/(дата обращения: 18.05.2024).

ключе образные аналогии спецпредставителя по Приднестровью Дмитрия Рогозина помогали понять возможные последствия неразумного выбора со стороны власти Молдавии: при ускоренном движении в НАТО на поворотах «молдавский поезд отдельные вагоны может и потерять»[85].Таким образом, обновлённый текст стратегического документа внешней политики намекает некую возможность дальнейшего расширения и самого постсоветского пространства, и государственности его отдельных членов при напряжённости отношений между Россией и Западом.

5.«Многополярный мир» является центральным понятием новой редакции Концепции и упоминается в ней неоднократно. С середины 1990-х годов содействие построению многополярного мира является одной из основных целей внешней политики России, а создание и укрепление положения России как самостоятельного «полюса» многополярного мира – главной задачей реализации российской внешней политики. В сложившихся условиях новых угроз и вызовов, Россия рассматривает устранение рудиментов доминирования США и других недружественных государств в мировых делах с целью создания условий для отказа любого государства от неоколониальных и гегемонистских амбиций как одну из приоритетных задач для содействия развитию многополярного мира. К тому же, Российская Федерация уделяет приоритетное внимание укреплению потенциала и повышению международной роли межгосударственного объединения БРИКС, ШОС, СНГ, ЕАЭС, ОДКБ и других межгосударственных объединений и международных организаций, а также механизмов с весомым участием России. Вместе с тем, незападные страны, представленные Китаем, Индией, Африкой и т.д., по-настоящему поднимаются в дипломатическую стратегию России. В этом плане, прошедший 27-28 июля в Санкт-Петербурге саммит «Россия-Африка» стал знаковым событием в реализации внешней политики Москвы, свидетельствующим о кардинальном изменении мировоззрения и международного позиционирования страны в отношении растущего незападного большинства в мире, заложенном в недавно принятой Концепции внешней политики. Возрожденный

[85] Там же.

интерес России к Африке носит не столько тактический, сколько стратегический характер. Он выходит далеко за рамки таких важных, но обыденных вопросов экономического сотрудничества, безопасности и технологического взаимодействия. В стратегическом плане российское руководство и политические элиты все чаще рассматривают Африку – наряду с Азией и Латинской Америкой – как часть восходящей волны, вместе с которой Россия сможет заменить нынешний мировой порядок с доминированием Запада на более диверсифицированную конструкцию, построенную на основе нескольких цивилизаций.

6.В новой Концепции выделяется прагматизм и гибкость внешней политики России. Как отметил вице-спикер Совета Федерации К. И. Косачев «Отношение России к другим государствам будет зависеть от их отношения к нам»[86], внешние отношения России строятся на принципе прагматизма и ведется с высокой степенью гибкости. На примере российско-европейских отношений в тексте 2016 года выделяется пункт №65: «Визовый режим остаётся одним из основных барьеров на пути развития контактов между Россией и ЕС. Поэтапная отмена визового режима на взаимной основе станет мощным импульсом для укрепления сотрудничества России и ЕС в экономической, гуманитарной, культурной, образовательной и иных областях»[87]. Из-за СВО Евросоюз приостановил соглашение об упрощении визового режима с Россией, который был в силе с 2007 года, вместе с тем, Москва внесла всех членов ЕС в список «недружественных» стран. На этом фоне в «Концепции-2023» не оставлен вышесказанный пункт, вместо этого, упоминается, что большинство государств Европы проводят агрессивную политику против России. Однако подчеркивается безальтернативность мирного сосуществования с европейскими странами и необходимость сформировать новую модель отношений с ЕС. Аналогично, «Концепция-2023» также лишена содержания о выполнении Договора между Российской Федерацией и Соединенными

[86]Вице-спикер Совфеда Косачев дал оценку новой концепции внешней политики РФ[Электронный ресурс] // Российская газета [Официальный сайт]. 2023. https://rg.ru/2023/03/31/otnoshenie-rossii-k-drugim-gosudarstvam-budet-zaviset-ot-ih-otnosheniia-k-nam-vice-spiker-sovfeda-kosachev-dal-ocenku-novoj-koncepcii-vneshnej-politiki-rf.html (дата обращения: 25.05.2023).

[87]Указ президента Российской Федерации об утверждении Концепции внешней политики Российской Федерации [Электронный ресурс] // Президент России [Официальный сайт]. 2016. http://www.kremlin.ru/acts/bank/41451/print(дата обращения: 25.05.2023).

Штатами Америки о мерах по дальнейшему сокращению и ограничению стратегических наступательных вооружений от 8 апреля 2010 года, которому Россия придает важное значение в Концепции 2016 года. Хотя в Концепции неоднократно критикуется негативное влияние США и Запада на российскую и международную безопасность, Вашингтон прямо назван главным инициатором и проводником антироссийской линии, однако особо подчеркивается то, что «Россия не считает себя врагом Запада, не изолируется от него, не имеет по отношению к нему враждебных намерений»[88]. Хотя Россия не испытывает оптимизма по поводу перспектив развития российско-западных отношений, всё же готова вернуться к прагматичному сотрудничеству с Западом.

В свете вышесказанного можно констатировать, что обновлённая внешнеполитическая стратегия России ориентирована на обслуживание внутренней политики с целью обеспечения безопасности России и создания благоприятных внешних условий для ее развития. Российское руководство внесло существенные коррективы во внешнюю политику, которая в целом демонстрирует тенденцию к стратегическому сжатию. Она характеризуется стремлением к минимизации стратегических издержек при одновременном обеспечении своих ключевых интересов за счет накопления и концентрации стратегических ресурсов в приоритетных направлениях. В ответ на недружественные действия Запада Россия намерена концентрировать созидательную энергию на географических векторах своей внешней политики, которые имеют очевидные перспективы с точки зрения расширения взаимовыгодного международного сотрудничества, в частности не западные государства и организации. При этом значение Ближнего зарубежья в дипломатической стратегии России стало более заметным.

Правовая основа настоящего исследования базируется на двух основополагающих документах: Стратегии национальной безопасности 2021 года («Стратегия-2021») и Концепции внешней политики 2023 года («КВП-2023»). Будучи

[88]Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В. В. Путиным 31 марта 2023 г.) [Электронный ресурс] // МИД РФ [Официальный сайт]. 2023. URL: https://www.mid.ru/ru/detail-material-page/1860586/ (дата обращения: 20.04.2023).

«дорожной картой для МИД и других ведомств России»[89], эти документы предоставляют ключ к пониманию особенностей реагирования России на гибридные войны и гибридные угрозы как с точки зрения внутренней, так и внешней политики страны. Так, в «Стратегии-2021» основное внимание уделяется внутренней политике России, подчёркивается важность суверенной независимости, политической стабильности, межнационального согласия, культуры и нравственности и т.д. для противодействия гибридных угроз и обеспечения безопасности страны. А «КВП-2023» устанавливает стратегические приоритеты России во внешней политике в ответ на гибридные войны недружественных стран, положив в основу практические действия страны в среднесрочной и на более отдалённую перспективу[90].

[89]Ларионов Петр. В МИД раскрыли детали проекта Концепции внешней политики России [Электронный ресурс] // Парламентская газета [Официальный сайт]. 2022. https://www.pnp.ru/politics/v-mid-raskryli-detali-proekta-koncepcii-vneshney-politiki-rossii.html (дата обращения: 25.05.2023).

[90]Совещание с постоянными членами Совета Безопасности [Электронный ресурс] // Президент России [Официальный сайт]. 2023. http://www.kremlin.ru/events/president/transcripts/70810(дата обращения: 25.05.2023).

1.2. Современные гибридные войны как предмет политологического анализа

В последние десятилетия международные процессы всё более усложняются; возникают новые вызовы и угрозы международной безопасности, мало подверженные традиционным инструментам дипломатии. Вместе с тем под воздействием глобализации и информатизации современный мир находится на столь высоком уровне взаимозависимости, что любое применение силы в форме прямой вооруженной агрессии (осуществляемой традиционными силами и средствами вооруженной борьбы) в любой точке земного шара может привести к глобальной войне и последующей за ней катастрофе. Достигнутое на сегодняшний день стратегическое равновесие сил взаимоуничтожения у ведущих стран мира также делает риск применения вооруженных сил для решения локальных проблем неприемлемым: любой локальный конфликт, в котором участвуют хотя бы две ведущих мировых державы, обладающих ядерным потенциалом, в любой момент может стать новой ядерной войной, в которой победителей не будет. В этих условиях применение традиционных вооруженных сил становится рискованным; применение же различных средств непрямой агрессии, исключающих прямое столкновение соперников «лоб-в-лоб», но при этом дающее им возможность «меряться силами» на территории третьих стран или в информационном, ментальном, когнитивном, кибернетическом пространствах, напротив, получило приоритетное значение. Так в геополитическом соперничестве великих держав (России, США, КНР) выдвинулись на передний план методы и технологии информационных, торговых (санкционных), дипломатических и ментальных войн, которые, в совокупности с методами, выработанными частными военными компаниями, картелями, повстанцами-партизанами, получили общее название гиб-

ридных войн. Все это привело к революции в концепциях и технологиях военного дела, которое тоже стало гибридным (то есть, сочетающим в себе классические и неклассические формы и методы вооруженной борьбы). Вопрос встал только за описанием и формализацией этого нового явления – на уровне создания нового понятийного аппарата или адаптации прежнего (взятого у классических войн) к новым реалиям.

С этой целью на Западе, в России и Китае независимо другу от друга был выдвинут ряд новых концепций, описывающих гибридные свойства современной войны. Однако не все из них прошли проверку временем. Как писал президент Академии военных наук генерал армии М. А. Гареев, «Авторы, падкие на сенсации, чуть ли не каждый день войнам будущего дают новые названия: трёхмерная, сетевая, асимметричная, бесконтактная, информационная и т.д. Да, все эти элементы будут иметь место, они отражают одну из характерных черт военного противоборства, но ни один из них в отдельности не характеризует облик войны в целом»[91]. Это высказывание в целом верно отражает действительность, в которой сущность и содержание гибридных форм войны требует систематизации и научного, в первую очередь, осмысления.

На сегодняшний день широко используемым в политической и экспертной среде стал термин «гибридная война», понимаемый как «зонтичный» термин, вобравший в себя чрезвычайно широкий диапазон видов современной международной борьбы (от классической до неклассической). Стоит отметить, что «зонтичный бренд» (англ. umbrella brand) – термин, пришедший из маркетинга, первоначально относился к виду стратегии расширения бренда, заключающийся в выпуске под одной маркой сразу нескольких групп товаров или товарных категорий, при этом в названии товаров доминирует имя компании-производителя, а в рекламе продукции компании демонстрируется её логотип. Данное понятие применительно к гибридным войнам используют такие ученые, как Саймонс Г., Евстафьев Д. Г., Манойло А. В., Стригунов К. С.и т.д. Говоря, что гибридная война

[91] Гареев М. А. Характер будущих войн // Право и безопасность. – 2003. – № 1–2.– С. 23–31.

представляет собой зонтичный бренд для различных видов вооруженной и невооруженной борьбы, имеют в виду, что данные виды борьбы используются в гибридных войнах в комбинированном виде, приобретая при этом гибридные черты. Так появляются гибридные цветные революции (типа попытки государственного переворота в Беларуси в 2020 году или внестоличная цветная революция в Боливии в 2019 году), гибридные информационные войны (в которых классические вооруженные конфликты становятся «конвейером» для производства пиар-новостей – см. работы Ж. Бодрийяра), гибридные торговые войны (США-КНР) и т.д.

Происхождение и развитие термина «гибридная война»

В настоящее время термин «гибридная война» продолжает оставаться предметом для дискуссий. Принято считать, что этот термин появился с 1990-х годах в связи с анализом «гибридных угроз» военными теоретиками США[92]. При этом он использовался в документах военного планирования США при формулировании угроз современного мира уже в начале 2000-х годов[93]. Несмотря на то, что существуют разные версии о том, кто именно первым публично ввёл данный термин в оборот (в качестве варианта данного вопроса предполагают Тома Мокайтиса[94], Уильяма Дж. Немета[95] и Фрэнка Г. Хоффмана), большинство исследователей сходится во мнении, что именно Фрэнк Г. Хоффман является «отцом-

[92] См., напр.: Robert G. Walker, Spec Fi: The United States Marine Corps and Special Operations. Master's thesis. Naval Postgraduate School, 1998; Mattis J. N., Hoffman F.G. Future Warfare: The Rise of Hybrid Wars // Proceedings. – 2005.– Vol. 132, №11; Hoffman F.G. Complex Irregular Warfare: The Next Revolution in Military Affairs. Orbis. – 2006. – Vol. 50, № 3. – P. 397–399; McCuen J. J. Hybrid Wars // Military Review. – 2008. – Vol. 88, Issue 2. – P. 107–113.; Gentile Gian P. The Imperative for an American General– Purpose Army That Can Fight // ORBIS. – 2009. – Vol. 53, № 3. – P. 457–470; Glenn Russell W. Thoughts on 'Hybrid' Conflict [Электронный ресурс] // Small Wars Journal. 2009. URL: https://small warsjournal.com/jrnl/art/thoughts-on-hybrid-conflict (дата обращения: 10.02.2021); Cilluffo F.J., Clark J.R. Thinking About Strategic Hybrid Threats: In Theory and in Practice // PRISM.–2014. – Vol. 4, Issue 1.– P. 47– 63.

[93] П. А. Цыганков и др. Гибридные войны в хаотизирующемся мире XXI века: сборник под редакцией. П. А. Цыганкова [и др.]. – М: Издательство Московского университета. – 2015. – С. 19.

[94] Buţa V., Vasile V. Persectives on the evolution and influenct of the hybrid warfare concept // Romanian Military Thinking. – 2015. – № 3. – С.11–32; Popescu N. Hybrid tactics: Russia and the West // European Union Institute for Security Studies, Alert. – 2015.– № 46.– С.1–2; Solmaz T. 'Hybrid Warfare': One Term, Many Meanings [Электронный ресурс] // Small Wars Journal. 2022. URL: https://smallwarsjournal.com/jrnl/art/hybrid-warfare-one-term-many-meanings (дата обращения: 20.02.2022).

[95] Бурило Е. А. «Цветные революции» как разновидность политического конфликта // Будущее науки. Сборник научных статей 7–й Международной молодежной научной конференции. Курск: Юго-Западный государственный университет, 2019. – С 289–292; Dominioni S., Tafuro Ambrosetti E. Russia's Hybrid Strategy: Mythor Reality? [Электронный ресурс] // Italian Institute for International Political Studies (ISPI) [Официальныйс айт]. URL: https://www.ispionline.it/en/pubblicazione/russias-hybrid-strategy-myth-or-reality-26805 (дата обращения: 05.04.2022); Królikowski H. Hybrid Threats and Warfare, Are We Really Facing Something New? // Internal Security. – 2017. –Vo.~9, Is.2. – P. 9–21.

основателем» концепции «гибридной войны», закрепив данный термин с системным анализом к этому новому типу угрозы[96]. К тому же, из-за заблуждения западных авторов «российская гибридная война» у зарубежных исследователей и аудитории также известна как «Доктрина Герасимова»[97].

Один из основных разработчиков теории гибридных войн – американский военный эксперт Фрэнк Хоффман, который в 2007 году опубликовал монографию под названием «Конфликты XXI века: рост гибридных войн». В этой книге он отметил, что форма современной войны меняется, традиционная «крупномасштабная регулярная война» и «мелкомасштабная нерегулярная война» постепенно превращаются в своего рода «гибридную войну» с более размытыми границами и более интегрированными стилями ведения боя[98], что и стало отправной точкой для размышлений и дискуссий на данную тему.

Теория Ф. Хоффмана о гибридных войнах получила широкое распространение в оборонной сфере США на рубеже 2000-х и 2010-х годов. С 2009 года данная теория стала постепенно доминировать в военном строительстве и боевой учёбе Вооружённых сил США; она стала известной широкому кругу специалистов. В 2010 году в «Четырёхлетнем обзоре состояния национальной обороны» (QDR) США теория гибридных войн фактически признана частью военной стратегии США в реагировании на разнообразные (и тоже гибридные по своей природе) угрозы безопасности[99]. В 2015 году, обвиняя Россию в ведении гибридных войн в Крыму и на Украине, в «Национальной военной стратегии» США стали рассматривать гибридные войны в качестве главной угрозы, для противостояния которой американским военным необходимо скорректировать свою оборонную

---

[96] Анапских И. А. и др. Западная Европа как фронт гибридной войны // Юридическая наука: история и современность. – 2020. – № 12. – С. 164–188; Круглов В. В., Воскресенский В. Г., Мурсаметов В. Я. Анализ взглядов военных теоретиков ведущих зарубежных государств на содержание и ведение современных и будущих войн // Военная мысль. – 2021. – № 7. – С.120–129; Пушкина М.А., Чирков П. С. Теория современных гибридных вой н // Аллея науки. – 2017. – Т. 2, № 8. – С.629–642; Фридман О. «Гибридная война» понятий // Вестник МГИМО – Университета. – 2016. – Т. 50, № 5.

[97] Mark Galeotti. I'm Sorry for Creating the 'Gerasimov Doctrine' [Электронный ресурс] // Foreign Policy. 2018. URL: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ (дата обращения: 15.12.2021).

[98] Frank Hoffman. Conflict in the 21st Century: The rise of Hybrid War. – Potomac Institute for Policy Studies, 2007. P. 17– 34.

[99] Quadrennial Defense Reviewe Report February 2010 [Электронный ресурс] // The U.S. Department of Defense. 2019. URL: https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDRasof29JAN10_1600.pdf (дата обращения: 05.04.2022).

стратегию. Именно в этом году в России был проведён ряд научных мероприятий, посвящённых исследованию феномена «гибридной войны»[100]. В том числе, в конце января 2015 года в Военном университете Министерства обороны РФ прошёл межвузовский круглый стол «Гибридные войны XXI века». В феврале 2015 года на факультете политологии МГУ им. М. В. Ломоносова был проведён научный семинар «Гибридные войны в хаотизирующемся мире XXI в.», а в мае того же года на факультете социологии и политологии Финансового университета при Президенте РФ был организован научный семинар по теме «Гибридные войны как феномен XXI в.»[101]. Одним из наиболее мощных стимулов к осмыслению и продвижению данного термина стал государственный переворот на Украине в 2013-2014 годах, начавшийся с гибридной цветной революции («Евромайдана») и получивший свое продолжение в виде гибридной же войны на юго-востоке страны (Донбасс). По мере проведения подобных мероприятий данный термин стал быстро распространяться в научном и политическом лексиконе России.

Таким образом, украинский конфликт, начавшийся в конце 2013 года («Евромайдан»), стал важной вехой в процессе исследования теории гибридных войн, не только для Запада, но и для России. После кульминации украинского кризиса в 2013-2014 годах на Западе началась так называемая реконцептуализация терминологии «гибридных войн». В российском дискурсе до украинских событий интерес к гибридным войнам сохранялся на уровне наблюдения и обсуждения того, как западные специалисты теоретизируют по поводу войн XXI в., при этом в основном это было интересно узкому кругу профессиональных военных и военно-академическому сообществу[102]. Однако после того, как Запад начал обвинять Россию в ведении гибридных войн на Украине, её исследования в России резко активизировались и довольно быстро вышли на новый качественный уровень, вплоть до сегодняшнего дня, когда она уже стала не только доминирующим

[100] Белозёров В. К., Соловьёв А. В. Гибридная война в отечественном политическом и научном дискурсе // Власть. –2015. – № 9. – С. 5–11.
[101] Там же.
[102] Фридман О. «Гибридная война» понятий // Вестник МГИМО – Университета. – 2016. – № 5(50). – С. 79–85.

инструментом в межгосударственных противоборствах, но и популярной темой в дискуссии широкой аудитории (включающих в себя не только профильных специалистов, но и представителей общественности и СМИ).

Стоит отметить, хотя термин «гибридная война» был впервые введён военными США, он не является оригинальным изобретением американцев, а естественным этапом эволюции ситуации в области международной безопасности и форм ведения войны. Хотя на предварительном этапе исследования феномена гибридных войн некоторые авторы были склонны считать её новым типом ведения боя, однако, с расширением и углублением исследований по данной тематике, всё больше экспертов и учёных утверждают, что в нем нет ничего нового, ведь гибридные методы и мышление существуют на протяжении всей военной истории. Как отметил член-корреспондент Академии военных наук Бартош А. А., «гибридность – свойство любой войны, поскольку противоборствующие стороны обязательно стремятся применять все имеющиеся в их распоряжении силы, средства и способы ведения боевых действий»[103].Исторические предпосылки данного неологизма прослеживаются у классиков военной стратегии крупных империй Древнего мира, в частности, гибридные идеи о войне часто связывают с классиками по размышлению существа войны, изменения элементов философии войны и науки о войне в ее целом. К этому числу авторов относятся китайский стратег и мыслитель Сунь-Цзы[104], византийский император Маврикий[105], выдающийся прусский военный теоретик Клаузевиц К. Ф.[106], офицер британской армии Чарльз Каллвелл[107]и русскийученый-геополитик Снесарев А.Е. [108]. Так, военный трактат «Стратегикон», написанный византийским императором Маврикием в VI веке н. э., посвящён тактике войны с «недисциплинирован-

[103] Бартош А. А. Стратегия и контрстратегия гибридной войны // Военная мысль. – 2018. – №10. – С. 5–20.
[104] Сунь Цзы. Искусство войны / [пер. с древнекит. Н. Кондрата]. – М.: Издательство АСТ. Москва, 2018.; «Гибридные войны» в хаотизирующемся мире XXI века / под. ред. П. А. Цыганкова. – М.: Изд– во МГУ, 2015. – С. 71.
[105] Цит. по: Boot M. Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present. – N.Y.: W.W. Norton, 2013. – P. 54.
[106] Клаузевиц К. О войне.– М.: Госвоениздат, 1934. – 692 с.
[107] Callwell E. Small Wars: Their Theory and Practice of Irregular Warfare.— M.: CreateSpace Independent Publishing Platform, 2016. – 438 с.; Калдор М. Культура новых войн // Логос. – 2019. – Т. 29. – № 3(130). – С. 1–21.
[108] Снесарев А.Е. Философия войны. – М.: Ломоносовъ, 2013. – 283 с.

ными, неорганизованными народами»[109]. Для описания подобных военных конфликтов также широкоиспользовался термин «малая война», который был введен в конце 19 века офицером британской армии Чарльзом Каллвеллом. В своей одноимённой классической работе «Малые войны», опубликованной в 1896 году, Чарльз Каллвелл определил «малые войны» как «любые военные кампании помимо тех, в которых с каждой воюющей стороны выступают только регулярные войска»[110]. Данный термин даже считается наиболее релевантным для понимания нерегулярного конфликта 21-го века[111].

Понятие и особенность «гибридной войны»

Сегодня в научной литературе встречается множество вариантов трактовок данного термина, при этом общепринятых определений нет – они еще не сведены к одному знаменателю. В том числе, по одному из наиболее авторитетных и часто используемых определений, гибридная война – это «Использование военных и невоенных инструментов в интегрированной кампании, направленной на достижение внезапности, захват инициативы и получение психологических преимуществ, используемых в дипломатических действиях, масштабные и стремительные информационные, электронные и кибероперации, прикрытие и сокрытие военных и разведывательных действий в сочетании с экономическим давлением»[112].

Верный, с нашей точки зрения, подход к определению современной гибридной войны как комбинации различных видов и форм вооруженной и невооруженной борьбы в данном определении отчасти нивелируется односторонностью, когда явление пытаются определить через объяснение его составляющих – приравнять отдельные черты и компоненты «гибридной войны» к самому явлению （их « совокупности»） .Другие известные определения гибридной войны в

[109] Boot M. Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present. – N.Y.: W.W. Norton, 2013. – P. 54.
[110] Whittingham D. Warrior-Scholarship in the Age of Colonial Warfare: Charles E. Callwell and Small Wars // The Theory and Practice of Irregular Warfare: Warrior–Scholarship in Counter–Insurgency / A. Mumford, B. C. Reis (eds).– L.: Routledge, 2014. – P. 18-34.
[111] Калдор М. Культура новых войн // Логос. –2019. – Т. 29. –№ 3(130). – С. 1–21.
[112] The Military Balance 2015. – By the International Institute for Strategic Studies. – P. 5–6; См.: Данюк Н.С. Внешняя политика Российской Федерации (2000-2016 гг.) и феномен «цветных революций»: дисс. ... канд. истор. наук: 07.00.15. – М., 2018. – 312 с.

основном строятся по такому же – субъективному (зависящему от наблюдательности конкретного автора) – принципу. Такой способ определения понятия основывается на внешнем виде вещи и часто приводит к тому, что понятие оказывается недостаточно глубоким и не отражает более существенного содержания.Более того, взгляды различных авторов на суть гибридных войн настолько различаются, что можно разделить их на несколько направлений (или «школ», понимая под школами наиболее крупные и проработанные направления, имеющие своих сторонников) по данной тематике; их описание и классификация подробно представлены в разделе 1.3.

В целом восприятие данного термина делится на два вида: в широком смысле гибридная война включает в себя как классические военные конфликты, так и различные невоенные противоборства, то есть вооружённые методы являются подмножеством арсенала гибридных войн, помимо которых существует и широкий диапазон средств противоборства ненасильственного в традиционном понимании характера; в узком смысле к гибридным войнам относятся различные формы борьбы с комплексным использованием невоенных средств; в отличие от традиционного вооружённого конфликта, в этом случае «гибридная война» и «традиционная война» (военный конфликт) являются взаимоисключающими формами международного противоборства.

В западном дискурсе, а также в большинстве российских исследований по данной тематике, термин «гибридная война» воспринимается и применяется чаще всего в его широком смысле. Однако анализ последних выступлений официальных представителей России в контексте СВО позволил выяснить, что в дискурсе российского правительства «гибридная война» используется в узком смысле. Так, в августе 2022 года секретарь Совета безопасности РФ Н. П. Патрушев отметил, что Запад развязал против России гибридную войну и балансирует на грани открытого вооружённого конфликта[113], а в январе 2023 года глава МИД РФ С. В. Лавров заявил, что происходящее на Украине – это уже не гибридная, а на-

[113] Патрушев заявил, что Запад балансирует между гибридной войной и открытым конфликтом с РФ [Электронный ресурс] // ТАСС.2022. URL: https://tass.ru/politika/15511991 (дата обращения: 10.01.2023).

стоящая война Запада с Россией[114]. К тому же, стоит отметить, что характер одного и того же конфликта может варьироваться в зависимости от рассматриваемого субъекта (схема 1).

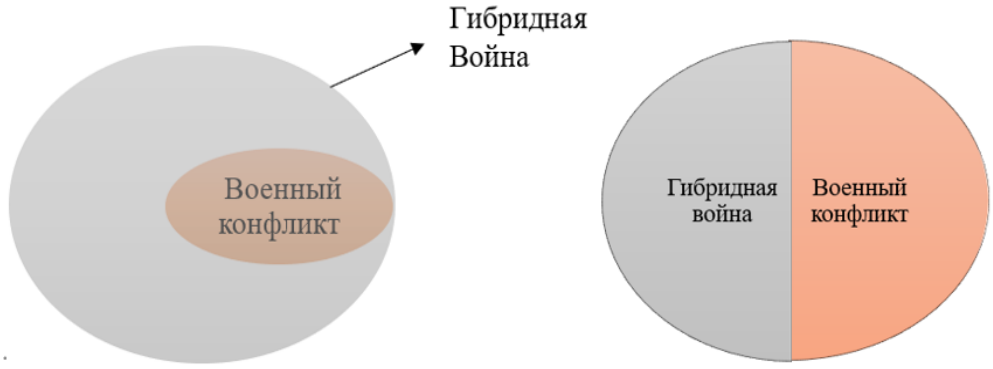


Схема 1. Соотношение между гибридной и традиционной войной (открытым военным конфликтом)

На примере сегодняшнего конфликта на Украине – вооружённый конфликт, безусловно, является гибридной войной в широком смысле, однако с точки зрения узкого смысла данного термина характер происходящего на Украине варьируется: для его прямых участников СВО – это пример классической общевойсковой операции между Россией и Украиной, но с учётом его косвенных участников – это типичная гибридная война США и их союзников против России руками прокси, в роли которых выступают режим Зеленского и другие прямые участники конфликта, воюющие против России.

Несмотря на вышеупомянутые различия взглядов на гибридные войны, большинство учёных сходятся во мнении о наличии у нее особенностей, таких, как многомерность, скрытость («необъявленная война»), многообразие акторов и т.д.

Самой яркой особенностью гибридных войн является её скрытость и многообразность её инструментария. В отличие от классической войны, гибридная война характеризуется высокой степенью скрытости и часто ведется без официального объявления. В гибридной войне размыты границы начала и окончания военных действий, фронта и тыла, что создает трудности для обнаружения ее

[114]Лавров заявил, что Россия ведёт с Западом уже не гибридную войну [Электронный ресурс] // РИА НОВОСТИ. 2023. URL: https://ria.ru/20230123/rossiya-1846778090.html (дата обращения: 28.01.2023).

признаков будущей жертвой агрессии и не меньшие трудности – в противостоянии ей. Кроме того, гибридная война ведётся во всех основных сферах жизнедеятельности общества с использованием широкого спектра инструментов, в том числе, невоенных средств, таких, как информационные операции; более того, нередко эти средства невооруженной борьбы играют решающую роль, а чисто военные средства – сервисную. Тем более, что в гибридных войнах внутренние аспекты ситуации в стране гораздо важнее, нежели внешнеполитические с точки зрения оценки «выигрыш/проигрыш», что принципиально меняет модель управления конфликтами, выводя на передний план проблематику сохранения социальной и социально-политической устойчивости[115].

Другой важной особенностью гибридных войн является полифилия и высокий уровень адаптивности её участников. Эту форму противостояния могут использовать различные игроки, как государственные, так и негосударственные, включая частные компании, наёмников, транснациональные и трансграничные криминальные группировки (в частности, наркокартели), экстремистские и террористические организации и т.д.: в гибридных войнах именно их вооруженные формирования используются вместо регулярных вооруженных сил[116]. Такая неунифицируемость участников гибридных войн, с одной стороны, затрудняет управление всеми видами акторов и ведет к сетецентричности современных гибридных войн, с другой стороны, это несёт в себе и некоторые преимущества для ведения гибридных действий: можно собрать необходимые ресурсы для операции прямо на месте (на избранном театре военных действий). Более того, при необходимости можно быстро и безболезненно вывести того или иного актора из ситуации, причём не только в форме «эвакуации», но и объявляя его враждебной силой. В этом и заключается привлекательность модели современных гибридных войн.

Термины, смежные с термином «гибридная война»

[115] Шеллинг Т. Стратегия конфликта. – М.: ИРИСЭН, Социум, 2014. – С. 98.
[116] Манойло А. В., Евстафьев Д. Г. Гибридные войны в контексте постглобализации // Контуры глобальных трансформаций: политика, экономика, право. – 2021. – Т. 14, № 4. – С. 160–175.

До широкого распространения неологизма «гибридная война» или практически одновременно с ним в экспертной среде существовал ряд смежных концепций, таких, как «управляемый хаос», «неограниченная война», по своей сути очень близких к современному пониманию гибридных войн. Эти концепции представляют собой теоретический базис, фундамент для теории гибридных войн, что, в свою очередь, требует тщательного изучения их особенностей, повлиявших на генезис современных представлений о гибридных войнах[117].

Термин «управляемый хаос» в своей первоначальной версии заимствован американскими аналитиками из физики. В 80-е годы XX века разработка теории «управляемого хаоса» проводилась на базе американского Института междисциплинарных исследований Санта-Фе, который открылся в 1984 году и специализировался именно на теории хаоса. В конце прошлого века, когда у США встала актуальная потребность радикального переустройства мира под стандарты единственной сверхдержавы, активизировались исследования по применению технологии «управляемого хаоса» в социальных процессах. В этом контексте, в 1992 году на конференции данного института, выступая с докладом «Теория хаоса и стратегическая мысль», Стивен Манн осуществил сопряжение этой теории с новыми (на тот момент) геополитическими концепциями завоевания мирового превосходства. Так термин «управляемый хаос» вошел в политические науки.

Среди основных идеологов данной теории также часто называют имя Дж. Шарпа, упоминая в данной связи его классический труд «От диктатуры к демократии»[118]. Однако Дж. Шарп в своих работах представил скорее методы создания «управляемого хаоса», а не саму концепцию. Для комплексного понимания теории «управляемого хаоса» интерес представляют, прежде всего, работы С. Манна, который в 1998 году прямо обрисовал американскую стратегию использования хаоса в интересах США: «Мы должны быть открыты перед возможностью усиливать и эксплуатировать критичность, если это соответствует нашим

[117] Манойло А. В., Стригунов К. С. Технологии неклассической войны. Генезис. Эволюция. Практика. – М.: Горячая линия – Телеком, 2020. – С. 52.
[118] Шарп Дж. От диктатуры к демократии: Стратегия и тактика освобождения / пер. с англ. Н. Козловской –М.: Новое издательство, 2005. – 84 с.

национальным интересам… Наш национальный интерес приоритетнее международной стабильности. В действительности, сознаем это или нет, мы уже предпринимаем меры для усиления хаоса, когда содействуем демократии, рыночным реформам, кода развиваем СМИ через частный сектор»[119].

Согласно С. Ману, для создания хаоса на той или иной территории существуют следующие средства:

1) содействие либеральной демократии, сутью которой является формирование и внедрение проамериканской позиции;

2) поддержка рыночных реформ – для того чтобы манипулировать экономическими факторами противника (как это и было осуществлено в России в 1990-е годы);

3) повышение жизненных стандартов у населения, прежде всего, в среде элиты: «продажная и коррумпированная элита легко поддаётся управлению, и против неё гораздо проще настроить население»[120];

4) вытеснение ценностей и идеологии: «связи в культуре и традициях часто сплачивают народы в кризисных ситуациях, а нарушение таких связей в стране-мишени уничтожит общину внутри её народов»[121].

Теория «управляемого хаоса» послужила основой и руководством для США в создании хаоса в тех или иных регионах, разжигании гибридных войн и цветных революций, а также подрыва режимов противника. Все цветные революции в странах Ближнего Востока, Северной Африки и Центральной Азии были успешными примерами применения стратегии «управляемого хаоса». Хотя их кульминация пришлась на 2010-е годы, и «Арабскую весну», в частности, Соединённые Штаты неустанно разыгрывают этот сценарий и сегодняшний конфликт между Россией и Украиной является типичным примером влияния «управляемого хаоса». Считая хаос управляемым, США пытаются использовать глобальную нестабильность для ослабления стратегических конкурентов, что

[119] Вашингтон ставит на «управляемый хаос» [Электронный ресурс] // Независимая. 2018. URL: https://www.ng.ru/armies/2018-04-10/8_7208_washington.html (дата обращения: 20.05.2021).
[120] Mann S. R. The Reaction to Chaos // Complexity, Global Politics, and National Security. – 1997. – P. 62–68.
[121] Mann S. R. Chaos Theory in Strategic Thought // Parametes. – 1992. – Vol. 22, № 1.– P. 54–68.

способствует созданию глобальной хаотизации и ведёт к глобальным катастрофическим последствиям.

Одной из концепций, сопряжённых с концепцией «управляемого хаоса», являются «операции, базирующиеся на достижении эффектов» (ОБДЭ – effects-based operations). Данная концепция официально предложена американским генералом Дэвидом Дептула в 1990-х годах. В монографии «Операции, базирующиеся на достижении эффектов: изменение в природе войны», Дэвид Дептула рассматривает ОБДЭ как новую форму войны с серьёзным потенциалом[122]. Монография и изложенная в ней концепция сразу вызвали резонанс в научных и военно-политических кругах США[123]. Благодаря этому уже в начале XX века концепция ОБДЭ стала привлекать широкое внимание высших эшелонов вооружённых сил США. Так, в «Совместной публикации 3-0, Доктрина для объединённых операций» (Joint Pub3-0, Doctrine for Joint Operations) 2006 года множество раз подчёркиваются эффекты в планировании и оценке военных операций с акцентом на установлении «взаимосвязи между задачей, эффектом и целью»[124].

Стратегия ОБДЭ исходит из того, что в военных операциях необходимо фокусироваться скорее на оказании влияния на поведение противника, нежели только на уничтожение его вооружённых сил. Вместе с тем в ней подчёркивается необходимость координации и управления всеми элементами национальной мощи для достижения желательных эффектов при решении задач в сфере национальной безопасности[125]. Так, согласно определению исследовательского центра RAND Corp., ОБДЭ – это «операции, понимаемые и планируемые в системном фрейме, которые рассматривают весь диапазон прямых, непрямых и каскадных эффектов, способных с различной степенью вероятности быть достигнутыми через применение военных, дипломатических, психологических и экономических

[122] Deptula D. A. Effects–Based Operations: Change in the Nature of Warfare. – Arlington VA: Aerospace Education Foundation. Defense and Airpower Series, 2001. – P. 8–9.
[123] Rickerman L.D. Effects–Based Operations: A New Way of Thinking and Fighting. – Fort Leavenworth, KS: School of Advanced Military Studies, Army Command and General Staff College, 2003. – P. 15–16.
[124] U.S. Joint Chiefs Staff. Joint Operations. Join Publication 3–0. [Электронный ресурс] // Washington D.C.: U.S. Department of Defense. 2006. Incorporating Change 1, 2008. URL: https://www.bits.de/NRANEU/others/jp-doctrine/jp3_0%2808ch1%29.pdf (дата обращения: 05.04.2022).
[125] Манойло А. В., Стригунов К. С. Технологии неклассической войны. Генезис. Эволюция. Практика. – М.: Горячая линия – Телеком, 2020. – С. 52.

инструментов»[126]. Таким образом, концепция ОБДЭ явно выходит за рамки обыкновенной тактики и требует стратегического мышления.

Другим параллельным и часто неверно интерпретируемым понятием при описании характеристик современных гибридных войн является «концепция «Неограниченная война», которую выдвинули в 1999 году генералы Народно-освободительной армии Китая Цяо Лян и Ван Сянсуе в своей одноименной книге[127]. Основные положения данной концепции заключаются в том, что, во-первых, война охватывает всю сферу жизни общества; во-вторых, война ведется без правил, традиций и обычаев. Для того чтобы достичь своей цели, участники войны могут пользоваться любыми методами. Авторы книги считают, что, с учётом нового диапазона угроз, прежнее мнение о войне как о форме исключительно наступательных действий безнадежно устарело и необходимо использовать в боевых действиях «составную силу во всех аспектах, связанных с национальными интересами», включая даже экстремальные и террористические методы. Подобные мнения настолько совпадают с идеями гибридных войн, что стратегия «неограниченной войны» рассматривается как восточный (или азиатский) аналог стратегии гибридных войн России и США[128,129].

Другой термин, часто встречающийся в исследованиях по теме гибридных войн, – «прокси-война» (также «опосредованная война», «война по доверенности», «война чужими руками»). По классическому определению американского политолога К. Дойча, прокси-война – это «международный конфликт между двумя странами, которые пытаются достичь своих собственных целей с помощью военных действий, происходящих на территории и с использованием ресурсов третьей страны, под прикрытием разрешения внутреннего конфликта в этой

---

[126]Davis P. Effects–Based Operations [Электронный ресурс] // RAND. 2001. P.7. URL: https://www.rand.org/content/dam/rand/pubs/monograph-reports/2006/MR1477.pdf (дата обращения: 06.06.2022).

[127] Liang Q., Xiangsui W. Unrestricted warfare. – Beijing: PLA Literature and Arts Publishing House Arts, 1999. FBIS Translated Text. – 228 p.

[128] Davis John R. The hybrid mindset and operationalizing innovation: toward a thoery of hybrid: SAMS. Monograph. – Fort Leavenworth (Kansas), 2014. – P. 7.

[129] Ранее было опубликовано в статье: Го Фэнли. Гибридная война в исследованиях ученых Китайской Народной Республики // Гражданин. Выборы. Власть. – 2022. – №1(23). – С. 140–152.

третьей стране»[130]. Не менее разумны взгляды Микрюкова В. Ю., который определяет прокси-войны как «конфликты, в которых в собственных интересах косвенно участвует третья сторона, обеспечивая одного из двух акторов конфликта военной, организационной, ресурсной, политической или иной поддержкой»[131]. Основной мотивацией ведения прокси-войн является стремление геополитических соперников или других акторов мировой политики (спонсоров) защитить свои геополитические интересы через своих «прокси», не прибегая к прямому военному конфликту. А «прокси», в свою очередь, нуждаются в военной, технической и политической поддержке со стороны своих спонсоров (третьей стороны конфликта). Прокси-война имеет многовековую историю и была стандартным видом конфликта во время холодной войны. Так, Корейская война (1950-1953), Война во Вьетнаме (1957-1975), Афганская война (1979-1989) и т.д. являются типичными примерами прокси войн времён столкновения СССР и США. Нынешний конфликт на Украине также являются прокси-войной, в которой режим Зеленского выступает в роли прокси США (главный спонсор).

Таким образом, на основании вышеизложенного можно прийти к следующему выводу: теория «управляемого хаоса» указывает на одно из общих направлений защиты национальных интересов в международной борьбе – создать и использовать хаос, управляемый своей стороной, чтобы ослабить противника и защитить собственные интересы. А концепцию ОБДЭ можно рассматривать как мышление о реализации стратегии «управляемого хаоса» – путём координации и управления всеми элементами государственной мощи для достижения требуемых эффектов в интересах национальной безопасности воздействующей стороны. При этом необходима постоянная оценка оказываемых эффектов для ввода корректив в свои действия и достижения нужного результата. Дальше «неограниченная война» ещё более подчёркивает многообразие оказания влияния на противника – средства не ограничены для достижения преимущества в межгосудар-

[130] Mumford A. Proxy Warfare. – Cambridge: Polity Press, 2013. – P.13.
[131] Микрюков В. Ю. Прокси–война [Электронный ресурс] // Научно-исследовательский центр «Национальная безопасность». 2015. URL: http://nic-pnb.ru/analytics/proksi-vojna/ (дата обращения: 06.06.2022).

ственной борьбе и защиты национальных интересов. Вместе с тем прокси-война отличается тем, что акторы чужими руками путём предоставления всесторонней поддержки своим прокси и вынуждая их действовать якобы по своей воле стремятся достичь своих геополитических интересов. А исследуемое в настоящей диссертации понятие «гибридной войны» вбирает в себя признаки всех описанных выше концепций, интегрируя их на собственной платформе – под общим «зонтичным брендом» (которым сам термин «гибридная война» и является).

Основные компоненты гибридных войн и их характеристики

О гибридных войнах говорят, когда попытаются отразить всю сложность и многогранность конфликтов противоборствующих сторон в открытом военном состоянии или до него.

В отличие от традиционных войн, где решающую роль играют прямые военные воздействия в одоление враждебного государства, в современных гибридных войн предпочтительными средствами ведения войны стали невоенные инструменты, а военная сила чаще всего используется только в крайних случаях при эскалации конфликтной ситуации. Результаты анализа существующих теорий и практик в сфере международных отношений позволили обобщить ряд наиболее результативных и адаптированных под современные реалии технологий (инструментов) ведения гибридных войн.

«Составной частью гибридной войны, так называемой «когнитивной арт-подготовкой» открытого вооружённого конфликта, является война информационная, а в более широком контексте – информационно-психологическая»[132]. «Информационная война», как и «гибридная война», является чрезвычайно широким по охвату изначально «зонтичным» термином, корректное в методологическом плане, определение которого было изначально крайне затруднительным[133]. В работах А. Манойло, Г. Почепцова, И. Панарина, О. Красовской, Я. Шатило

[132] Евстафьев Д. Г., Манойло А. В. Информационные войны и психологические операции как базис гибридных войн нового поколения // История. – 2021. – Т. 12. – Выпуск 6 (104).
[133] Там же.

выдвигались концептуальные подходы к пониманию «информационных войн»[134]. В их числе одним из наиболее обоснованных подходов является рассмотрение современных информационных войн как особого вида вооружённого конфликта – информационных операций и оперативных комбинаций на каналах открытых телекоммуникационных систем[135].

Информационные войны рассматриваются как базис современных гибридных войн[136].

По мнению А. В. Манойло и Д. Г. Евстафьева, современные гибридные войны стали результатом технологической революции информационных войн, произошедшей в 2014–2015 гг., которая фактически подтолкнула процесс «сборки» различных невоенных форм силового подавления противника подобщим «зонтичным» брендом[137].

Кроме того, необходимо разграничить понятия «информационная война» и «кибервойна», ведь в качестве двух основных элементов гибридных войн они могут применяться не только одновременно, но и в полной согласованности друг с другом; при этом, с точки зрения механизмов принятия соответствующих решений, в том числе, и решений об ответных действиях, это принципиально различные явления[138]. Американский учёный М. Либицки, один из разработчиков американской концепции информационной войны, в своей классической книге «Что такое информационная война» выделил семь основных форм информационного противодействия: 1) война «средств управления и контроля»; 2) разведывательная война; 3) радиоэлектронная война; 4) психологическая война; 5) «хакерская война»; 6) экономико-информационная война; 7) кибервойна, которую он

---

[134] Красовская О. В. Информационная война как коммуникативный феномен // Политическая лингвистика. –2016. –№ 4 (58). – С. 53–59; Почепцов Г. Г. Информационные войны. Новый инструмент политики. – М.: Алгоритм, 2015. – 256 с.; Панарин И. Н. Технология информационной войны. – М.: КСП+, 2003. –320 с.

[135] Манойло А. В. Информационные войны и психологические операции. Руководство к действию. –М.: Горячая линия – Телеком, 2018. – 480 с.

[136] Clark M. Russian Hybrid Warfare [Электронный ресурс] // The Institute for the Study of War. 2020. URL: http://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20IS W%20Report %202020.pdf (дата обращения: 10.02.202).

[137] Евстафьев Д. Г., Манойло А. В. Информационные войны и психологические операции как базис гибридных войн нового поколения // История. – 2021. – Т. 12. – Выпуск 6 (104).

[138] Там же.

описывает как комбинацию предыдущих шести методов[139]. То есть, по сути, по мнению М. Либицки, кибервойна является особой формой информационной войны. При этом между ними есть и принципиальные различия: суть информационной войны заключается в манипуляции информацией с целью оказания воздействия на целевую аудиторию, поэтому она всегда связана с манипулированием информацией/защитой, психологическим воздействием, для реализации чего можно использовать различные средства, включая информационно-коммуникационные технологии (ИКТ) и сети, или же классические пропагандистские методы – расклеивание пропагандистских листовок или сбрасывание их с самолёта над нужной территорией и т.д., то есть ИКТ-технологии не являются необходимыми в информационной войне. А кибероперации, наоборот, не всегда направлены на защиту или манипулирование информацией (например, они могут быть осуществлены для подрыва инфраструктуры страны-мишени), но обязательно связаны с использованием ИКТ-технологий.

Конечно, что касается различных элементов гибридных войн, между ними, помимо принципиальных различий, существуют много общего: их ударное воздействие выполняет функцию интегратора, содержательной основы для других инструментов воздействия на противника, способствует преодолению имманентной мозаичности и слабой управляемости различных участников противоборства[140].

Ещё одним распространённым элементом гибридных войн является использование деструктивных социально-политических технологий, известных как «цветные революции». Более того, по разнообразию интенсивности и степени скрытности используемых методов этот комплекс технологий можно подразделить на разные направления действий: от простой поддержки оппозиции и создания внутри страны-мишени «пятой колонны», до оформления агентов влияния и перехода её под внешнее управление.

---

[139] Libicki M. C. What is Information Warfare? – Washington: National defense university, 1995. – 104 p.

[140] Евстафьев Д. Г., Манойло А. В. Информационные войны и психологические операции как базис гибридных войн нового поколения // История. – 2021. – Т. 12. – Выпуск 6 (104).

Типичными примерами применения такого рода технологий является организация цветной революции, под которой подразумевается технология осуществления государственного переворота и тем самым внешнего управления политической ситуацией в стране-мишени. Надо обратить внимание на то, между гибридными войнами и цветными революциями имеются существенные отличия: гибридные войны – это долгосрочная последовательность боевых операций, её цель заключается не столько в военном уничтожении противника или захвате территорий и ресурсов (как в традиционной войне), сколько в установлении контроля над системой ценностей страны-мишени и превращении её в вассала воздействующей стороны. А цветная революция – это технология, её единственной целью является организация государственного переворота, после реализации которого цветная революция заканчивается[141]. На этом основе профессор МГУ А. В. Манойло на раннем этапе исследования данного феномена отнёс цветную революцию и гибридную войну к разным фазам в реализации современного противоборства: «зачастую реализуется следующая цепочка: цветная революция (инцидент – протест – майдан) – вооружённый мятеж – гражданская война – гибридная война. Цветная революция при этом играет роль спускового механизма гибридной войны, а ее технологии могут использоваться организаторами гибридных войн для провоцирования вооружённого конфликта, дальнейшее течение которого будет проходить в гибридной форме»[142]. С точки зрения автора настоящей диссертации, дальнейшее развитие данного направления исследований и новые научные работы в области цветных революций и гибридных войн показали, что цветная революция фактически является одной из фаз и основных компонентов гибридных войн. Несмотря на это, многие из прогнозов А. В. Манойло послужили полезными ориентирами для последующих исследований, в том числе его мнение о том, что цветная революция формирует условия, необходимые для

[141] Манойло А. В. Информационные войны и психологические операции: руководство к действию. – М.: Горячая линия Телеком, 2018. – С. 350–351.
[142] Манойло А. В. Гибридные войны и цветные революции в мировой политике // Право и политика. –2015. – № 7 –С. 918–929.

перевода конфликта в военную фазу и довольно часто играет сигнальную функцию для эскалации конфликта.

Практика показывает, что такие действия не только эффективнее, но и существенно дешевле прямого военного вмешательства. Исторически это очень заметно: от скрытого использования Германией внутренних революционных сил России в годы Первой мировой войны до почти открытого применения таких технологий против Венесуэлы в 2019 году.

Важнейшим аспектом современных гибридных войн является их экономическая составляющая. Экономические санкции как инструмент давления на оппонента в дипломатии имеет давнюю историю начиная с античности[143]. Вместе с тем стоит отметить, что экономические санкции стали самостоятельным инструментом внешней политики как альтернатива вооружённому конфликту только после Первой мировой войны. С этого времени они применяются регулярно, постепенно превращаясь в наиболее действенный механизм в конфликтах между государствами. С наступлением эпохи глобализации, когда мировая экономика стала неразрывным целым, роль экономических инструментов в «гибридной войне» существенно возросла. От континентальной блокады, примененной наполеоновской Францией к Великобритании в 1806-1814 годах, до более широко распространённой морской блокады в период XIX-XX веков, с активно используемых экономических санкций после Второй мировой войны до технологического противоборства сегодняшнего дня – масштабы применения и разнообразие экономических инструментов в международной политике постепенно расширяются. Более конкретные методы и кейсы применения экономических инструментов в гибридных войнах рассматриваются в разделе 1.5.

Ключевое отличие гибридных войн от традиционных конфликтов заключается в смещении используемых военных и невоенных инструментов в несиловую часть спектра[144]. По данным российского Генштаба, соотношение военных и невоенных технологий, используемых в рамках гибридных войн, составляет 1: 4 в

[143] Арский Ф. Перикл. Жизнь замечательных людей. – М.: Молодая гвардия, 1971. – С. 185; Zarate J. Treasury's War. The Unleashing of a New Era of Financial Warfare. PublicAffairs. – NewYork, 2013. – P. 3.
[144] Бартош А. А. Трансформация современных конфликтов // Вопросы безопасности.– 2018. – № 1. – С. 1–18.

пользу невоенных видов борьбы[145]. Но, «несмотря на существующую тенденцию «гуманизации» образов межгосударственных конфликтов, военная составляющая остается неотъемлемой частью их структуры»[146], занимая «деликатное и решающее положение»[147]. Впрочем, в силовом (военном) компоненте гибридных войн также происходят заметные изменения, которые отражаются в первую очередь в изменении ее роли в структуре современных конфликтов – с доминирующей на вспомогательную (как это уже было показано выше), при этом интенсивность и масштаб использования прямой вооруженной силы снижаются (за исключением специальной военной операции на Украине, которая является не столько гибридной, сколько традиционной общевойсковой. Обсуждение характера происходящего на Украине проведено в разделе «Понятие и особенность гибридной войны»). К тому же, изменяются формы и способы применения силы – с прямого на скрытое, с маскировкой под частные военные компании (ЧВК), «добровольцев-отпускников» и разного рода партизанские (милиционные) формирования. О формах и способах применения вооружённых сил в современных гибридных войнах более подробно изложено в разделе 1.5.

Исходя из вышесказанного, можно сделать вывод, что после появления в широком научном дискурсе термина «гибридная война» последний стал чрезвычайно широким по охвату «зонтичным» термином[148]. Интегрировав в себя ранее уже существующие концепции о межгосударственной борьбе, такие, как «управляемый хаос», «информационная война», «цветная революция», «неограниченная война» и т.д., сегодня он не просто представляет собой совокупность существующих современных форм и методов межгосударственного противоборства, а качественно новый концепт, включающий в себя знания о формах, методах и технологиях международных конфликтов, начиная от уже известных форм, мето-

[145] Бартош А. Гибридная война становится новой формой межгосударственного противоборства [Электронный ресурс] // Военное обозрение. 2017 г. URL: https://topwar.ru/112955-gibridnaya-voyna-stanovitsya-novoy-formoy-mezhgosudarstvennogo-protivoborstva.html (дата обращения: 15.05.2021).

[146] Тиханычев О. В. Гибридные войны: новое слово в военном искусстве или хорошо забытое старое? // Вопросы безопасности. – 2020. – № 1. – С. 30–44.

[147] Ма Цзяньгуан. Откровение сирийской войны. – М.: У Хань, 2017. – С. 23.(马建光.《叙利亚战争启示录》，长江文艺出版社，2017 年.第 23 页).

[148] Манойло А. В. Информационные войны и психологические операции: руководство к действию. – М.: Горячая линия –Телеком, 2018. – С. 84.

дов и технологий и заканчивая пока еще недостаточно изученными гибридными технологиями будущего. С точки зрения автора настоящей диссертации, под гибридными войнами следует понимать доминирующую модель современного международного противоборства, характеризующуюся комплексным использованием широкого набора сил и средств борьбы, в основном невоенных, в интегрированной кампании с целью продвижения своих национальных интересов.

1.3. Современные научные подходы к исследованию гибридных войн

Результаты анализа существующих исследований в области гибридных войн позволяют сделать вывод о том, что у современных научных исследователей, как отечественных, так и зарубежных, выделились два типа подходов к исследованию гибридных войн. Первый тип (в теоретическом плане） исследований посвящён теоретической дискуссии вокруг понятия гибридных войн и сосредоточен, в частности, на том, в какой степени новая теория ознаменовала собой перелом в военной мысли, какова связь между теорией гибридных войн и традиционными представлениями о войне. Второй тип исследования (в практическом плане) рассматривает, как новые идеи влияют на государственную политику и как они реализованы на практике, в частности, в международных конфликтах и противостояниях. В этом плане, проблематика Сирии, Украины и борьба между Россией и Западом стали популярными кейсами по внедрению идеи гибридной войны[149]. Другими словами, основное внимание уделяется идеологическому содержанию теории гибридных войн и её влиянию на практику. В этом плане по отношению к гибридным войнам исследователи и эксперты делят-

[149] См.: Ма Цзяньгуан. Откровение сирийской войны. – У Хань, 2017. – 272 с. (马建光. 《叙利亚战争启示录》，长江文艺出版社，2017年,272页);Цзя Юаньпей, Сун Цюн. Методы ведения информационных войн Запада против России и российские контрмеры // JournalofJournalismStudies.– 2020. – № 22. – С. 233–234.（贾渊培，宋琼.西方对俄罗斯舆论战方式及其应对策略研究,载《新闻研究导刊》2020年第22期，第233至234页.）; Хан Кеди. «Гибридная война» России в Украине // Исследование стратегических решений. – 2021. – № 6. – С. 51–80（韩克敌. 俄罗斯在乌克兰的“混合战争”,载《战略决策研究》2021年第6期，第51至80页. ）;Гао Кай, Чжао Линь. Гибридная война – новый подход России к стратегической игре// Journal of Journalism Studies. – 2019. – № 117. – С. 10–13.（高凯，赵林. “混合战争”— 俄罗斯新战略博弈手段，载《新闻研究导刊》2019年第7期，第10至13页.）;Шэн Шилян. Как Россия ответила на гибридную войну от США // Военный сборник. – 2016. – № 11.– С. 20–23. (盛世良. 俄罗斯如何应对美国的 «混合战争» 军事文摘 2016年第11期第20至23页.);Дуань Цзюньцзе. Практика российской «гибридной войны» и ее последствия // Современные международные отношения. — 2017. – № 3. – С. 31–36. (段君泽. 俄式“混合战争”实践及其影响, 载现代国际关系 2017年第3期第31至36页).

ся на две крупные школы:

- консервативную, сторонники которой рассматривают гибридные войны как что-то давно уже известное, существовавшее не только в современности, но и в глубокой древности, поскольку все без исключения войны всегда были «гибридными»;

- школу новаторов, к которой принадлежат те, кто рассматривают гибридные войны как принципиально новое явление.

При этом внутри каждой из школ существуют еще по два направления: радикальное и умеренное.

Таким образом, на сегодня можно выделить четыре научных подхода к исследованию гибридных войн:

- умерено-консервативный;

- радикально-консервативный;

- умеренно-новаторский;

- радикально-новаторский.

В рамках консервативной школы, отрицающей новизну гибридных войн, ее сторонники-радикалы утверждают, что гибридные войны являются понятием, лишённым смысла и навеянным модными политическими предпочтениями[150]. По мнению Р. В. Арзуманяна, «гибридность не является чем-то исключительным в стратегической истории… Гибридность разлита везде, что делает сложным создание концепции, которая была бы аналитически полезной»[151]. Анологично Ю. Ю. Першин утверждает, что «ничего нового в этой теории и понятии гибридной войны нет. Любая война обязательно является гибридной»[152]. К тому же, некоторые учёные даже считают, что «эта надуманная концепция является сознательным мифом-вирусом Запада с целью ввести в заблуждение военных теоретиков и

[150] Колесников Д. И., Кривенко А. М. К проблеме сущности и специфики гибридной войны // Военный академический журнал. – 2020. – № 1 (25). – С. 110–114.
[151] Арзуманян Р. В. Стратегия иррегулярной войны: теория и практика применения. Теоретические и стратегические проблемы концептуализации, религиозные и военно-политические отношения в операционной среде иррегулярных военных действий / Под общ. ред. А. Б. Михайловского. – М.: АНО ЦСОиП, 2015. – 334 с.
[152] Першин Ю. Ю. Записки о «гибридной войне» // Вопросы безопасности. – 2016. – №4. – С. 63–85.

политологов России и других стран »[153]и тем самым сделали вывод о том что этот термин контрпродуктивен – «сосредоточение внимания и усилий на подготовке к гибридной войне чревато забвением инвариантных основ и принципов военной стратегии и тактики и, следовательно, не полной, односторонней подготовкой страны и армии к возможной войне»[154]. В отличие от них, сторонники умеренно-консервативного подхода, хотя не видят инновационного прорыва в содержании гибридных войн, в целом не отрицают разумность и ценность продолжения исследований в данном направлении. Стоит отметить, что данная точка зрения разделяется большинством исследователей современных войн и локальных вооруженных конфликтов. Так, А. А. Бартош считает, что «российским специалистам следует более внимательно изучить основные направления новой революции в военном деле»[155]. Что касается гибридных войн, то «современная наука только «нащупывает» критерии этого феномена. Сегодня нужно уделять гораздо больше внимания этому явлению, чем это делалось до сих пор»[156]. «Так что отсутствие революционных сдвигов в «гибридной войне» не должно быть причиной для отказа от изучения этого явления, значимость и необходимость исследования, которое нельзя переоценить»[157].

Сторонники новаторской школы, напротив, подчеркивают необходимость и актуальность исследований по гибридные войнам и формам и методам противодействиям им, единодушно признавая гибридные войны новым явлением. Одним из самых главных разногласий внутри данной школы является то, что её «радикальные» сторонники рассматривают гибридные войны как некое новое явление, принципиально отличающееся от «классических» войн, более того, такая точка зрения являлась преобладающей именно на первом этапе (до и после крымского

[153] Золотухин В. М., Логинова Г. Е. К вопросу о природе и сущности гибридной войны в современном мире: философско– культурологический аспект // Вестник Кемеровского государственного университета культуры и искусств. –2017.– № 41. – Ч. I. – С. 99–104.

[154] Бельков О. А. Гибридная война – выдуманная реальность?//Гибридные войны XXI века: материалы межвузовского круглого стола. – М.: ВУ, 2015. – 310 с.

[155] Бартош А. А. Модель управляемого хаоса в культурно– мировоззренческой сфере // Вестник Московского государственного лингвистического университета. – 2014. – Вып. 39. - С. 9–27.

[156] Бартош А. А. Гибридная война как возможный катализатор глобального конфликта // Вопросы безопасности. – 2016. – № 4. – С. 41–53.

[157]Бартош А. А. Гибридная война: интерпретации и реальность [Электронный ресурс]// Независимое военное обозрение. 2016. URL: https://nvo.ng.ru/concepts/2016-09-16/1war.html (дата обращения: 20.10.2021).

кризиса 2014 г.) проведённого исследования к рассматриваемому феномену[158]. В отличие от них, «умеренные новаторы» считают, что гибридные войны становятся новым явлением с истоками и корнями в прошлом, «подобно тому, как изобретение печатного дела привело к поголовной грамотности с последующими далеко не всегда добросовестными манипуляциями сознанием. Так и в настоящее время расширение средств коммуникации приводят не только к социально-экономическим и политическим трансформациям, но и к изменению использования средств противоборства враждующих сторон»[159].В табл. 1 приведена типология современных научных подходов к гибридным войнам.

Таблица 1. **Типология современных научных подходов к гибридным войнам**

Подход к исследованию гибридных войн	**Подгруппа**	**Взгляды**	**Примечание**
Консервативный	Радикально-консервативная	Ничего нового в гибридных войнах нет, следовательно, нет исследовательской ценности данного феномена	-
	Умеренно-консервативная	Гибридные войны не вышли из рамки традиционной войны, но стоит провести дополнительные исследования их в новых условиях	Мейнстримный подход к феноменугибридных войн на данный момент
Новаторский	Радикально-новаторская	Гибридные войны принципиально отличаются от «классических» войн; подчёркивается актуальность исследования данного феномена	Преобладающая позиция на первом этапе (до и после крымского кризиса 2014 г.) исследования гибридных войн

[158] Цыганков П. А. «Гибридные войны»: понятие, интерпретации и реальность // Гибридные войны в хаотизирующемся мире XXI века: сб. – М.: Изд– во Москов. университета, 2015. – С. 42.
[159] Колесников Д. И., Кривенко А. М. К проблеме сущности и специфики гибридной войны // Военный академический журнал. – 2020. – № 1 (25). – С. 110–114.

	Умеренно-новаторская	Гибридные войны– новое явление с истоками в прошлом, есть смысл проведения исследования к нему	-

Определяя гибридные войны как всем давно известное явление, консервативная школа оправдывает свою позицию как теоретическими обоснованиями, так и историческими фактами.

На теоретическом уровне ряд авторов доказывают, что задолго до того, как американский исследователь Ф. Хоффман выдвинул неологизм «гибридная война» в начале XXI века, подчёркивая повышенные роли в современной войне таких невоенных элементов, как информационно-психологические, идеологические, террористические и т.д., соответствующие концепции ведения войн такого типа уже существовали. Так, ещё в конце XIX века французский социолог Гюстав Лебон в книге «Психология народов и масс» писал, что «великие перевороты, предшествующие изменению цивилизации, например, падение Римской империи и основание арабской, на первый взгляд определяются политическими переменами, нашествием иноплеменников, падением династий. Но более внимательное изучение этих событий указывает, что за этими кажущимися причинами чаще всего скрывается глубокое изменение идей народов»[160]. Позже в 1960 году военный теоретик русского зарубежья Е. Месснер также предсказал, что, в отличие отпрежних войн, в которых приоритетом являлось завоевание территории враждебного государства, в нынешних войнах важнейшим фактором станет психологическое воздействие, «завоевание душ» граждан противника, и в итоге войны будут осуществляться пропагандистами, повстанцами, диверсантами, террористами[161].

Подобных теорий существует немало; самым убедительным теоретическим обоснованием давно существовавшего «гибридного мышления» в истории военного искусства являются высказывания китайского стратега и мыслителя Сунь Цзы, который в своём трактате «Искусство войны» указал: «Подчинить армию

[160] Райгородский Д. Я. (ред.-сост.). Психология масс: хрестоматия. – М.: Самара: Бахрах, 2006. – С. 5.
[161] Месснер Е.Э. Всемирная мятежевойна. – М.: Жуковский: Кучково поле, 2004. – С. 130.

врага, не сражаясь, – вот подлинная вершина превосходства» … «Поэтому высшее пресуществление войны – разрушить планы врага; затем – разрушить его союзы; затем – напасть на его армию; и самое последнее – напасть на его города. Осада города применяется только тогда, когда это неизбежно»[162]. Философия Сунь-Цзы заключается в достижении максимальной победы с минимальными затратами. По его мнению, лучшая стратегия – избежать прямого военного конфликта с помощью комбинации (военных и разведывательных) тактик и победить противника без боя»[163]. То есть популярная теория гибридных войн имеет истоки ещё в VI веке до нашей эры[164].

Что касается приведения исторических фактов, то, основываясь на определениях гибридных войн и их структуре, различные авторы показывают существования в истории каждой составляющей гибридных войн, тем самым, делая вывод об отсутствии новизны в понятии гибридных войн. Например, исходя «из опыта» Троянской войны, завоеваний А. Македонского, жёсткой пропагандисткой политики фашисткой Германии и т.д., эти авторы (например, А. А. Бартош) утверждают, что информационные войны велись во все времена[165]; «комплекс мероприятий по блокированию торговли Великобритании, проводившихся Францией в 1806-1814 годах рассматривается в качестве одного из первых примеров экономической войны»[166]; принцип гибридных войн – «скрытого привлечения сторонних вооружённых группировок при сопровождении вооружённых действий всесторонними отвлекающими манёврами – также используется доста-

[162] Сунь Цзы. Искусство войны / [пер. с древнекит. Н. Кондрата]. – М.: АСТ, 2018. – 192 с.
[163] Ранее было опубликовано в статье: Го Фэнли. Гибридная война в исследованиях ученых Китайской Народной Республики // Гражданин. Выборы. Власть. – 2022. – №1(23). – С. 140–152.
[164] Тиханычев О.В. Гибридные войны: новое слово в военном искусстве или хорошо забытое старое? // Вопросы безопасности. – 2020. – № 1. – С. 32; Го Фэнли. Гибридная война в исследованиях ученых китайской народной республики // Гражданин. Выборы. Власть. – 2022.– № 1(23). – С. 140–152.
[165] Першин Ю. Ю. Записки о «гибридной войне» // Вопросы безопасности. – 2016. – № 4. – С. 63–85.
[11.] Цыганков П. А. «Гибридные войны»: понятие, интерпретации и реальность // «Гибридные войны» в хаотизирующемся мире XXI века: сб. – М.: Изд– во Москов. университета, 2015. – С. 32–42.
[166]Катасонов В. Экономические войны и экономические санкции [Электронный ресурс] // Военное обозрение. 2015. URL: https://topwar.ru/68238-ekonomicheskie-voyny-i-ekonomicheskie-sankcii.html (дата обращения: 06.01.2022).

точно давно: от греческих наёмных армий, описанных в «Анабасисе» Ксенофонта, до ирландских наёмников «дикие гуси» (Wild Geese) XVII века»[167].

Определяя гибридные войны как новое явление, сторонники новаторской школы в основном апеллируют к появлению новой военной техники (роботизируемой, нередко, с наличием искусственного интеллекта) и к изменению ролей военных и невоенных элементов, применяемых в современных гибридных войнах. Как отмечают В. М. Золотухин и Г. Е. Логинова, современная война не может не быть негибридной, поскольку «ведётся не только на уровне современной техники и технологий, но связана с осмыслением их ценностных аспектов в различных культурах»[168]. В этом плане нет достаточных оснований рассматривать явление гибридных войн как «хорошо забытое старое» или инновацию.

В то же время, «гибридные войны» напрямую связаны с усложняющейся международной обстановкой: с одной стороны, развитие международных отношений и связанных с ними глобальных процессов, особенно, таких, как глобализация и информатизация, обогатили арсенал современных войн и, в конечном итоге, породило феномен «гибридной войны»; с другой стороны, распространение «гибридных войн» формирует новый мировой ландшафт (можно даже сказать, что он уже стал состоянием существования сегодняшнего мира), что, в свою очередь, обуславливает ценность исследований, ведущихся в данной области, и подчеркивает необходимость их дальнейшего совершенствования. Аналогично Г. Е. Логинова считает, что гибридные войны – «это новая по своему содержанию (масштабам), предмету, цели война. Соответственно, она новая, прежде всего, по способу ее ведения»[169]. Однако исследование феномена «гибридной войны» не должно остаться на уровне теоретического обсуждения ее концепции и природы (хотя это и является неотъемлемым звеном познания природы данного явления),

---

[167] Тиханычев О. В. Гибридные войны: новое слово в военном искусстве или хорошо забытое старое? // Вопросы безопасности. – 2020. – № 1. – С. 32.

[168] Золотухин В.М., Логинова Г.Е. К вопросу о природе и сущности гибридной войны в современном мире: философско-культурологический аспект // Вестник Кемеровского государственного университета культуры и искусств.– 2017. – №41. – Ч. I. – С. 103.

[169] Логинова Г. Е. Проблема гибридной войны в современной геополитике: теоретический аспект // Актуальные проблемы гуманитарных наук в техническом вузе: Сборник научных трудов. – Кемерово: Кузбасский государственный технический университет им. Т. Ф. Горбачева, 2017.

а скорее должно заключается в прикладном, практико-ориентированном ключе, принося конкретную пользу обеспечению безопасности государства путем повышения информированности о реальных и потенциальных угрозах в данной области и, тем самым, повышения способности противостояния им на системном уровне.

1.4 Основные тенденции и закономерности эволюции современных гибридных войн

Анализ исторической ретроспективы позволяет констатировать, что угроза гибридных войн сугубо актуальна в настоящее время и будет все так же актуальна и в обозримом будущем. Более того, по мере развития человеческой цивилизации, в особенности, новой техники и технологий, в перспективе инструментарий ведения межгосударственного противоборства будет расширяться и дополняться другими «гибридными» подходами, встречавшимися ранее в истории, но модифицированными в новых условиях.

В 2020-ом году в корпорации РЭНД разработали для Пентагона ряд прогнозов по военным тенденциям. В частности, в докладе «Будущее войны в 2030 году» среди важных тенденций отмечаются актуальность повышения способности действовать на значительном удалении без соприкосновения с основными силами противника благодаря широкому внедрению форм и методов информационно-психологической войны и технологий искусственного интеллекта (ИИ). В другой работе РЭНД «Вглядываясь в хрустальный шар. Целостная оценка будущего войны» также подчёркиваются смещение тактики ведения боевых действий в сферу информационной войны, повстанческих сил и сил специальных операций, включая возможность широкого использования ИИ[170]. На этой основе мы можем прогнозировать, что в будущих гибридных войнах с высокотехнологическим характером выделятся следующие основные тенденции:

[170] Бартош А. А. Вычисляем будущие конфликты [Электронный ресурс] // Военно-промышленный курьер. 2021. № 2 (865). URL: https://vpk-news.ru/articles/60450 (дата обращения: 05.06.2022).

1. Одним из основных направлений эволюции будущих войн станет то, что информационно-манипулятивные методы в гибридных войнах будут модернизироваться и в конечном итоге станут основным инструментом реализации государственной политики. На данный момент по мере популярности информационно-манипулятивных технологий и технологий противодействия им, методы информационных манипуляций становятся все менее эффективными для достижения политических целей, но в дальнейшем они дополнятся другими технологиями и методами, такими, как кибердударами и точечным использованием политико-силовых методов[171]. Милитаризация глобального информационного пространства становится очевидным фактом, что отмечалось в работах как российских, так и зарубежных специалистов[172].

2. Другим важным изменением в будущих гибридных войнах является то, что усиливается тенденция к интеллектуализации и дистанционности боевых действий (Remote Warfare). С быстрым развитием таких технологий как «глубокое обучение», ИИ демонстрирует скачок в развитии, и его применение в военной области продолжает расширяться, поэтому будущие военные действия неизбежно проявят беспрецедентные интеллектуальные особенности. В частности, беспилотные кластерные операции – один из основных видов боевых операций в интеллектуальной войне – станет главной силой атак на противника на линии огня. В будущей эре интеллекта появится новая модель ведения боевых действий с наделением машин человеческим интеллектом, и роботы перейдут от помощи людям в бою к замене их во многих операциях с высоким риском для выполнения заданий людьми. В какой-то степени это неизбежно приведёт к физическому отсоединению человека от оружия. Но это не означает, что машины смогут полностью заменить людей; способ сочетания людей и оружия приобретёт совершенно новую форму. Беспилотные боевые системы будут глубоко интегрированы с людьми как органичный симбиоз, сочетающий творческий потенциал и вдум-

[171] Манойло А.В., Евстафьев Д. Г. Гибридные войны в контексте постглобализации // Контуры глобальных трансформаций: политика, экономика, право. – 2021. – Т. 14. – № 4. – С. 160–175.
[172] Simons G. Digital Communication Disrupting Hegemonic Power in Global Geopolitics // Russia in Global Affairs. – 2019. – No. 2. – C. 108–125.

чивость человека с точностью и скоростью машин.

3. В военных действиях уже используется широкий спектр беспилотников, а роботы-солдаты, беспилотные автомобили и катера также выходят на поле боя, превращая войну из прямого человеческого конфликта в косвенную дуэль «человекоподобных материалов». По мере интеллектуализации поля боя, усиливается и тенденция дистанционных боевых действий, что значительно снизит и порог решения на применение силы.

4. Наконец, окончательной формой эволюции современных войн станет «битва за мозг», которая также называется «когнитивная война» или «ментальная война». В марте 2021 года советник министра обороны России Андрей Ильницкий ввёл в дискурс определение «ментальной войны», которое вызвало значительный резонанс в России и за рубежом[173]. Андрей Ильницкий предупреждал, что «ментальная война становится важнейшим инструментом межгосударственного противоборства». В этом новом виде войны Запада против России русские «культура, традиции, убеждения и мировоззрение людей выступают главным призом ментальной войны против нас»[174]. Вскоре его слова подтвердили в начале октября того же года в стане НАТО, и, хотя там «ментальную войну» называют «когнитивной», суть ее – одна и та же. 8 октября 2021 года западный интеллектуальный ресурс «The Grayzone» раскрыл，как НАТО разрабатывает концепцию и технологии когнитивной войны, используя предполагаемые угрозы со стороны Китая и России[175]. Руководитель Инновационного центра НАТО (iHub)[176]Дю

[173] В Минобороны обвинили Запад в развязывании ментальной войны с РФ [Электронный ресурс] // Известия. 2021. URL: https://iz.ru/1142000/2021-03-25/v-minoborony-obvinili-zapad-v-razviazyvanii-mentalnoi-voiny-srf (дата обращения: 15.06.2022); В Минобороны заявили, что США начали против России ментальную войну [Электронный ресурс] // РИА НОВОСТИ. 25.03.2021. URL: https://ria.ru/20210325/ssha-1602735487.html (дата обращения: 15.06.2022); Советник Министра обороны России рассказал, как победить США в «ментальной войне» [Электронный ресурс] // RT. 30.03. 2021. URL: https://russian.rt.com/russia/news/847721-minoborony-mentalnaya-voina-pobeda (дата обращения: 15.06.2022); Советник Шойгу рассказал о «ментальной войне» против России [Электронный ресурс] // Радио Свобода. 2021. URL: https://www.svoboda.org/a/31168918.html (дата обращения: 15.06.2022).

[174] Советник министра обороны России рассказал о новом типе войны [Электронный ресурс] // РИА НОВОСТИ. 2021. URL: https://ria.ru/20210822/mentalnye-1746750876.html (дата обращения: 15.06.2022).

[175] BenNorton. Behind NATO's 'cognitive warfare': 'Battle for your brain' waged by Western militaries // The Grayzone. 2021. URL: https://thegrayzone.com/2021/10/08/nato-cognitive-warfare-brain/ (дата обращения: 15.06.2022).

[176]iHub спонсируется Командование по трансформации союзников (ACT) НАТО и его исследования напрямую поддерживаются и контролируются НАТО. Таким образом, iHub, по сути, представляет собой внутренний исследовательский центр или мозговой центр НАТО.

Клюзель признал, что его руководство разрабатывает стратегию когнитивной войны, которая «прямо сейчас является одной из самых горячих тем для НАТО»[177].

Дю Клюзель определил когнитивную войну как имеющее «универсальный охват» «искусство использования технологий для изменения восприятия человеческих целей». Эти технологии включают области NBIC (НБИК) – нанотехнологии, биотехнологии, информационные технологии и когнитивные науки. Они создают в совокупности «своего рода очень опасный коктейль, который может ещё больше манипулировать мозгом».

Когнитивная война начинается в информационной сфере (как отметил Дю Клюзель, «информация – топливо когнитивной войны»), технологии ее реализации базируются на информационной и психоэмоциональной составляющих, поэтому своего рода она и есть гибридная война[178]. Но этот новый метод боевых действий намного мощнее и выходит далеко за рамки информационно-психологической войны. Если результатом информационно-психологической войны является нежелание противника продолжать борьбу из-за разочарования в своём деле и идеалах, то когнитивная война идёт ещё дальше. Когнитивная война – это игра на знаниях, на том, как наш мозг обрабатывает информацию и превращает её в знания, а не только игра на информации или на психологических аспектах нашего мозга. В этом случае противник изощрённо программируется на саморазрушение и самоликвидацию, у него незаметно создаётся нужная врагу «начинка». В информационно-психологической войне не предусмотрены достижения долгосрочных политических успехов и обманутые и распропагандированные люди могут исправлять допущенные ими глупости и ошибки, когда в какой-то момент приходят в себя. А в когнитивной войне этого не произойдёт, ведь речь идёт о глубинном перепрограммировании человека, целых обществ и стран, последствия которого не обратимы.

---

[177] Ben Norton. Behind NATO's 'cognitive warfare': 'Battle for your brain' waged by Western militaries [Электронный ресурс] // The Grayzone. 2021. URL: https://thegrayzone.com/2021/10/08/nato-cognitive-warfare-brain/ (дата обращения: 15.06.2022).

[178] Там же.

В 2020 году iHub опубликовал доклад под названием «Когнитивные войны», в котором подчёркивается «Мозг станет полем битвы 21 века»[179]. До недавнего времени НАТО разделяло войну на пять оперативных видов: морскую, наземную, воздушную, космическую и кибернетическую. Но с развитием стратегий когнитивной войны «человеческая область» будет новым, шестым уровнем. Первые пять сфер могут принести тактические и оперативные победы, а человеческая сфера вполне может быть решающей областью, в которой многодоменные операции достигнут сокрушительного эффекта и окончательного результата.

Быстрое развитие современных технологий, включая неврологию, интерфейс мозг-компьютер и биомедицину, огромные мировые инвестиции в нейробиологию позволяют небезосновательно констатировать, что когнитивная область, вероятно, станет полем сражений будущего со стратегическим значением.

[179] Cluzel F.D. Cognitive Warfare [Электронный ресурс] // InnovationHub. 2020. URL: https://www.innovationhub-act.org/sites/default/files/2022-02/CW%20article%20Claverie%20du%20Cluzel%20final_0.pdf(дата обращения: 20.10.2022).

1.5 Классификация организационных форм и методов ведения гибридной войны

Разнообразие «гибридных» форм боевых действий обусловлено, прежде всего, тем, что «нельзя рассматривать гибридную войну неким единым, однородным явлением. Подобные действия различаются по целям, применяемым методам и степени «гибридности», что, в свою очередь, требует уточнения их классификации»[180]. В современных гибридных войнах на передний план выходят такие виды борьбы, как информационно-психологическое давление, экономические санкции, цветные революции, комбинированное применение вооружённых сил, а остальные компоненты в инструментарии гибридных войн используются либо реже, либо чаще всего в сочетании с вышеперечисленными формами и методами, играя вспомогательную роль. Так, информационно-психологические операции часто сопровождаются дипломатическим давлением, а оппозиция задействуется в первую очередь при реализации все тех же цветных революций. При изучении противоборства в информационном пространстве часто используются следующие понятия: информационная война, психологическая война, информационно-психологическая война и информационно-психологическое противоборство. Соотношение этих терминов довольно подробно описано в трудах А. В. Манойло, к мнению которого мы присоединяемся; так, он считает, что термины «информационная война» и «психологическая война» следует воспринимать

[180] Бартош А. А. Модель гибридной войны // Военная мысль. – 2019. – № 5. – С. 6–23; Фадеев А.С., Ничипор В. И. Военные конфликты современности, перспективы развития способов их ведения. Прямые и непрямые действия в вооружённых конфликтах XXI века // Военная мысль. – 2019. – № 9. – С. 33–41; Дорохов В. Л., Петрушин А. И., Никоноров Г. А. О совершенствовании территориальной обороны с учётом особенностей гибридных войн // Военная мысль. – 2009. – № 12. – С. 39–47.

как синонимы, а под общим понятием информационной борьбы понимают совокупность как вооруженных, так и невооруженных форм и методов[181].

Способы проведения информационно-психологической войны инициативно обобщены профессором МГУ А. В. Манойло, который структурно разделил весь процесс реализации информационно-психологической войны на три уровня (см. схема 2) и проанализировал конкретные технологии и характеристики на каждом уровне:

1) первый уровень – информационные вбросы (низовой – тактический уровень ведения ИПВ), представляющие собой блок специально подготовленной информации для стимулирования объекта атак на совершение немедленных ответных действий;

2) второй уровень – информационные операции (оперативный уровень ведения ИПВ), представляющие собой последовательность информационных атак;

3) высший уровень (стратегический уровень) – уровень соответствует самой информационно-психологической войне как разновидности международного конфликта[182].

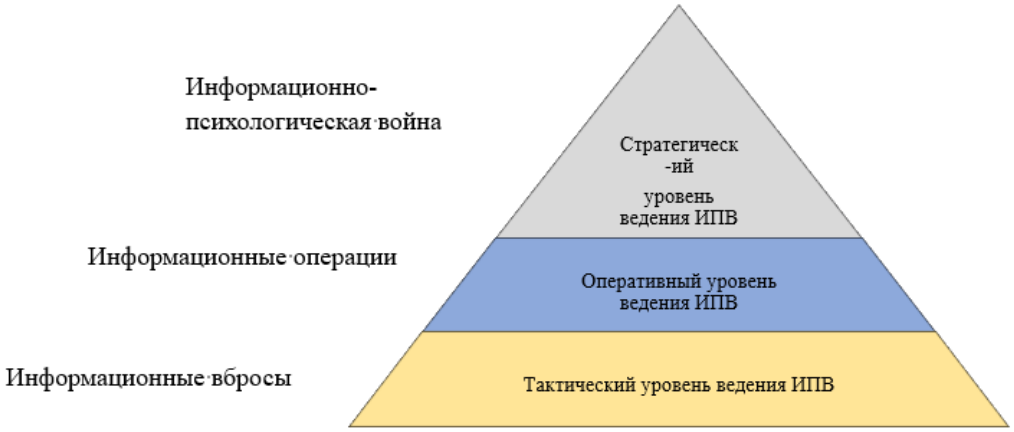


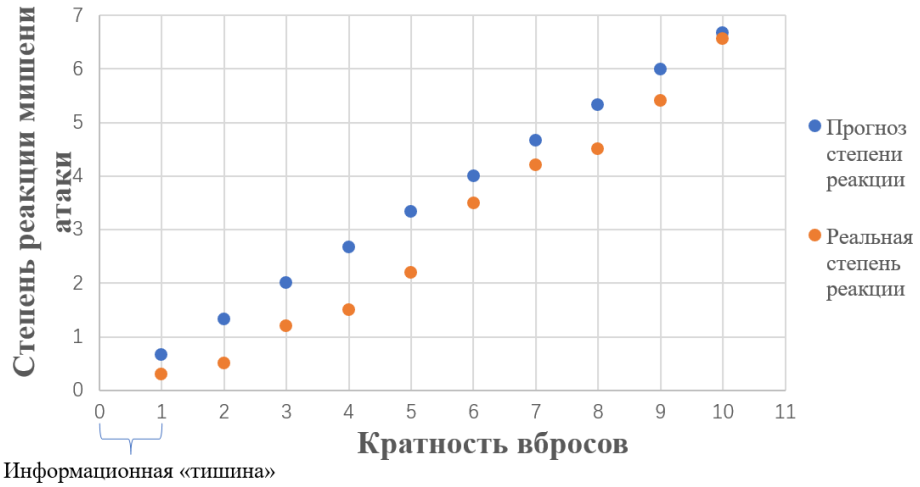
Схема 2. Структура ведения ИПВ (по теории проф. А. В. Манойло)

Каждый из вышеназванных уровней характеризуется собственным набором технологий и методов.

В первую очередь, любая операция ИПВ «начинается с информационного

[181] См.: *Манойло А. В.* Информационные войны и психологические операции. Руководство к действию. — М.: Горячая линия – Телеком, 2018. — 480 с.
[182] Манойло А.В., Пономарева Е. Г. Современные информационно-психологические операции: технологии и методы противодействия // Обозреватель. – 2019. – № 2. – С. 5–17.

вброса, который является блоком специально подготовленной информации, стимулирующей объект атаки на совершение немедленных ответных действий. Как правило, информационные вбросы применяются сериями последовательно, но через заранее намеченные промежутки времени (периоды информационной «тишины»), чтобы обеспечить эффект экспозиции»[183]. «В этом процессе информационная «тишина» – техническая пауза, разделяющая два последовательных вброса»[184], очень важна для достижения желаемых результатов атакующей стороны. Ведь она даёт возможность не только мишени атаки полностью «переварить» вбрасываемую информацию и перейти в возбуждённое состояние, но и сценаристам информационных атак корректировать план в последующем выбросе по реакциям объекта воздействия. Таким образом, благодаря многократным вбросам по одному и тому же объекту, инициатор атаки последовательно подводит мишень к постоянному, нарастающему с течением времени паническому состоянию, тем самым вынуждая жертву агрессии принимать неверные для себя, но выгодные для инициатора атаки решения. Такой итерационный цикл продолжается до тех пор, «пока воля объекта атаки не окажется полностью сломлена или подчинена атакующей стороне»[185]. На схеме 3 представлена модель, визуально отражающая процесс проведения информационно-психологической операции (ИПО).



[183] Там же.
[184] Там же.
[185] Там же.

Схема 3. Информационная операция в действии

Эта методика активно применялась при организации государственных переворотов в ряде стран Северной Африки, в частности, ««добровольный» уход Бен Али и Х. Мубарака являются типичными примерами эффективных информационных атак»[186].

В международных академических кругах признается, что в основе цветных революций лежит теория «ненасильственной революции» Джина Шарпа, работы которого рассматривают как инструкцию к совершению государственного переворота и «библию новых революционеров». В своём трёхтомном труде «Политика ненасильственных действии» Д. Шарп выделил 198 методов проведения ненасильственных действий (организации цветных революций)，разделённые на три большие группы:

1) методы ненасильственного протеста и убеждения;

2) методы отказа от сотрудничества (социального, экономического и политического);

3) методы ненасильственного вмешательства[187].

Почти все цветные революции происходили с использованием классических методик, разработанных Д. Шарпом. С течением времени технологии цветных революций были значительно усовершенствованы (примером могут служить попытки организации гибридных госпереворотов в Боливии-2019, в Венесуэле-2019 и в Белорусии-2020).

В 2014 году, сразу после цветной революции 2013-2014 годов на Украине, профессор А. В. Манойло выделил пять основных этапов технологии цветной революции (которые он назвал технологиями демонтажа политических режимов):

1) обучение активистов из молодёжной среды «содействия демократизации» и формирование организованного протестного движения;

---

[186] Манойло А. В. Информационные войны и психологические операции: руководство к действию. – М.: Горячая линия Телеком, 2018. – С. 84.

[187] Gene Sharp. The Politics of Nonviolent Action, Vol. 2: The Methods of Nonviolent Action. – Boston: Porter Sargent Publishers,1973. – P. 117–445.

2) создание инцидента, способного вызвать мощный общественный резонанс и вывести активистов на улицу;

3) осуществление конфликтной мобилизации – вовлечение все больших слоёв населения;

4) формирование политической толпы, к которой внедряется перепрограммирование с новыми ценностями и императивами;

5) от имени толпы выдвижение ультимативных требований к властям[188].

В отличие от классических цветных революций, современные цветные революции носят ярко выраженный гибридный характер и имеют специфические особенности реализации:

- во-первых, их организационная структура стала сетевой с появлением одновременно некоторых центров координации (оперативных штабов или центров управления протестными массами) ;

- во-вторых, в самой структуре цветных революций произошла смена механизмов мобилизации ресурсов для организации массового протеста. В цветных революциях нового поколения заказчики цветной революции переходят от роли «культиватора» к роли «венчурного капиталиста», поощряя местных жителей страны-мишени автоматически выбирать местные проблемы для провоцирования инцидента, а затем выбирают из ряда «проектов» один для «точечного инвестирования»;

- в-третьих, существует тесная взаимосвязь между цветной революцией и бурно развивающейся субкультурой футбольных фанатов. Случаи из Гонконга Китая и Таиланда показывают, что использование «групп фанатов» для сбора средств, организации логистики и контроля комментариев на платформах социальных сетей становится отличительной чертой новых «цветных революций»[189].

---

[188] Манойло А.В. Цветные революции и проблемы демонтажа политических режимов в меняющемся мире // Вестник МГОУ. – 2014. – № 2. – С. 1–14.

[189] Методики Запада к продвижению цветных революций меняются, к которому Китай должен бдителен [Электронный ресурс] // TheGlobalTimes.2020. URL: https://world.huanqiu.com/article/40zcpYrwMO3 (дата обращения: 20.07.2022). (西方推动“颜色革命”方式正发生变化中国应保持警惕 // 环球时报.06.12.2020).

Практика показывает, что такие действия не только эффективнее, но и существенно дешевле прямого военного вмешательства. В мировой истории это проявлялось многократно, начиная «от скрытого использования Германией внутренних революционных сил России в годы Первой мировой войны и до почти открытого применения таких технологий против Венесуэлы в 2019 году»[190].

На сегодняшний день можно выделить следующие основные способы ведения гибридной войны в экономической сфере:

- экономическое эмбарго – приостановление (полностью или частично) экономических взаимодействий со страной-объектом агрессии. Наиболее типичными примерами являются общее эмбарго, введённое администрацией Дж. Буша в отношении Ирана в 1990 году, и частичное эмбарго США против СССР во время так называемой Холодной войны, направленное на ослабление военного потенциала последних;

- торговые санкции – ограничения на экспорт конкретных товаров, технологий или услуг в страну-объект гибридной агрессии и на импорт конкретных товаров, технологий или услуг из страны-объекта гибридной агрессии;

- финансовые санкции – ограничения на движение капитала у страны-мишени и её граждан и организаций, включая не только замораживание их финансовых активов и ограничения финансовых операций, но и прямые санкции против банковской системы страны-мишени путём исключения её банков или других финансовых учреждений из системы SWIFT и прекращения всей её финансовой деятельности с использованием доллара США с внешним миром;

- «Умные санкции» («smart sanctions»), направленные на руководство, политические элиты и другие ключевые фигуры, принимающие решения и определяющие ход экономических процессов в стране-мишени гибридной агрессии[191].

Мировая история демонстрирует большое разнообразие методов, применяемых с использованием этой составляющей противоборства, от прямого бло-

---

[190] Тиханычев О. В. Гибридные войны: новое слово в военном искусстве или хорошо забытое старое? // Вопросы безопасности. – 2020. – № 1. – С. 30–44.

[191] Cortright D., Lopez G.A., Stephanides J. et al. Smart Sanctions: Targeting Economic Statecraft. – New York: Rowman & Littlefield, 2002. – 256 p.

кирования зарубежных счетов Ирака в 2012 году и Венесуэлы в 2019 году до блокировки доступа иранских банков к системе SWIFT в 2018 году и технической блокировки китайских компаний. При этом США непрерывно развивают экономические методы с целью превращения их в эффективный инструмент оказания гибридного давления на своих противников. В частности，самым типичным примером такого использования данных методов выступают всесторонние санкции Запада в отношении России, введённые им с началом СВО. После вхождения Крыма в состав Российской Федерации санкции стали ведущим инструментом гибридной войны США и их союзников против России[192].

В апреле 2022 года Институт финансовых исследований Чунъян Китайского народного университета опубликовал отчёт, в котором всесторонне разобраны методы, особенности, влияние и другие детали санкций, введённые США в отношении России. В упомянутом докладе указывалось, что за 8 лет, с 2014 года до 2022 года (по состоянию на 1 апреля 2022 года), страны во главе с США ввели 8068 санкций против России, что в 1,5 раза больше, чем против Ирана за последние 40 лет. Из них 5314 новых санкций было введено с 22 февраля[193]. Сейчас Россия самая санкционированная страна в мире.

Несмотря на то, что соотношение между компонентами гибридных войн постепенно смещается в пользу несиловых, вооружённые силы по-прежнему остаются определяющими в структуре гибридных войн, при этом формы и методы их использования адаптируются к сегодняшним реалиям и чаще проявляются как:

- косвенное применение вооружённых сил в формах: наёмников, ЧВК, создания «гражданской армии» внутри страны-противника из её граждан;

- прямое применение регулярных вооружённых сил на заключительных этапах войны под предлогом «гуманитарной интервенции», проведения операций

---

[192] Капканщиков С. Г., Капканщикова С. В. Гибридная война как угроза экономической безопасности России и санкции как ее ведущий инструмент // Национальные интересы: приоритеты и безопасность. – 2018. – Т. 14. № 6. – С. 1044–1059.

[193] Отчёт о санкции Запада против России // Институт финансовых исследований Чунъян Китайского народного университета, 2022. (中国人民大学重阳金融研究院研究报告：《大杀器？美国对俄罗斯制裁评估与启示》. 2022 年 4 月); Китайский мозговой центр опубликовал первый в мире Отчёт о санкции Запада против России [Электронный ресурс] // CHINANEWS.2022. URL:https://www.chinanews.com.cn/cj/2022/04– 02/9718600.shtml (дата обращения: 15.04.2022) (中国智库发布首份美国对俄制裁评估报告 // 中国新闻网. 2022 年 4 月 2 日).

по принуждению к миру и по другим «уважительным причинам»[194].

В качестве примера применения силовых действий первого типа выступает «созданное США для противодействия сначала СССР, а потом и демократическому правительству Афганистана движение Талибан[195]. Или создание и поддержка ими же так называемой «сирийской умеренной оппозиции». Другим характерным примером является использование наёмной военной силы из небольших стран НАТО (Польши, Румынии) для создания коалиционных сил при ведении различных операций, таких, как война в Ираке»[196].

[194]Бартош А. А. Стратегия и контрстратегия гибридной войны // Военная мысль. –2018.– №10. – С. 5–20.
[195] Запрещённое в РФ.
[196] Тиханычев О. В. Гибридные войны: новое слово в военном искусстве или хорошо забытое старое? // Вопросы безопасности. –2020. – № 1. – С. 36.

1.6 Современные подходы к организации противодействия гибридным войнам

Хотя неологизм «гибридные войны» зародился в США, теория гибридных войн более проработана в России, так как она опирается на более широкую философско-теоретическую базу, которой не хватает на Западе из-за инструментального отношения к данной теории[197]. Вокруг вопроса об усилении или отказе от изучения проблематики гибридных войн продолжается широкая дискуссия; в ней присутствует значительная «разноголосица среди российских учёных, политологов и военных специалистов»[198]. Несмотря на это, под угрозой развертывания беспрецедентно ожесточенной гибридной войны со стороны Коллективного Запада в контексте СВО, российское руководство впервые официально подняло вопрос противодействия гибридным войнам недружественных стран на уровень государственной стратегии, утвердив гибридные войны как основную стратегию Запада для сдерживания России в своём внешнеполитическом документе. Российский опыт по противодействию гибридным войнам етально проанализирован в разделе 2.2.

«Пока единого мнения по вопросу о гибридной войне нет и в военных кругах США. К тому же, американские военные предпочитают использовать термин «операции полного спектра» для описания современных многомерных операций, характерных для гибридной войны. А само понятие гибридной войны часто применяется по отношению к своему противнику и конкуренту[199] в контексте описа-

[197] Фридман О. «Гибридная война» понятий // Вестник МГИМО–Университета. – 2016. – № 5 (50). – С. 79–85.
[198] Бартош А. А. Гибридная война: интерпретации и реальность [Электронный ресурс] // Независимое военное обозрение. 2016. URL: https://nvo.ng.ru/concepts/2016-09-16/1war.html (дата обращения: 20.10.2021).
[199] Клименко С. Теория и практика ведения «Гибридных войн» (по взглядам НАТО) 2015 // Зарубежное военное обозрение. – 2015. – № 5. – С. 109–112.

ния недостойного поведения в МО, нечестности, коварства или варварства»[200]. В связи с этим термин «гибридная война» «практически не используется непосредственно в документах стратегического планирования ВС США»[201], так как «в этом случае им придется применять это понятие и по отношению к себе», «хотя идея гибридности войны уже была достаточно обыденной для военной мысли США»[202].

Кроме вышесказанных крупнейших игроков в сфере гибридных войн, подходы НАТО и Китая к организации противодействия гибридным войнам также отличаются яркой спецификой и содержатопределенный полезный опыт.

Подход НАТО к организации противодействия гибридным войнам

Иной подход к проблеме гибридных войн демонстрирует НАТО. С одной стороны, руководители альянса признаются, что концепция «гибридная война» сама по себе не несет ничего нового, как отметил генсекретарь альянса Й. Столтенберг: «первая известная нам гибридная война была связана с Троянским конем, таким образом, это мы уже видели» [203]. Вместе с тем они рассматривают её как «удобное средство для анализа сегодняшних международных конкурентов и противоборств, и выработки предметных планов»[204]. Так, обвиняя Россию в ведении гибридных войн против Украины, на саммите в Уэльсе в 2014 году НАТО стала первой военно-политической организацией в мире, заговорившей о феномене гибридных войн на официальном уровне. Уже тогда верховный главнокомандующий ОВС НАТО в Европе генерал Ф. Бридлав поднял вопрос о необходимости готовить НАТО к участию в гибридных войнах[205]. В дальнейшем тема-

---

[200] Бартош А. А. Гибридная война: интерпретации и реальность [Электронный ресурс] // Независимое военное обозрение. 2016. URL: https://nvo.ng.ru/concepts/2016-09-16/1war.html (дата обращения: 20.10.2021).

[201] ARMY PLANNING. Comprehensive Risk Assessment Needed for Planned Changes to the Army's Force Structure [Электронный ресурс] // USGAO. 2016. URL: http://www.globalsecurity.org/military/li brary/report/gao/676516.pdf (дата обращения 28.07.2022); HybridWarfare, GAO- 10-1036R [Электронный ресурс] // USGAO. 2010. URL: http://www.globalsecurity.org/military/library/report/gao/d101036r.pdf (дата обращения 28.07.2022).

[202] Фридман О. «Гибридная война» понятий // Вестник МГИМО– Университета. – 2016. – № 5 (50). – С. 79–85.

[203] Jens Stoltenberg. Zero– sum? Russia, Power Politics, and the Post War Era [Электронный ресурс] // NATO. 2015.URL: http://www.nato.int/cps/en/natohq/opinions118347.htm (дата обращения 31.04.2022).

[204] Бартош А. А. Гибридная война: интерпретации и реальность [Электронный ресурс] // Независимое военное обозрение. 2016. URL: https://nvo.ng.ru/concepts/2016-09-16/1war.html (дата обращения: 20.10.2021).

[205]Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales [Электронный ресурс] // NATO. 2014. URL: https://www.nato.int/cps/en/natohq /official_texts_112964.htm (дата обращения: 12.07.2022).

тика гибридных войн стала одной из центральных в повестке альянса. На саммите в Варшаве в 2016 году были разработаны стратегия и конкретные планы по эффективному преодолению вызовов в связи с гибридной войной[206]. В стратегии НАТО «одна из основных задач гибридной войны – создавать «управляемый хаос» в государстве-мишени ниже планки вмешательства существующих организаций обеспечения международной безопасности на постсоветском пространстве, таких как ООН, ОБСЕ или ОДКБ»[207]. При этом подчёркиваются как базовая роль высоких технологий, так и необходимость объединить все организационные возможности в противодействие «гибридным угрозам».

В своей оборонной стратегии НАТО придерживается следующих подходов по противодействию гибридным войнам, ведущимися против Альянса его противниками:

1) создание специализированного органа по ведению и противодействию гибридным войнам и улучшению обмена разведданными. В 2017 году в штабквартире НАТО было принято решение о создании Объединённого управления по разведке и безопасности (Joint Intelligence and Security Division – JISD), включающего в себя подразделение, специально занимающееся мониторингом и анализом гибридных угроз, что стало важным шагом в интеграции политической и военной разведки союзников при решении задач мониторинга и оценки широкого спектра вызовов и угроз, в том числе гибридного типа. Одной из задач данной структуры является координация разведданных, которые выявляют общую картину тенденций в области гибридных войн и позволяют членам НАТО выработать общее понимание конкретной ситуации. Позже, в 2018 году, были созданы контргибридные группы поддержки (Counter Hybrid Support Teams, CHST) в качестве еще одного ключевого элемента в системе инструментов гибридных войн НАТО для обеспечения собственной безопасности и сдерживания своего противника, а также для стремления собственного интереса в мировом масштабе. Такие

[206] Заявление по итогам встречи на высшем уровне в Варшаве [Электронный ресурс] // NATO. 2016. URL: http://www.nato.int/cps/en/natohq/official-texts133169.htm (дата обращения: 12.07.2022).
[207] Бартош А. А. Гибридная война: интерпретации и реальность [Электронный ресурс] // Независимое военное обозрение. 2016. URL: https://nvo.ng.ru/concepts/2016-09-16/1war.html (дата обращения: 20.10.2021).

группы состоят в основном из гражданских экспертов, набранных из пула экспертов НАТО, а также специалистов, делегируемых в эти структуры союзниками. Эксперты CHST могут быть направлены по просьбе союзника в зону реального или потенциального гибридного конфликта не только в случае кризиса, но и для оказания помощи в создании национального потенциала по борьбе с гибридными угрозами. Так, в ноябре 2019 года первая группа CHST была развёрнута в Черногории[208];

2) адаптация учений НАТО к гибридным угрозам. Чтобы улучшить свою структуру и возможности в гибридных сценариях, НАТО ввел больше гибридных элементов в регулярно проводимые странами Альянса военные учения, некоторые из которых проводились параллельно и в координации с Европейским союзом. При этом НАТО принял ещё более амбициозный режим проведения военных учений, включая более короткие (по времени) учения, в которых участвуют также гражданские лица, принимающие решения на высоком и высшем уровнях. Кроме того, была расширена программа подготовки и обучения НАТО, чтобы включить в нее регулярные обсуждения текущих проблем и обмены мнениями по гибридным угрозам;

3) комплексная борьба с киберугрозами и дезинформацией. Союзники НАТО полны решимости использовать весь спектр возможностей для сдерживания и противодействия всему спектру киберугроз, включая те, которые осуществляются в рамках гибридных войн. НАТО объявил киберпространство новой оперативной сферой и подготовил стратегическое руководство по реагированию на кибератаки, в котором представлен широкий спектр инструментов – политических, военных, дипломатических и экономических. Союзники продолжают усиливать киберзащиту национальных сетей и инфраструктуры в приоритетном порядке в рамках Обязательства по киберзащите (the Cyber Defence Pledge). Поскольку большая часть киберпространства находится в частных руках, НАТО также подчёркивает необходимость углублять государственно-частное партнер-

[208] Rühle M. NATO’s Unified Response to Hybrid Threats [Электронный ресурс] // CEPA. 22.03.2021. URL: https://cepa.org/natos-unified-response-to-hybrid-threats/ (дата обращения: 06.07.2022).

ство, в том числе в рамках Отраслевого киберпартнерства НАТО (the NATO Industry Cyber Partnership), чтобы создать «сообщества доверия», в которых различные заинтересованные стороны могут обмениваться информацией о киберугрозах, обсуждать меры реагирования и новейшие технологии защиты и наступления.

Кроме того, НАТО обращает особое внимание на противодействие дезинформации. Его веб-сайт под названием «Проясняем ситуацию» («Setting the Record Straight») служит «универсальным магазином» для разоблачающих мифы информационных бюллетеней, выступлений, интервью, опровержений, видео и изображений и действует на нескольких языках, включая русский. Вместе с тем Альянс также постоянно взаимодействует со СМИ для того, чтобы они удаляли или корректировали недостоверные факты и интерпретации, а также транслировали собственную идеологическую повестку НАТО – «более точную и правдоподобную, чем у противников Альянса»;

4) изучение новых прорывных технологий. Чтобы обнаружить эффективные средства и новые технологии потенциального агрессора, используемые им для подрыва в рамках осуществления гибридных действий, НАТО скорректировал структуру своего Международного персонала, создав новые подразделения, занимающиеся инновациями и информационной политикой. Эти дополнительные изменения подчеркивают решимость НАТО не допустить получение агрессором преимуществ за счет использования новых технологий. Данная работа также открыла много возможностей для сотрудничества с частным сектором;

5) расширение сотрудничества с партнёрами. В противостоянии гибридным угрозам Альянс развернул сотрудничество с широким кругом партнёров, считая, что установление тесных связей с государствами-единомышленниками по всему миру само по себе является сдерживающим фактором для потенциальных гибридных агрессоров[209]. В первую очередь, это воплощается в углублении отношений с ЕС. Так, были разработаны так называемые «учебные пособия» и

[209] Rühle M., Roberts C. Enlarging NATO's toolbox to counter hybrid threats [Электронный ресурс]// NATO Review magazine. 19.03.2021. URL: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html (дата обращения: 06.07.2022).

«оперативные протоколы» (playbooks and operational protocols) для повышения взаимной осведомленности гибридных угроз и помощи в согласовании ответов на них. Эта деятельность поддерживается Европейским центром передового опыта по противодействию гибридным угрозам (Hybrid CoE), специально созданным в 2016 году для содействия практическому сотрудничеству между НАТО и ЕС. Кроме традиционных партнёров, с недавнего времени НАТО также активно взаимодействует с партнёрами в Азиатско-Тихоокеанском регионе;

6) противодействие гибридным угрозам является долгосрочной стратегической задачей для НАТО и его союзников. Это требует отхода от устоявшейся практики преднамеренных, последовательных и очень неторопливых процессов планирования и принятия решений, которые были типичны для операций НАТО по реагированию на кризисные ситуации в эпоху после окончания Холодной войны, и перехода к более динамичному взаимодействию, при котором постоянно обновляемая ситуационная осведомленность стимулирует политические дискуссии, разработку вариантов, принятие решений и политический контроль. Чтобы делать это наиболее эффективно, НАТО рассматривает каждый гибридный субъект как уникальное образование с уникальной стратегической мотивацией. Такой более специализированный подход повышает способность НАТО сдерживать гибридные атаки, влияя на потенциальных гибридных агрессоров, и лучше противостоять так называемой «серой зоне», ставшей современным театром военных действий;

7) внедрение инноваций в механизм регулярных встреч членов Альянса с вовлечением всего правительства. Для того чтобы противостоять «гибридным общегосударственным подходам» (whole-of-government approach) государств-противников Альянса, НАТО вышел за рамки установленных форматов встреч на высшем уровне глав государств и правительств и встреч министров иностранных дел и обороны. Так, в мае 2019 года состоялась первая в истории неофициальная встреча Североатлантического совета с участием советников по национальной безопасности и старших национальных руководителей по гибридным угрозам, на которой была подчёркнута ценность сбора экспертных знаний, как о граждан-

ских, так и о военных угрозах, обмена национальным опытом по противодействию гибридным действиям, а также необходимость общегосударственного подхода к противодействию гибридным угрозам.

Подходы Китая к организации противодействия гибридным войнам

Теория гибридных войн – это теория с западным происхождением и российской спецификой. В Китае этот термин чаще всего употребляется при анализе борьбы между Россией и Западом, мало кто из китайских учёных применяет это заимствованное слово к своей стране, например, говоря о том, что какая-либо страна ведет против Китая гибридные войны (хотя, по сути, есть такой факт). Один и тот же вопрос (по сути) Китай анализирует с использованием своей теории и терминов. Таким образом, «исследование гибридных войн в китайских источниках вплоть до недавнего времени носило обрывочный и фрагментарный характер, принимая форму пересказов»[210] и поверхностных интерпретаций исследований западных и российских экспертов. Но это не означает, что китайские учёные не имеют собственного мнения о формах и методах ведения войн нового типа, просто в своих работах они используют другое название[211]. На самом деле на тему «гибридных войн» можно найти как минимум три источника в Китае:

- во-первых, «Искусство войны», написанное китайским стратегом и мыслителем Сунь Цзы в VI веке до н.э., которое считают одним из базисов теорий современных гибридных войн;

- во-вторых, «идеи, выдвинутые генералами Народно-освободительной армии Китая Цяо Ляном и Ван Сянсуем в своей книге «Неограниченная война» (издана в 1999 году), которые фактически во многом совпадают с идеями гибридной войны»[212];

- в-третьих, Всеобъемлющая концепция национальной безопасности, официально выдвинутая 15 апреля 2014 года председателем Госсовета КНР Си

[210] Ранее было опубликовано в статье: Го Фэнли. Гибридная война в исследованиях ученых Китайской Народной Республики // Гражданин. Выборы. Власть. – 2022. – №1(23). – С. 140–152.
[211] Го Фэнли. Гибридная война в исследованиях ученых Китайской народной республики // Гражданин. Выборы. Власть. – 2022. –№ 1(23). – С. 140–152.
[212] Ранее было опубликовано в статье: Го Фэнли. Гибридная война в исследованиях ученых Китайской Народной Республики // Гражданин. Выборы. Власть. – 2022. – №1(23). – С. 140–152.

Цзиньпином, представляет собой стратегическое руководство для противодействия современным гибридным угрозам и защиты национальной безопасности Китая[213].

Начиная с 18-го съезда КПК (2012 г.), Центральный комитет партии во главе с председателем Си Цзиньпином сделал национальную безопасность главным приоритетом и разработал стратегические планы национальной безопасности, сосредоточившись на общем положении стратегии «Великого возрождения китайской нации» и изменениях мировой ситуации. Подчёркивая важность выбора своего пути обеспечения национальной безопасности «с китайской спецификой», 15 апреля 2014 года китайский лидер Си Цзиньпин впервые официально выдвинул Всеобъемлющую концепцию национальной безопасности (ВКНБ), которая стала первой в истории Коммунистической партии Китая (КПК) стратегической идеей, определяющей деятельность КНР в области национальной безопасности, и фундаментальным руководством для работы по национальной безопасности в новую эпоху. ВКНБ богата философским содержанием и основана на комплексном учете международной обстановки, основных реалий и стратегии развития Китая. В данной концепции слово «всеобъемлющая» обозначает системный характер национальной безопасности, включая как традиционную безопасность, такую как политическая, территориальная и военная безопасность, так и безопасность нового типа, такую как культурная, кибернетическая и экологическая безопасность. В то же время, подчеркивая комплексность национальной безопасности, данная теория выступает против генерализации вопросов безопасности и требует определить границы безопасности[214].

К тому же, в конце 2017 года председатель КНР Си Цзиньпин выдвинул важное утверждение о «колоссальных мировых изменениях, возникших впервые

---

[213] «Основа Всеобъемлющей концепции национальной безопасности» вышла в свет [Электронный ресурс] // Китайское правительство. 2022. URL: http://www.gov.cn/xinwen/2022– 04/15/content_5685392.htm (дата обращения06.05.2022) (《总体国家安全观学习纲要》出版发行 // 中国政府网. 15.04.2022. URL: http://www.gov.cn/xinwen/2022-04/15/content_5685392.htm).

[214]Партийная школа ЦК КПК. Основные вопросы по идеям Си Цзиньпина о социализме с китайской спецификой в новой эпохе. – Пекин: издательство «Партийная школа ЦК КПК», Народное издательство, 2020. – С. 331– 338. （中共中央党校.《习近平新时代中国特色社会主义思想基本问题》, 北京: 中共中央党校出版社；人民出版社, 2020, 331– 338 页).

за столетие» (иногда переводится как «беспрецедентные перемены века»), ставшее горячей темой в китайских научных кругах. По словам Си Цзиньпина, «Социализм с китайской спецификой вступил в новую эпоху. Чтобы хорошо справиться с дипломатической работой в эту эпоху, мы должны правильно понимать веяние времени и международные тенденции. Глядя на мир, мы сталкиваемся с беспрецедентными переменами века»[215]. Данное утверждение быстро набрало популярность в Китае и рассматривается как лучшее резюме нынешней международной ситуации. По мнению китайских ученых, это суждение об огромных изменениях в международном ландшафте и совокупных трудностях в управлении внутри страны[216]. Не менее популярной в Китае является также идея «Сообщества человеческой судьбы», которая была впервые предложена председателем КНР Си Цзиньпином в выступлении в МГИМО во время своего визита в Россию в марте 2013 года. 28 сентября 2015 года на выступлении в общих прениях 70-й сессии Генеральной Ассамблеи ООН председатель Си Цзиньпин детально разъяснил основные коннотации «Сообщества человеческой судьбы» с позиции «пяти аспектов»: партнерство, модель безопасности, перспектива развития, цивилизационный обмен и экологическая система. 18 января 2017 года, выступая с программной речью на заседании «Совместное строительство сообщества человеческой судьбы», китайский лидер не только ответил на вопрос «Что происходит с миром и что мы должны делать?» с исторической и философской точек зрения, но и систематически изложил практический путь строительства Сообщества человеческой судьбы[217].

---

[215]Выступление Си Цзиньпина при встрече с участниками– посланниками в ежегодной рабочей конференции для посланников за рубежом 2017 года [Электронный ресурс] // Центральное народное правительство КНР.2017. URL: http://www.gov.cn/xinwen/2017– 12/28/content_5251251.htm (дата обращения 28.01.2023) (习近平接见 2017 年度驻外使节工作会议与会使节并发表重要讲话 // 中华人民共和国中央人民政府. 2017 年 12 月 28 日).

[216]Мир находится в разгаре великих перемен, невиданных за столетие [Электронный ресурс] // BeijingDaily. 2019. URL: https://ie.bjd.com.cn/bjd/Html/20190114/0/7ED2E8CD5F30C46APhone.html?newsid=7ED2E8CD5F30C46A&from-groupmessage&isappinstalled=0 (дата обращения 28.01.2023) （世界处于百年未有之大变局 // 北京日报. 2019 年 1 月 14 日）; Цзинь Канронг. Интерпретация «беспрецедентные изменения за столетие» [Электронный ресурс] // Наблюдатель. 2020. URL: https://www.guancha.cn/JinCanRong/2020_10_16_568238.shtml (дата обращения 28.01.2023) (金灿荣：解读“百年未有之大变局” // 观察者网.2020 年 10 月 16 日).

[217] Строим лучший мир вместе — К 10– летию идеи Председателя КНР Си Цзиньпина о создании Сообщества человеческой судьбы [Электронный ресурс] // Центральное народное правительство КН Р. 23. 03.2023. URL: http://www.gov.cn/xinwen/2023– 03/23/content_5747952.htm (дата обращения 28.01.2023) (携手建设更加美好的世

Все вышеизложенные идеи и концепции являются частью системы теории и практик, инициированной КНР в ответ на международную турбулентность. Таким образом, можно констатировать, что теория гибридных войн большее внимание уделяет «внешним силам» и «угрозам», а китайский подход сосредоточен на «внутреннем управлении» и «безопасности». Как и государственное устройство КНР, подобная позиция Китая по международной ситуации и национальной безопасности имеет яркую китайскую специфику со строгой и чёткой логикой.

Определяя Китай главным конкурентом, США используют все больше методов и технологий гибридных войндля сдерживания Поднебесной и защиты своего господства – провоцирование торговых войн, подавление китайской высокотехнологичной промышленности, «поощрение сепаратистских настроений на Тайване и Гонконге, создание новых военно-стратегических объединений в Индо-Тихоокеанском регионе – всё это наиболее очевидные проявления многосторонней, гибридной войны»[218].Типичные гибридные методы США в отношении Китая также включают:

1) информационно-психологические методы. Используя преимущества в глобальной коммуникационно-технологической сфере, США дискредитируют Китай с помощью вброса дезинформации, включая обвинение в адрес китайской модели развития и пропаганду так называемой «теории китайской угрозы», чтобы очернить международный имидж Китая и поколебать политические убеждения его внутренней общественности. В частности, такие районы с особой историей и геополитическим значением, как Синьцзян, Гонконг и Тибет, часто попадают в фокус американской информационной войны. Международное медиаагентство США утверждает, что «успешно» провело различные медиапроекты в китайских регионах Гуандун, Синьцзян и Тибет[219]. В 2021 году, исказив факты путём так называемых «рыбацких интервью», канал CNN сфабриковал сущест-

界—写在习近平主席提出构建人类命运共同体理念十周年之际 // 中华人民共和国中央人民政府.2023 年 3 月 23 日).

[218] Тавровский Ю. В. США–Китай: идёт война гибридная [Электронный ресурс] // Независимая. 02.09.2018.URL: https://www.ng.ru/dipkurer/2018-09-02/9107301_dipuschina.html (дата обращения: 06.03.2022).

[219] U.S. Agency for Global Media: FY 2021 Congressional Budget Justification. [Электронный ресурс] // U.S.DEPARTMENTofSTATE. 2020. URL: https://www.state.gov/wp-content/uploads/2020/02/FY-2021-CBJ-Final.pdf (дата обращения: 06.03.2022).

вование в Синьцзяне (СУАР, Синьцзян-Уйгурский автономный район КНР) таких сенсационных «преступлений», как «принудительный труд», «принудительная стерилизация» и даже «геноцид», на этом основании Вашингтон наложил санкцию на ряд китайских учреждений и граждан[220];

2) политические методы. Во-первых, США оказывают политическую поддержку сепаратистам и антиправительственным организациям Китая, в особенности в Гонконге и Тибете. Во-вторых, США пытались объединить своих союзников и мобилизовать международное сообщество по вопросам Гонконга и Синьцзяна, чтобы изолировать Китай. 28 мая 2020 года США вместе с Австралией, Канадой и Великобританией опубликовали «Совместное заявление по Гонконгу», заявив, что Китай подорвал «свободу и автономию» Гонконга, что вызвало «глубокую озабоченность» этих стран[221]. Впоследствии на 47-й сессии ООН, состоявшейся 22 июня 2021 года, США объединили позиции своих союзников в «Совместном заявлении о ситуации с правами человека в Синьцзяне»[222];

3) экономические методы. С марта 2018 года США провоцировали торговую войну с Китаем, и, одновременно, начали проводить политику по подавлению развития науки и техники Китая. В мае 2019 года США определили технологический гигант Китая Huawei как «угрозу национальной безопасности»[223] и внесли его в «чёрный список»[224]. Кроме того, Вашингтон также оказал значительное давление на своих союзников и партнёров, чтобы те присоединились к блокаде Huawei, заявив, что предоставляемые ею услуги несут в себе риски, свя-

---

[220]Выступление пресс-секретаря МИД КНР ХуаЧуньи на пресс-конференции 26 марта 2021 года [Электронный ресурс] // Embassy of the People's Republic of China in the Democratic Socialist Republic of Sri Lanka. 2021. URL: http://lk.china– embassy.org/fyrth/202103/t20210326_8909867.htm (датаобращения: 06.03.2022) (2021 年 3 月 26 日外交部发言人华春莹主持例行记者会 //中华人民共和国驻斯里兰卡民主主义社会共和国大使馆.26.03.2021. URL: http://lk.china-embassy.org/fyrth/202103/t20210326_8909867.htm

[221] Joint Statement on Hong Kong [Электронный ресурс] // U.S. Department of State . 2021.URL: https://www.state.gov/joint-statement-on-hong-kong/ (дата обращения: 06.12.2021).

[222]Joint statement on human rights situation in Xinjiang at 47th Session of UN Human Rights Council [Электронный ресурс] // the Government of Canada. 2021. URL: https://www.international.gc.ca/world-monde/international-relations-relations_internationales/un-onu/statements-declarations/2021-06-22-statement-declaration.aspx?lang=eng (дата обращения: 06.12.2021).

[223] Trump administration hits China's Huawei with one– two punch [Электронный ресурс] // Reuters. 2019. URL: https://www.reuters.com/article/us-usa-china-trump-telecommunications/trump-administration-hitschinas-huawei-with-one-two- punch-idUSKCN1SL2QX (дата обращения: 06.12.2021).

[224] Trump's blacklisting of Huawei is failing to halt its growth [Электронный ресурс] // Bloomberg. 06.01.2020. URL: https://www.bloomberg.com/news/articles/2020-01-06/trump-s-blacklisting-of-huawei-is-failing-to-halt–its-growth (дата обращения: 06.12.2021).

занные с разведкой[225]. Хотя европейские партнёры Вашингтона уже разобрались в том, что Huawei не представляет технической угрозы безопасности (об этом официальные органы Великобритании, Франции и Германии обнародовали свои выводы расследования, и нижеупомянутые публичные выступления высокопоставленных чиновников Великобритании также подтверждают этот факт)[226], они были вынуждены объединиться в борьбе с Huawei из-за давления со стороны США.

США также оказывают экономическую поддержку антиправительственным группам в Китае. Так, в период 1990-2018 годы Национальным фондом демократии (NED) было вложен порядка 13 миллионов долларов США в поддержку развития «демократии» Гонконга – в «правозащитные» НПО, которые затем стали организаторами и основными участниками протестных демонстраций. В инциденте гонконгских протестов против законопроекта об экстрадиции 2019 г.[227] сотрудники ЦРУ вместе с Национальным фондом демократии (NED) даже лично присоединились к группе протеста и руководили ею в попытке устроить «цветную революцию» в Гонконге[228].

Руководствуясь «Всеобъемлющей концепцией национальной безопасности» (ВКНБ), КНР продолжает совершенствовать систему обеспечения общей национальной безопасности, систему обеспечения правопорядка и систему обра-

---

[225] Wintour P. US urges Britain to take another 'hard look' at letting Huawei into 5G [Электронный ресурс] // The Guardian. 2020. URL:https://www.theguardian.com/technology/2020/feb/14/us-urges-britain-to-take-another-hard-look-at-letting-huawei-into-5g (дата обращения: 10.12.2021).

[226]См., напр.: заявления представителей Британского национального центра кибербезопасности (NCSC)，Германского федерального управления по информационной безопасности (BSI)，Французского национального агентство кибербезопасности (ANSSI): Britain managing Huawei risks, has no evidence of spying: official [Электронный ресурс] // Reuters. 2019. URL: https://www.reuters.com/article/us-huawei-europe-britain-idUSKCN1Q91PM) (дата обращения: 20.12.2021); German IT watchdog says ‘no evidence’ of Huawei spying [Электронный ресурс] // Thelocal. 2018. URL: https://www.thelocal.de/20181216/german-it-watchdog-says-no-evidence-of-huawei-spying/ (дата обращения: 10.11.2021); There’s no proof to show Huawei was spying in Europe, France says [Электронный ресурс] // The print.2020.URL:https://theprint.in/world/theres-no– proof-to-show-huawei-was-spying-in-europe-france-says/357011/ (дата обращения: 20.12.2021).

[227] Dan Cohen. Behind a made– for–TV Hong Kong protest narrative, Washington is backing nativism and mob violence [Электронный ресурс] // The Gray zone. 2019.URL: https://www.state.gov/joint-statement-on-hong-kong/ (дата обращения: 08.12.2021).

[228] Выступление пресс-секретаря МИД КНР Хуа Чуньин на пресс-конференции 26 марта 2021 года [Электронный ресурс]// Embassy of the People’s Republic of China in the Democratic Socialist Republic of Sri Lanka. 2021. URL: http://lk.china-embassy.org/fyrth/202103/t20210326_8909867.htm (дата обращения: 06.03.2022) (2021 年 3 月 26 日外交部发言人华春莹主持例行记者会 //中华人民共和国驻斯里兰卡民主主义社会共和国大使馆.26.03.2021. URL: http://lk.china‐embassy.org/fyrth/202103/t20210326_8909867.htm).

зования в области национальной безопасности, а также повышать уровень осведомлённости всех слоев общества Китая о целях, задачах и угрозах национальной безопасности.

В январе 2014 года была официально создана Центральная комиссия национальной безопасности (ЦКНБ), после чего 15 апреля 2014 года состоялось первое заседание ЦКНБ, на котором генсекретарь Си Цзиньпин официально предложил ВКНБ курировать как внешнюю, так и внутреннюю безопасность страны. После этого ЦКНБ оперативно опубликовала «Руководство для кадров по ВКНБ» и на различных уровнях государственного аппарата была проведена большая работа по совершенствованию системы национальной безопасности.

1 июля 2015 года был обнародован первый в Китае настоящий всеобъемлющий «Закон о национальной безопасности»[229], согласно которому 15 апреля каждого года является «Днем образования в области национальной безопасности (National Security Education Day)[230]. Впоследствии под руководством ВКНБ был принят ряд законов и нормативных актов в области национальной безопасности, включая «Закон о борьбе с терроризмом», «Закон об управлении внутренней деятельностью иностранных неправительственных организаций», «Закон о кибербезопасности», «Закон о национальной разведке», «Правила реализации Закона о борьбе со шпионажем», «Закон о поддержании национальной безопасности в САРГ», «Закон о биологической безопасности» и т.д. Таким образом, правовая система национальной безопасности в КНР постепенно формируется.

Китай имеет долгую историю ведения пропаганды и образования в области национальной безопасности, но в прошлом содержание такого образования в основном ограничивалось традиционными областями безопасности, такими как

---

[229] Еще в 1993 году в Китае был принят «Закон о национальной безопасности», но этот закон не соответствовал своему названию, так как назывался «национальная безопасность», а по сути представлял собой «расследование по борьбе со шпионажем». После введения Всеобъемлющей концепции национальной безопасности в ноябре 2014 года в «Закон о национальной безопасности» в редакции 1993 года были внесены поправки, которые превратились в «Закон о борьбе со шпионажем», а 1 июля 2015 г. был обнародован действительно всеобъемлющий «Закон о национальной безопасности».

[230] Министерство юстиции и Национальное управление по пропаганде права КНР развёртывают кампанию по пропаганде права на 2020 г. в рамках Дня образования в области национальной безопасности [Электронный ресурс] // Синьхуа. 2020.URL: http://www.xinhuanet.com/legal/2020– 04/07/c_1125823054.htm (дата обращения: 12.06.2022) (司法部、全国普法办部署开展 2020 年全民国家安全教育日普法宣传活动 //新华网.07.04.2020).

секретность и контршпионаж. Под руководством ВКНБ пропаганда и обучение в области национальной безопасности приобрела новый вид, расширившись до широкого спектра областей безопасности. В соответствии с «Законом о национальной безопасности» в последние годы развивается не только осведомлённость по национальной безопасности всего населения страны, но и система образования в области национальной безопасности, при этом образование по специальности «национальной безопасности» также было включено в учебные планы административных отделов образования и ВУЗов. Так, 14 апреля 2021 года был создан Исследовательский центр ВКНБ – специальное учреждение для проведения систематических исследований ВКНБ с целями совершенствовать теоретическую систему ВКНБ, продвигать стратегические идеи данной теории, как внутри страны, так и за рубежом, фокусироваться на обслуживании процесса принятия решений по вопросам национальной безопасности и выдвигать политические рекомендации по обеспечению национальной безопасности. К тому же, в некоторых ВУЗах были организованы исследовательские центры национальной безопасности, и там же усиливается популярность специальности «национальная безопасность». Тем самым, ситуация с общим и профессиональным образованием в области национальной безопасности Китая значительно улучшилась.

По-прежнему акцентируя на экономическое строительство как на центральное звено, Китай продолжает развивать свою «жёсткую силу» и укреплять общую национальную мощь. Это основа для обеспечения социальной стабильности страны и эффективного противодействия внешним угрозам. В этом плане «отец мягкой силы» Джозеф Най неоднократно подчёркивал, что «жесткая сила» государства, включая военную мощь, по-прежнему играет важную роль в современной мировой системе[231]. Со второго десятилетия XXI века международный дискурс Китая значительно усилился в игре великих держав, в основном благодаря быстрому экономическому развитию страны, повышению уровня жизни его народа и стремительному росту его международного влияния.

[231] Nye J. Is Military Power Becoming Obsolete? [Электронный ресурс] // Project Syndicate. 2010. URL: https://www.project-syndicate.org/commentary/is-military-power-becoming-obsolete-2010-01 (дата обращения: 12.06.2021).

Особое внимание уделяется улучшению жизни народа и совершенствованию механизма предотвращения и разрешения социальных конфликтов. Один из главных ценных опытов Китая в этом аспекте заключается в том, что, сохраняя темпы экономического развития, он придает большое значение повышению комплексности, координации и устойчивости развития на основе продвижения социальной справедливости и благосостояния народа, а также придает большое значение примирению интересов всех сторон общества, тем самым предотвращает и уменьшает социальные конфликты у истоков. В то же время он постоянно совершенствует институциональные механизмы защиты законных прав и интересов массовых слоев населении и механизмы оценки рисков социальной стабильности для предотвращения и снижения конфликтов интересов, а также создает благоприятные условия для того, чтобы направлять общественные силы на разрешение различных социальных конфликтов с помощью правовых процедур. В том числе, Китай расширяет каналы раскрытия информации о принятии решений местными органами власти, стандартизирует электронное правительство и улучшает функцию выражения общественного мнения, для которого действуют «правительственные почтовые ящики», онлайн-коммуникации и другие разделы. Чтобы упростить иерархию, ускорить предоставление информации и повысить прозрачность информации о принятии решений, Генеральный офис Госсовета КНР открыл рубрику «Жалобы и предложения по государственным услугам», чтобы общественность могла отразить свои мнения и внести предложения по улучшению государственных услуг и оптимизации бизнес-среды. Кроме того, в целях дальнейшего повышения уровня государственных услуг был создан механизм быстрого реагирования, основным каналом для выражения жалоб населения стала горячая линия «12345», по которой предоставляются круглосуточные услуги живыми операторами в режиме 24/7, что позволяет населению более удобно и своевременно решать проблемы и отражать свои требования, а правительству – повысить эффективность своих услуг[232].

[232]О дальнейшем совершенствовании Горячей линии правительственных услуг [Электронный ресурс] // Центральное народное правительство КНР. 08.01.2021.URL: http://www.gov.cn/zhengce/2021–

Придерживаясь принципа историзма, Китай активно стремляется к международному сотрудничеству для совместного противодействия гибридным угрозам. В ответ на технологическое эмбарго США Китай сосредоточился на дружественных Китаю технологических державах и развивает с ними технологическое сотрудничество, что эффективно страхует его от негативных последствий американского технологического контроля. Так, в 2018 году Китай и Россия подписали пакет соглашений о сотрудничестве в ядерном секторе; в марте 2021 года Китай и Иран подписали 25-летнее соглашение о стратегическом сотрудничестве, охватывающее финансы, телекоммуникации, железные дороги, здравоохранение, информацию и другие технологическиемкие области. Все эти проекты международного технологического сотрудничества станут для Китая важным рычагом для преодоления технологической блокады Вашингтона. Если взять в качестве примера сотрудничество между Россией и Китаем, то у двух стран есть большие перспективы для сотрудничества в области защиты национальной безопасности. Так, в марте 2021 года министр иностранных дел Китая Ван И предложил Китаю и России совместно решить проблему «цветной революции»[233].

01/08/content_5577884.htm (дата обращения: 20.10.2021) (政务服务便民热线有了“总客服”// 中华人民共和国中央人民政府. 08.01.2021. URL: http://www.gov.cn/zhengce/2021-01/08/content_5577884.htm).

[233] Скосырев В. КНР предлагает России вместе бороться с цветными революциями [Электронный ресурс]// Независимая газета. 2021. URL: https://www.ng.ru/world/2021-03-09/18097china.html (дата обращения: 12.06.2022).

Выводы по главе I.

Современные гибридные войны представляют собой сложное конвергентное явление и выражаются в комплексном использовании широкого набора сил и средств борьбы, прежде всего невоенных, объединённых единым замыслом и согласованных по целям, задачам, методам и инструментам воздействия на противника. Целью таких войн, как правило, становится продвижение собственных национальных интересов в сфере международных отношений и соперничества между государствами за ресурсы, смыслы и влияние.

Современные научные подходы к гибридным войнам сегодня можно классифицировать по типам. В зависимости от содержимого фокуса исследования существующие научные работы по данной теме классифицированы автором на два типа. Первый тип (в теоретическом плане) исследования посвящён теоретической дискуссии, в частности, сосредоточен на том, в какой степени новая теория ознаменовала собой перелом в военной мысли, какова связь межу теорией гибридных войн и традиционными представлениями о войне. Второй тип исследования (в практическом плане) рассматривает, как новые идеи гибридных войн влияют на государственную политику и реализованы в практике. К тому же, по отношению к феномену гибридных войн вокруг вопроса о ценности исследования по данной тематике современные научные подходы представлены двумя крупными течениями, или школами: консервативный и новаторской, каждый из которых включает в себя две платформы: умеренную и радикальную.

В современных гибридных войнах используется широкий диапазон инструментов, в основном невоенных, при этом неотъемлемой составляющей в структуре гибридных войн остаётся её военная часть, использование которой все чаще осуществляется в форме сплава традиционных общевойсковых или специ-

альных военных операций с «креативным» формами и методами ведения боевых действий, осуществляемыми некомбатантами. Все большее значение приобретает внедрение робототехники и различных форм дистанционной войны, а также технологий ИИ, что следует рассматривать как объективную тенденцию. В войнах будущего «Битва за мозг» противника (термин, введенный военными экспертами США) с большой степенью вероятности станет главной и приоритетной целью любой гибридную войну.

Триада ценности теории гибридных войн заключается в следующем:

1) интегрировав различные концепции подобного рода под одним «зонтичным брендом», данный неологизм отличается неограниченной инклюзивностью и адаптивностью и стал «терминатором» различных концепций о современных международных противоборствах;

2) данный термин адекватно описывает облик современной международной системы отношений в ее конфликтном измерении и раскрывает, настолько расширился инструментарий агрессивного воздействия на противника. Ценность данной концепции выросла в глазах международных и региональных держав и организаций, которые рассматривают гибридные войны как удобное средство для анализа сегодняшних международных конкурентов и противоборств и выработки предметных планов;

3) Гибридные войны стали главным инструментом современной международной борьбы и их распространение формирует новый мировой ландшафт. Гибридные войны могут стать состоянием существования международной системы в ближайшем будущем.

Все это обусловило то, что феномен гибридных войн будет сохранять свое долгосрочное присутствие, при этом давно созрела возможность для России перейти от теоретической дискуссии на стратегическое и тактическое применение технологий гибридных войн. В этом плане опыт НАТО и Китая в ответ на гибридные угрозы даёт некие полезные уроки для других стран, включая Россию.

Глава II. Российский опыт противодействия гибридным войнам[234]

2.1. Гибридизация традиционных вооружённых конфликтов, информационных войн и цветных революций как новый источник вызовов и угроз национальной безопасности Российской Федерации

«Перераспределение мирового потенциала развития, формирование новой архитектуры, правил и принципов мироустройства сопровождаются нарастанием геополитической нестабильности, обострением межгосударственных противоречий и конфликтов»[235]. Новые реалии международной политики ставят перед Россией беспрецедентно суровые вызовы и угрозы. В этом контексте вопросам обеспечения национальной безопасности Российской Федерации руководством страны уделяется повышенное внимание[236]. При этом в России сформирована достаточно объёмная система документов стратегического планирования на дан-

[234] При подготовке данного раздела диссертации использованы следующие публикации, выполненные автором лично или в соавторстве, в которых, согласно Положению о присуждении ученых степеней в МГУ, отражены основные результаты, положения и выводы исследования: Го, Фэнли. Гибридная война в исследованиях ученых китайской народной республики / Ф. Го // Гражданин. Выборы. Власть. – 2022. – № 1(23). – С. 140-152; Го, Фэнли. Особенность противодействия информационным операциям со стороны Российской Федерации / Ф. Го // Вопросы национальных и федеративных отношений. – 2023. – Т. 13. – № 6 (99). – С. 2554-2560; Го Фэнли. Российский подход к информационному противоборству / Ф. Го // Вопросы политологии. – 2023. – Т. 13. – № 3 (91). – С. 1253-1260; Го, Фэнли. Гибридная война США и их союзников против России в контексте специальной военной операции / Ф. Го // Гражданин. Выборы. Власть. – 2023. – № 2 (28). – С. 146-155; Го, Фэнли. Гибридная война США и их союзников против России в контексте специальной военной операции / Ф. Го // Гражданин. Выборы. Власть. – 2023. – № 2 (28). – С. 146-155; Го, Фэнли, Манойло, А.В. Торговая война США против Китая в период президентского правления Д. Трампа как составляющая современных гибридных войн / Ф. Го, А.В. Манойло // Вестник Московского университета. Серия 12. Политические науки. –2022. – № 5. – С. 81-92.

[235] Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] // Президент России. 2021. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 25.10.2022).

[236] Путин рассказал о состоянии безопасности в России [Электронный ресурс] // РИА НОВОСТЬ. 2022. URL: https://ria.ru/20221025/putin-1826724536.html (дата обращения: 25.10.2022).

ном направлении[237], среди которых одним из важнейших является Стратегия национальной безопасности Российской Федерации.

Стратегия национальной безопасности Российской Федерации (далее – «Стратегия»)[238] – это базовый документ по планированию развития системы обеспечения национальной безопасности России, который был принят в 2021 году, сменив утратившую силу Стратегию национальной безопасности Российской Федерации в редакции 2015 года. В обновлённой Стратегии национальной безопасности России (далее – «Стратегия-2021») зафиксированы национальные интересы и стратегические приоритеты Российской Федерации, разъяснён ряд важнейших вопросов по обеспечению национальной безопасности.

Анализ действующих документов стратегического планирования России, в частности, «Стратегии-2021», и реалии нынешней ситуации позволили выделить следующие основные вызовы и угрозы национальной безопасности России.

«Рост геополитической нестабильности и конфликтности, усиление межгосударственных противоречий сопровождаются повышением угроз использования военной силы»[239]. Ослабление и разрушение норм и принципов международного права, продолжающийся демонтаж системы договоров и соглашений в области контроля над вооружениями ведут к нарастанию напряжённости и обострению военно-политической обстановки, в том числе вблизи государственной границы России. «Называя Россию угрозой и даже военным противником, некоторые западные страны инициируют в СНГ дезинтеграционные процессы для подрыва связей России с её традиционными союзниками»[240]. «Попытки силового давления на Россию, её союзников и партнёров, расположение военной инфраструктуры НАТО вблизи российских границ, активизация разведывательной деятельно-

[237] Назаров В. П., Афиногенов Д. А. Проблемы развития общей теории национальной безопасности в контексте корректировки Стратегии национальной безопасности Российской Федерации [Электронный ресурс] // Власть. 2020. Том 28, № 1. С. 9–19.

[238] Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] // Президент России. 2021. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 25.10.2022).

[239] Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] // Президент России. 2021. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 25.10.2022).

[240] Там же.

сти, отработка применения против России наёмников» [241] также способствуют усилению военных рисков для Российской Федерации. «Увеличивается опасность перерастания вооружённых конфликтов в локальные и региональные войны»[242], в том числе, с участием ядерных держав. В этом отношении наиболее характерным примером (хотя предыдущие инциденты с попыткой прохода украинских кораблей через Керченский пролив в ноябре 2018 года и провокация британского эсминца Defender вблизи Крыма в июне 2021 года были также резонансными случаями) служит военный конфликт между Россией и Украиной, точнее говоря, между Россией и «Коллективным Западом», что уже стало одной из наиболее актуальных угроз безопасности не только для России, но и всего мира на данном этапе.

Наряду с обострением традиционных угроз безопасности, перед Россией стоят нетрадиционные угрозы, под которыми понимаются угрозы, исходящие от неклассических акторов международных отношений (в частности, организаций и группировок международного терроризма), военные угрозы, исходящие непосредственно от некоторых государств (например, милитаризация киберпространства), или невоенные угрозы (экологические, биологические, демографические и миграционные проблемы)[243]. Основными формами нетрадиционных угроз безопасности России на данном этапе являются:

• разведывательная и иная деятельность специальных служб и организаций иностранных государств, отдельных лиц, наносящая ущерб национальным интересам;

• деятельность террористических и экстремистских организаций;

• деятельность по инспирированию цветных революций;

---

[241] Там же.
[242] Там же.
[243] Buzan B. New patterns of global security in the twenty– first century // International affairs. – 1991. –Vol. 67, № 3. – P. 433–451.

• размывание традиционных российских духовно-нравственных ценностей и ослабление единства многонационального народа Российской Федерации [244].

И, наконец, все большей угрозой становятся кибернетические и информационные атаки, а также – цветные революции.

Бурное развитие и распространение информационно-коммуникационных технологий (ИКТ) повышает вероятность возникновения ряда нетрадиционных угроз международному миру и безопасности, в частности, в отношении самой России. Прежде всего, использование в России иностранных ИКТ и оборудования повышает её уязвимость к деструктивным воздействиям из-за рубежа, что воплощается не только в увеличении количества компьютерных атак со стороны иностранных государств «на российские информационные ресурсы, включая объекты критической информационной инфраструктуры»[245] страны, но и в «активизации деятельности спецслужб иностранных государств по проведению разведывательных и иных операций в российском информационном пространстве в целях дестабилизации общественно-политической ситуации»[246], подрыва её суверенитета и нарушения территориальной целостности России. При этом анонимность в сети Интернет облегчает совершение преступлений, расширяет возможности для легализации доходов, полученных преступным путём, и финансирования терроризма, распространения наркотических средств и противоправной информации. Так, в Интернете часто размещаются недостоверная информация и фейковые новости (фейки), «материалы террористических и экстремистских организаций, призывы к массовым беспорядкам, осуществлению экстремистской деятельности, совершению самоубийств, осуществляется пропаганда криминального образа жизни, потребления наркотических средств»[247]и т.д. К тому же, стремление транснациональных корпораций к монопольному положению в сети

[244] Стратегии национальной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 31.12.2015 г. № 683 [Электронный ресурс] // Президент России. 2015. URL: http://www.kremlin.ru/acts/bank/40391 (дата обращения: 20.09.2022).
[245] Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] // Президент России. 2021. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 25.10.2022).
[246] Там же.
[247] Там же.

и контролированию всех информационных ресурсов блокирует «альтернативные Интернет-платформы и конструктивную информацию, из-за чего пользователям сети навязывается искажённый взгляд на исторические факты, а также на события, происходящие в Российской Федерации и в мире»[248].

«Российские духовно-нравственные и культурно-исторические ценности подвергаются активным нападкам со стороны США и их союзников, а также со стороны транснациональных корпораций и иностранных некоммерческих неправительственных организаций»[249]. Они оказывают информационно-психологическое воздействие на общественное сознание путём целенаправленного размывания российских традиционных ценностей, фальсификации исторической правды, формирование враждебного образа России, реабилитации фашизма, разжигания межнациональных и межконфессиональных конфликтов. На фоне кризиса западной либеральной модели участились попытки информационно-психологических диверсий и «вестернизации» культуры, что усиливает угрозу диверсификации российских духовно-нравственных и культурно-исторических ценностей, которые «формировались на протяжении столетий отечественной истории и рассматриваются в качестве основы российского общества, позволяющей сохранять и укреплять суверенитет Российской Федерации и достигать новых высот в развитии общества и личности»[250].

Согласно Стратегии национальной безопасности Российской Федерации 2015 года (утратившей силу в связи с принятием Стратегии-2021, но, тем не менее, представляющей определённый интерес с точки зрения изучения истории вопроса), одной из «основных угроз государственной безопасности является деятельность радикальных общественных объединений и иностранных организаций, а также частных лиц, направленная на дестабилизацию внутриполитической и социальной ситуации в стране, включая инспирирование цветных революции»[251].

---

[248] Там же.
[249] Там же.
[250] Там же.
[251] Стратегии национальной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 31.12.2015 г. № 683 [Электронный ресурс] // Президент России. 2015. URL: http://www.kremlin.ru/acts/bank/40391 (дата обращения: 20.09.2022).

Здесь впервые в документе стратегического планирования был представлен термин «цветная революция», что отражает обострение противоречий между Россией и Западом после «Евромайдана» на Украине. На сегодняшний день в условиях, когда Гибридные войны стали доминирующим инструментом межгосударственной борьбы, угроза цветных революций постоянно модернизируется и обостряется.

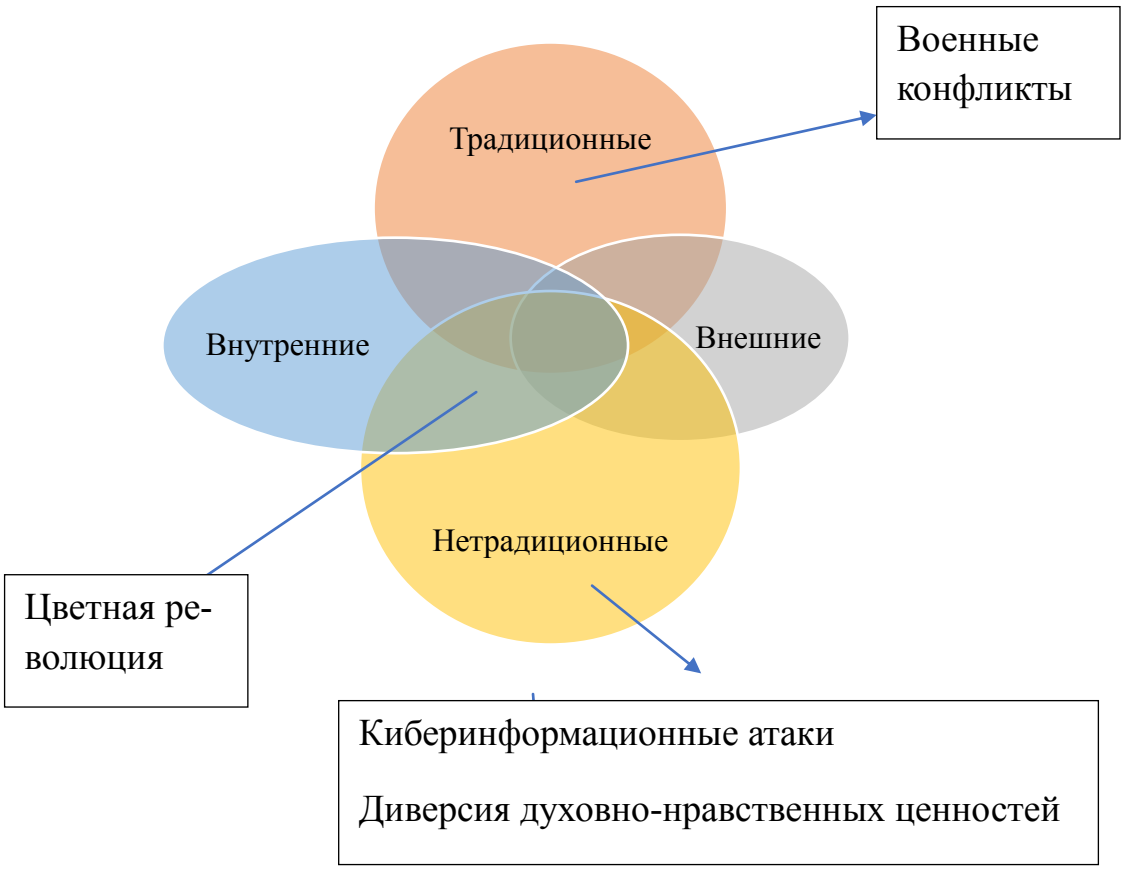


Схема 4. Основные формы угроз национальной безопасности РФ

Следует учитывать, что, хотя информационные «штабы» «дестабилизаторов» находятся за рубежом, предпосылками для запуска процесса цветных революций являются внутренние противоречия, присущие любому обществу. Причём «в России имеются все основания говорить о противоречиях достаточно острых, способных породить энергию стихийного недовольства»[252]. В частности, потенциально опасными являются тенденции снижающегося уровня жизни граждан

[252] Чепрасов К. В. Создание национальной гвардии как ответ на гибридные вызовы безопасности России // Вопросы безопасности. – 2016. – № 2. – С. 8– 19.

России, увеличения поляризации отдельных групп общества и социального расслоения, разрастания масштабов коррупции. Все это выступает потенциальными «узлами критичности» российской государственности, на которые могут воздействовать средствами «мягкой силы». Как отметила А. Шевченко, на данный момент внутренние проблемы угрожают стране и обществу сильнее, чем вызовы из-за рубежа, хотя последние тоже никуда не исчезли»[253].

Резюмируя вышеуказанное, можно констатировать, что сегодня национальная безопасность Российской Федерации сталкивается с широким спектром гибридных угроз (схема 4). Гибридизация традиционных вооружённых конфликтов и появление новых вызов и угроз, в частности, информационных войн и цветных революций, их комплексность и непредсказуемость требуют системного подхода к обеспечению безопасности страны. Как показано в стратегическом документе «Стратегия-2021», руководство РФ готово применять симметричные и ассиметричные меры в ответ на гибридные угрозы[254].

Формы и методы гибридной войны США и их союзников против России

Разноплановость и многомерность гибридных войн требует выявить наиболее угрожаемые направления и сосредоточить основные силы и ресурсы на них. «В сложившихся условиях наиболее активными фронтами гибридной войны США и их союзников против России являются военное, экономическое и информационно-психологическое давление»[255]. Стоит отметить, что происходящее на Украине – это типичная гибридная война Вашингтона против России руками «прокси», в роли которого выступают режим Зеленского и другие прямые участники конфликта, воюющие против России. Наступательный и оборонительный подход гибридных войн, продемонстрированный США и Россией в контексте СВО, стал наглядным и новейшим материалом для исследования стратегии и контрстратегии гибридных войн.

---

[253] Цит. по Коренев Е. «Осажденная крепость» с открытыми воротами. Новая Стратегия национальной безопасности РФ [Электронный ресурс] // РСМД. 2022. URL: https://russiancouncil.ru/analytics-and-comments/ columns/ riacdigest/-osazhdennaya-krepost-s-otkrytymi-vorotami-novaya-strategiya-natsionalnoy-bezopasnosti-rf/ (дата обращения: 01.10.2022)

[254] Там же.

[255] Бартош А. А. Стратегия и контрстратегия гибридной войны // Военная мысль. — 2018. — № 10. — С. 5–20.

Военное давление США на Россию осуществляется в основном следующим образом:

во-первых, разрушение системы контроля над вооружениями с целью открытия «клапана» гонки вооружений с Россией. Это особенно активно проявилось в деятельности администрации Д. Трампа. Так, в 2019 году Вашингтон прекратил участие США в Договоре о ликвидации ракет средней и меньшей дальности (ДРСМД), открыв путь к развёртыванию гиперзвуковых ракет в Восточной Европе с коротким подлётным временем до Москвы, в 2020 году он вышел из Договора по открытому небу и угрожал выйти из Договора по запрещению ядерных испытаний (ДВЗЯИ)[256];

во-вторых, прямые военные провокации, включая размещение американских вооружённых сил в Европе и усиление военного присутствия НАТО в Восточной Европе, а также проведение отдельных провокационных мероприятий в виде военных учений у российских границ. Настойчиво расширяя военное присутствие в Европе, по состоянию на март 2022 года Соединённые Штаты уже располагают 100 тыс. военнослужащих в Европе[257]. Несмотря на декларации Вашингтона о защите Европы, очевидная цель – подавление России военными средствами. С развёртыванием системы ПРО в Восточной Европе и второго позиционного района стратегической ПРО в Польше вся европейская часть России станет мишенью для американских крылатых ракет. При этом значимая часть военных провокаций и мер сдерживания в отношении России осуществляется союзниками и сателлитами США, в частности, входящими в НАТО. В последние годы Североатлантический союз продолжительно усиливает своё военное присутствие в восточной части альянса. На встрече НАТО в верхах 2016 года в Варшаве союзники приняли решения о крупнейшем усилении коллективной обороны альянса за последнее поколение – создание усиленного передового присутствия на северо-востоке Североатлантического союза и специальное передовое

[256] Арбатов А. Г. Украинский кризис и стратегическая стабильность. // Полис. Политические исследования. – 2022. –№ 4. – С. 10– 1.

[257] США довели группировку своих войск в Европе до 100 тысяч человек[Электронный ресурс] // Интерфакс. 2022. URL: https://www.interfax.ru/world/829578 (дата обращения: 25.01.2023).

присутствие на юго-востоке. В результате чего в 2017 году четыре многонациональные боевые группы были созданы в Латвии, Литве, Польше и Эстонии. В контексте СВО были дополнены ещё четыре новых многонациональных боевых групп в Болгарии, Венгрии, Румынии и Словакии при усилении существующих боевых групп на северо-востоке, при этом союзники договорились увеличить размер многонациональных боевых групп с батальона до бригады при необходимости[258];

в-третьих, разжигание войны и конфликтов чужими руками в виде «прокси». Происходящее на поле боя на Украине является живым примером этого излюбленного приёма Пентагона. Одной из основ американской внешней политики является противодействие сближению Европы и России и формирование единой Евразии. На этой основе годами США всячески пытаются вбить клин в отношения между Европой и Россией, вплоть до разжигания сегодняшнего драматического конфликта на европейском поле боя, в котором Украина используется американской стороной в роли плацдарма и контрагента[259].

Основные цели продолжающихся годами военных провокаций США против России кроются в следующем: во-первых, втянуть Россию в гонку вооружений и истощить её (стратегия измора) как разорили СССР в своё время; во-вторых, заставить Россию ответить таким образом, чтобы «угрожать европейской безопасности», тем самым, усиливая зависимость безопасности Европы от США и солидарность с НАТО; в-третьих, удовлетворить интересы военно-промышленного комплекса США («переливать кровь» в ВПК США).

Как отметил Ф. Спинни, который почти 30 лет проработал аналитиком в Управлении анализа и оценки программ Министерства обороны США, «ВПК отчасти несёт ответственность за сегодняшний российско-украинский конфликт и активно извлекает из него выгоду»[260]. По официальным данным Пентагона об-

[258] NATO’s military presence in the east of the Alliance [Электронный ресурс] // NATO.2022 URL: nato.int/cps/en/natohq/topics136388.htm (дата обращения: 25.01.2023).
[259] Манойло А. В. Информационные диверсии в конфликте на Украине // Вестник МГОУ. – 2022. – №4.
[260] Interview: U.S. military complex to benefit from Russia– Ukraine conflict: ex– Pentagon analyst [Электронный ресурс] // Xinhua . 2022. URL: https://english.news.cn/20220316/819b5fa5927c462abae6b9a4b5d67 bff/c.html (дата обращения: 06.01.2023)

щая сумма американской помощи Украине с 2014 года достигла 32 миллиардов долларов, из которых 29,3 миллиарда – с начала СВО России на Украине[261]. Несмотря на то, что ещё шестьдесят лет назад президент США Д. Эйзенхауэр в своём «прощальном» обращением предупредил американцев об опасности развития военно-промышленного комплекса страны – «мы должны остро остерегаться приобретения военно-промышленным комплексом чрезмерного влияния в правительственных органах... потенциал чудовищного роста неуместной власти существует и будет развиваться»[262], это прозорливое предостережение не возымело никакого эффекта. За многие годы в США образовался комплексный «механизм наживы на чужих войнах», лоббируемых его огромным ВПК. В результате действия этого механизма масштабы военных расходов и доходов от иностранных военных продаж непрерывно увеличиваются. По данным СИПРИ (Stockholm International Peace Research Institute, SIPRI), военные расходы США в 2021 году составили 801 миллиард долларов, что составляет 38 % от всех мировых расходов на вооружение и больше, чем следующие девять стран вместе взятые[263]. Последний Закон о бюджетных ассигнованиях на национальную оборону (NDAA) увеличивает оборонный бюджет США на 2023 год ассигнования до рекордных 857,9 миллиарда долларов, при этом десять миллиардов долларов предусмотрены на военную помощь Тайваню, 800 миллионов – Украине. Еще шесть миллиардов пойдут на сдерживание России в Европе[264].

Видно, что для защиты глобальной гегемонии Вашингтон решил воевать на два фронта – одна «битва» идет в Европе, а вторая, более новая, в Азиатско-Тихоокеанском регионе. В Азиатско-Тихоокеанском регионе США развивают

---

[261]Pentagon Press Secretary Brig. Gen. Pat Ryder Holds an On–Camera Press Briefing [Электронный ресурс] // U.S. Department of Defense. 2023 URL: https://www.defense.gov/News/Transcripts/Transcript/Arti cle/3288141/pentagon-press-secretary-brig-gen-pat-ryder-holds-an-on-camera-press-briefing/ (дата обращения: 05.02.2023).

[262] President Dwight D. Eisenhower's Farewell Address [Электронный ресурс] // National Archives. 1961. URL: https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address (дата обращения: 25.01.2023).

[263]Tian Nan, Fleurant Aude, Kuimova Alexandra et al. Trends in World Military Expenditure 2021 [Электронный ресурс] // Stockholm International Peace Research Institute. 24.04.2022. URL: https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf (дата обращения: 06.12.2022).

[264] FY23 NDAA Agreement Executive Summary [Электронный ресурс] // United States Senate Armed Services Committee on armed services. 2022. URL: https://www.armed-services.senate.gov/imo/media/doc/fy23ndaa-agreement_-summary.pdf (дата обращения: 06.02.2023).

полным ходом Тихоокеанскую инициативу по сдерживанию (Pacific Deterrence Initiative), направленную на финансирование стратегического соперничества США с Китаем в Индо-Тихоокеанском регионе, при этом пытаются спровоцировать Китай вопросом Тайваня на, видимо, неизбежный силовой ответ (как это сделала Россия на Украине). В европейском регионе, NDAA предусматривает, прежде всего, продление и модификацию Инициативы содействия безопасности Украины (Ukraine Security Assistance Initiative) с наращиванием военной поддержи Украине в 2023 году и упрощением её процедуры. Вместе с тем в рамке финансирования Европейской инициативы сдерживания (the European Deterrence Initiative) повысится боеготовность американских военных сил в Европе. Пентагон не только наживается на региональных беспорядках, но и стимулирует своих союзников увеличивать военные бюджеты. Демонизировать своих соперников, нагнетать политические страхи и региональную напряжённость с лучшим результатом запуска гонки вооружений – это не только привычные методики реализации стратегии «соперничества великих держав» Вашингтона, но и актуальное требование развития его ВПК[265].

На экономическом фронте санкции являются привычным методом Вашингтона для сдерживания своих соперников. После начала СВО США и их союзники постепенно наращивают военную помощь Украине, что сильно истощил российские вооружённые силы на поле боя. По официальным данным Пентагона общая сумма американской помощи Украине с 2014 года достигла 32 миллиардов долларов, из которых 29,3 миллиарда – с начала СВО России на Украине[266]. Ежедневные расходы России на СВО составляют около 1 млрд долларов в день[267]. Наряду с этим, Коллективный Запад наложил на Россию беспрецедентные экономические санкции, в частности, финансовые санкции, торговые ограничении,

[265] Interview: U.S. military complex to benefit from Russia– Ukraine conflict: ex– Pentagon analyst [Электронный ресурс] // Xinhua. 2022. URL: https://english.news.cn/20220316/819b5fa5927c462 abae6b9a4b5d67bff/c.html (дата обращения: 06.01.2023).

[266] Pentagon Press Secretary Brig. Gen. Pat Ryder Holds an On– Camera Press Briefing [Электронный ресурс] // U.S. Department of Defense. 2023 URL: https://www.defense.gov/News/Transcripts/ Transcript/Article/3288141/pentagon-press-secretary-brig-gen-pat-ryder-holds-an-on-camera-press-briefing/ (дата обращения: 05.02.2023).

[267] Абел Аганбегян. Российский академик оценил стоимость военной операции в 1 млрд долларов в день [Электронный ресурс] // Капитал страны. 2023. URL: https://kapital-rus.ru/news/392921-rossiiskii_akademik-ocenil_stoimost_voennoi_operacii_v_1_mlrd_dollar/ (дата обращения: 01.02.2023).

что уже привело к приостановке соответствующих проектов.

Финансовые санкции – это высокоинтенсивная форма экономических санкций. Они могут оказать большее воздействие, чем торговые санкции в нынешней международной финансовой системе, возглавляемой США. Первая волна западных санкций после СВО пришлась на финансовый сектор, в частности: 1) замораживание активов крупнейших российских банков и ограничение их клиринговых и финансовых возможностей; 2) исключение российских банков из системы SWIFT, отрезавшее Россию от международной финансовой системы; 3) замораживание валютных резервов российского центрального банка. По состоянию на 25 февраля 2022 года международные резервы России составляли 629,4 млрд., из которых около половины, находившейся в финансовой системе США и Европы, заморожена; 4) ограничение способности российского центрального банка ликвидировать свои золотые резервы; 5) приостановка операций MasterCard и Visa в России.

В частности, в сфере торговли энергоносителями, жизненно важными для России, реализуется энергетическое эмбарго и прекращение поставок нефтегазового оборудования и компонентов с целью перекрыть «главную артерию» российской экономики. Кроме того, наиболее существенное влияние на реальный сектор экономики России оказывает нарушение логистической цепочки, вызванное технологическими санкциями, торговыми ограничениями и закрытием воздушного пространства и портов для России. Научно-технологические санкции распространились даже на академическую, образовательную и интеллектуальную сферы. Так, некоторые известные журналы запретили российским учёным подавать статьи, немецкий исследовательский фонд отменил все научное сотрудничество с Россией и закрывается доступ российских ученых к международной базе данных научного цитирования (Web of Science).

Суть этих беспрецедентно интенсивных экстремальных санкций заключается в попытке США насильственно «отсоединить» Россию всесторонне: в политической, финансово-экономической, научно-технической сферах и международных делах, с целью изолировать Россию от международной финансово-

экономической системы и сделать ее «островом в мировой экономике» и «изгоем цивилизованных стран».

С начала 21-го века информационно-психологическое противоборство стало все более напряженным в российско-американских отношениях. На фоне СВО Коллективный Запад ведёт ожесточённую войну против России в когнитивной сфере, пользуясь преимуществами СМИ и Интернет-технологий.

Прежде всего, это выражается в блокировании информации от российской стороны, которое осуществляется следующими основными способами:

- во-первых, блокируют официальную российскую информацию на главных Интернет-платформах. Например, YouTube объявил о глобальном запрете каналов российских официальных СМИ, доступ к которым ограничился Mega в ЕС; на праформе Twitter российские официальные СМИ добавили теги и удаляют их посты об украинском конфликте;

- во-вторых, обрыв основных каналов России для передачи информации масштабными кибератаками. По результатам исследования «Лаборатории Касперского», количество кибератак на российские организации в марте 2022 года было в восемь раз больше, чем за тот же период 2021 года[268]. Помимо DDoS-атак, кибератаки осуществлялись путем создания специальных веб-страниц с привлекательными «антивоенными» темами, чтобы приманить пользователей Интернета и превратить посетителей данных страниц в участников кибератак. 14 марта The Guardian также признала, что в кибервойне против России участвуют больше 300000 хакеров по всему миру [269]. Некоторые из хакерских групп представляются структурами гражданского общества, но, очевидно, имеют тесные организационные и идеологические связи с правительствами США и НАТО. При этом информационные агрессоры втягивают Китай в кибервойну против России, чтобы скрыть настоящие адреса кибератак обходным путем и свалить свою вину на Пе-

[268] «Касперский» выявил рост числа DdoS-атак на компании России в 8 раз [Электронный ресурс] // РБК. 2022. URL: https://www.rbc.ru/technology_and_media/ 01/04/2022/624699a89a79473501fa15f9 (дата обращения: 01.02.2023).

[269] 'It's the right thing to do': the 300,000 volunteer hackers coming together to fight Russia [Электронный ресурс]// The Guardian. 2022. URL: https://www.theguardian.com/world/2022/mar/15/volunteer-hackers-fight- russia (дата обращения: 01.02.2023).

кин. Так, отчёт мониторинга информационного пространства, опубликованный 11 марта 2022 года Китайским национальным центром реагирования на чрезвычайные ситуации в Интернете (CNCERT), показывает, что с конца февраля 2022 года китайский Интернет продолжает страдать от кибератак из-за рубежа. Адреса этих атак в основном указываются из США, а их главной целью является Россия[270];

- в-третьих, запустить «кампанию отключения» против России, прекратив обслуживание западных Интернет-компаний в стране и исключив Россию из международного Интернета. Так, компания Cogent отключила свою коммуникационную магистраль от российских провайдеров, Sectigo прекратила выдачу SSL-сертификатов в Россию, а Namecheaper прекратили поддерживать российские доменные имена. Вышесказанными тремя каналами Запад пытался максимально блокировать официальный голос России.

Наряду с этим, наращиваются усилия по разжиганию антироссийских и русофобских настроений в ОТКС (открытая информационно-телекоммуникационная сеть). Пользуясь антивоенными настроениями, акторы ИО фабрикуют и распространяют массивную дезинформацию, дискредитирующую Россию и руководство страны, которая направлена, с одной стороны, на оказание давления на общественное мнение международного сообщества, а с другой стороны, на коррекцию восприятия российских граждан и деморализацию армию страны, и далее превратить некоторые неустойчивые элементы в обществе России в оппозиционеров против своего правительства. В соответствии с опросом Pew Research Center, проведенном в начале апреля 2022 года, 70 % американских респондентов рассматривают Россию как врага, по сравнению с 41 % в январе[271]. Кроме того, влияние когнитивной войны, в свою очередь, подталки-

[270] Китайский Интернет подвергается иностранным кибератакам [Электронный ресурс]// Cyberspace Administration of China. 2022. URL: http://www.cac.gov.cn/2022– 03/11/c_1648615063553513.htm (дата обращения: 01.02.2023)（我国互联网遭受境外网络攻击 // 中国国家互联网信息办公室.11.03.2022. URL: http://www.cac.gov.cn/2022–03/11/c_1648615063553513.htm.

[271] Wike R., Fetterolf J., Faganet M. al. Report of Pew Research Center: Seven–in–Ten Americans Now See Russia as an Enemy [Электронный ресурс] // Pew Research Center. 2022. URL: https://www.pewresearch.org/ global/2022/04/06/ russia-nato-ukraine-march-2022-acknowledgments/ (дата обращения: 15.06.2022).

вает эскалацию санкций международных организаций и правительств к России, что приводит к иррациональному эффекту «против всего российского»

2.2. Российский опыт противодействия гибридным войнам в отношениях с США и их союзниками

Система национальной безопасности – это совокупность органов управления, сил и средств, законодательных актов, ориентированных на обеспечение безопасности и защиту жизненно важных интересов государства и общества от внешних и внутренних угроз. В Российской Федерации реализуется государственная политика по обеспечению национальной безопасности, выражающаяся в согласованных действиях всех элементов системы обеспечения национальной безопасности, достигаемых за счёт реализации комплекса мер нормативно-правового, организационного, технического характера и др.

В состав действующих основополагающих документов по обеспечению национальной безопасности входят:

1) Конституция Российской Федерации, принятая всенародным голосованием 12.12.1993 года;

2) Федеральный закон «О безопасности» от 09.11.2020 года № 390-ФЗ, заменивший одноимённый закон 1992 года;

3) «Стратегия национальной безопасности Российской Федерации» от 02.07.2021 года № 400.

Основными нормативными документами, определяющими государственную политику России по составляющим национальной безопасности, являются доктрины, в том числе: Военная доктрина Российской Федерации; Доктрина информационной безопасности Российской Федерации и т.д.

Кроме вышеуказанных базовых документов в системе нормативно-правовых актов обеспечения национальной безопасности России дополняются и

нормативные документы в конкретных сферах общественной жизни, что представлено в соответствующей тематике. В том числе, Закон об иноагентах, который является важным аспектом противления внешним вмешательствам.

Впервые понятие НКО-иноагент было введено в российское законодательство Федеральным законом от 20.07.2012 года № 121-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента» (далее – Закон об иноагентах), который был принят в ответ на масштабное протестное движение на президентских выборах 2012 года и направлен на предотвращение вмешательства иностранных государств во внутренние дела России. Стоит отметить, что данный закон не был самостоятельной мерой, а был рядом поправок к существующим законам, в частности к Федеральному закону «Об общественных объединениях» от 19 мая 1995 года № 82-ФЗ и «О некоммерческих организациях» от 12 января 1996 года № 7-ФЗ (далее – Закон об НКО). В соответствии с Законом об иноагентах статус «иностранного агента» получили НКО, которые занимаются «политической деятельностью» на территории России и финансируются иностранными государствами, международными и иностранными организациями, иностранными гражданами и лицами без гражданства. НКО-иноагенты обязаны зарегистрироваться как таковые в Министерстве юстиции России и маркировать свой статус во всех публикациях в СМИ и в Интернете, сдавать финансовую отчётность, а также раз в год проходить бухгалтерский аудит (для юрлиц)[272].

Будучи значимой составляющей Закона об иноагентах, 24 ноября 2014 года были подписаны поправки к избирательному законодательству, по которому НКО, попавшим в реестр «иностранные агенты», запрещено любое участие в российском избирательном процессе, в том числе в кампаниях референдумов и в мониторинге выборов любого уровня. Вместе с тем поправки были внесены в ряд за-

[272]Федеральный закон от 20.07. 2012 г. № 121-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента» [Электронный ресурс] // Президент России. 2012. URL: http://kremlin.ru/acts/bank/35748 (дата обращения: 01.10.2022).

конодательных актов, регулирующих финансирование политических партий[273].

Изначально Закон об иноагентах нацелен на НКО, получающие средства из-за рубежа и занимающиеся «политической деятельностью», однако со временем сфера его действия постепенно расширялась. 25 ноября 2017 года в качестве ответной меры на признание Минюстом США российского телеканала RT иноагентом российская власть приняла закон № 327-ФЗ, вводящий понятие «СМИ-иностранный агент»[274]. Впоследствии в обновлённом законе 2019 года иноагентом признается не только юридическое лицо, но и физическое лицо (физлицо – СМИ-иноагент), распространяющее информацию иностранных СМИ и финансируемое за счёт иностранного бюджета[275].

В конце 2020 года был принят закон, вносящий поправки к Закону об иноагентах, согласно которому иноагентами могут быть объявлены общественные объединения, не зарегистрированные в качестве юридических лиц, а также физические лица (в отличие от вышеуказанного реестра физлиц – СМИ-иноагентов). Нововведения в данном документе также включают следующее: исключено двоякое толкование понятия «политическая деятельность» и введено понятие посредника при получении денежных средств и иного имущества от иностранного источника – это может быть гражданин РФ или российское юрлицо. Таким образом, в стан агентов могут войти те, кто занимается политической деятельностью именно на зарубежные средства.

14 июля 2022 года президент В. В. Путин подписал закон «О контроле за деятельностью лиц, находящихся под иностранным влиянием», который объединяет и актуализирует основные положения об иноагентах, содержащиеся в раз-

---

[273]Федеральный закон от 24.11.2014 № 355-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросу финансовой отчётности политических партий, избирательных объединений, кандидатов на выборах в органы государственной власти и органы местного самоуправления»[Электронный ресурс] // Президент России. 2014 г.URL: http://www.kremlin.ru/acts/bank/39075 (дата обращения: 20.10.2022).

[274] Федеральный закон от 25 ноября 2017 года № 327-ФЗ «О внесении изменений в статьи 10.4 и 15.3 Федерального закона “Об информации, информационных технологиях и о защите информации” и статью 6 Закона Российской Федерации “О средствах массовой информации» [Электронный ресурс] // Президент России. 2017. URL: http://www.kremlin.ru/acts/bank/42487 (дата обращения: 01.10.2022).

[275] Федеральный закон от 2 декабря 2019 г. N 426– ФЗ «О внесении и изменений в Закон Российской Федерации “О средствах массовой информации» и Федеральный закон «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // Президент России. 2019. URL: http://www.kremlin.ru/acts/bank/44875 (дата обращения: 01.10.2022).

личных законах, в единый законодательный акт, в соответствии с которым формируется статус иностранного агента[276]. Новый закон расширил понятие «иностранного агента» и распространил его на всех, кто попал под «иностранное влияние». При этом «получать зарубежное финансирование для включения в реестр иноагентов больше необязательно. Иноагентами смогут признать людей, которые находятся «под иностранным влиянием» и занимаются в России политической деятельностью, сбором военно-технических сведений о стране или распространяют сообщения для неограниченного круга лиц»[277]. «Вместо нескольких существующих реестров (сейчас существуют отдельные списки НКО, СМИ, незарегистрированных общественных объединений и физлиц-иноагентов) вводится единый реестр иноагентов. Кроме этого, создаётся отдельный реестр физических лиц, аффилированных с иностранными агентами, в который включат руководителей и сотрудников организации-иноагента и экс-работников»[278]. В новом документе вводятся и «новые запреты для иноагентов, в том числе, иноагенты не смогут преподавать в школах и вузах, работать на госслужбе, организовывать любые публичные мероприятия, не будут иметь возможность получать финансирование от государства»[279] и т.д. Согласно закону, Роскомнадзор теперь имеет право блокировать сайты «иностранных агентов» по запросу Министерства юстиции без решения суда[280].

Стоит отметить, что, кроме Закона об иноагентах, другой органической составляющей в системе правового регулирования деятельности иностранных структур стал Закон о «нежелательных организациях». В контексте наблюдения ряда деструктивных влияний, оказываемых иностранными НКО на безопасность России, среди них – появление в России экстремистских организаций, финансируемых из-за рубежа, санкции США и других государств в отношении россий-

[276] Путин подписал закон об иноагентах [Электронный ресурс] // РИА НОВОСТЬ. 2022. URL: https://ria.ru/20220714/zakon-1802397942.html (дата обращения: 01.11.2022).
[277] Федеральный закон от 14.07.2022 г. № 255– ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием» [Электронный ресурс] // Президент России. 2022 г. URL: http://kremlin.ru/acts/bank/48170 (дата обращения: 01.112022).
[278] Путин подписал закон об иноагентах [Электронный ресурс] // РИА НОВОСТЬ. 2022. URL: https://ria.ru/20220714/zakon-1802397942.html (дата обращения: 01.11.2022).
[279] Там же.
[280] Там же.

ских компаний[281], в 2015 году был принят Федеральный закон об ужесточении контроля за деятельностью иностранной или международной неправительственной организации на территории Российской Федерации (далее – Закон о «нежелательных организациях»). В отношении иностранной или международной НКО, чья деятельность угрожает безопасности государства (Российской Федерации), данный закон даёт прокурорам право во внесудебном порядке объявлять эти организации «нежелательными» в России и закрывать их. При внесении в список «нежелательных организаций» счета организаций замораживаются, а дочерние отделения закрываются на территории РФ. За нарушение этого запрета иностранные НПО должны будут заплатить административный штраф до 100 тыс. руб., а их сотрудники – понести уголовное наказание (до 500 тыс. руб. штрафа, до 5 лет принудительных работ, до 8 лет лишения свободы). Среди санкций также предусматривается запрет на въезд в РФ сотрудникам «нежелательных организаций», также в отношении россиян, поддерживающих с ними связи, предусмотрены административные и уголовные меры наказания[282].

По указанным документам, очевидно, наблюдается стремление российской власти к поэтапному сокращению иностранного влияния путём ужесточения контроля над деятельностью иностранных организаций и их «агентов» на территории России. Хотя зафиксированные в этих документах меры подвергнулись критике, в частности, правозащитных организаций, безусловно, их реализация увеличила эффективность воспрепятствования деятельности иностранных структур, формирующих угрозы «цветных революций» или способствующих возникновению очагов напряжённости на межэтнической и межконфессиональной основе[283]. Собственно, с точки зрения защиты национальных интересов и обеспечения безопасности России эта инициатива разумна, ведь она совпадает с

[281] Обухова Т. В. Некоторые вопросы противодействия осуществлению деятельности на территории Российской Федерации иностранной или международной неправительственной организации, в отношении которой принято решение о признании нежелательной на территории Российской Федерации её деятельности // Вестник Санкт-Петербургского университета МВД России. – 2019. – No1(81). – С. 121–127.

[282] Федеральный закон от 23.05.2015 г. № 129– ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»[Электронный ресурс]// Президент России. 2015 г.URL: http:// kremlin.ru/acts/ bank/39720 (дата обращения: 01.10.2022).

[283] Субботина С. Дума предлагает создать список нежелательных иностранных организаций [Электронный ресурс]// Известия. 2014. URL: http://izvestia.ru/news/579968 (дата обращения: 24.10.2022).

реалиями России, где немало возможностей, позволяющих иноагентам активно воздействовать на внутриполитическую ситуацию в стране, влиять на результаты выборов, на молодёжь[284].

Таблица 2. **Правовое регулирования РФ деятельности «иноагентов»**

Название закона	Главное содержание закона	Контекст
Федеральный закон от 20.07.2012 г. №121-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента»	Впервые введено понятие «НКО-иноагент»	Протесты на президентских выборах 2012 года (Снежная революция)
Федеральный закон от 24.11.2014 г. № 355-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросу финансовой отчетности политических партий, избирательных объединений, кандидатов на выборах в органы государственной власти и органы местного самоуправления»	НКО-иноагентам запрещено участие в избирательном процессе	Политический кризис на Украине (2013-2014 годы)
Федеральный закон от 23.05.2015 г. № 129-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»	Дополняется Закон о «нежелательных организациях»	После присоединения Крыма к России ИВ Запада против России перешла на отрытый этап
Федеральный закон от 25.11.2017 г. № 327-ФЗ «О внесении изменений в статьи 10.4 и 15.3 Федерального закона «Об информации, информационных технологиях и о защите ин-	Введено понятие «СМИ-иноагент»	Минюст США включил телеканал RT в список иноагентов

[284] Замахина Т. Принят закон о контроле за деятельностью иноагентов [Электронный ресурс] // Российская газета. 2022. URL: https://rg.ru/2022/06/29/priniat-zakon-o-kontrole-za-deiatelnostiu-inoagentov.html (дата обращения: 24.10.2022).

формации» и статью 6 Закона Российской Федерации «О средствах массовой информации»		
Федеральный закон от 02.12.2019 г. № 426-ФЗ «О внесении изменений в Закон Российской Федерации «О средствах массовой информации и Федеральный закон «Об информации, информационных технологиях и о защите информации»	СМИ-иноагентом может быть признано и физлицо (введено понятие «физлицо-СМИ-иноагент»)	Протестные акции в Москве, начавшиеся в середине 2019 года; 1 мая был подписан закон о «суверенном Интернете»
Федеральный закон от 30.12.2020 г. № 481-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия угрозам национальной безопасности»	Незарегистрированные общественные объединения – «иностранные агенты»	Инцидент с «отравлением» А. Навального
Федеральный закон от 14.07.2022 г. № 255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием»	Физические лица – «иностранные агенты»; Единый реестр; Новые ограничения; определиться в понятиях, подробно описав, что означает статус иноагента, разъяснить понятие «иностранное влияние»	СВО России в Украине

В систему обеспечения национальной безопасности входит значительное количество государственных органов, принимающих участие в пределах своих полномочий в формировании и реализации политики обеспечения национальной безопасности РФ, включая Президента РФ, Совет безопасности РФ, Федеральное собрание РФ, Правительство РФ, судебные органы и т.д. В том числе, Совет безопасности России осуществляет подготовку решений Президента РФ по во-

просам обеспечения защищённости жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, проведения государственной политики по обеспечению национальной безопасности. Как уже было отмечено, национальная безопасность включает в себя как внутренние, так и внешние факторы и если внутренние можно контролировать в рамках российского законодательства, в том числе наделяя подразделения органов внутренних дел властными полномочиями в своей деятельности, то за пределами РФ указанные возможности ограничены. В этом плане Интерпол играет важную роль в пресечении преступлений и способствовании поимки преступников за пределами государства[285].

Кроме того, стоит отметить, что уникальной и важной площадкой для обмена информацией и налаживания международного сотрудничества по вопросам противодействия новым вызовам и угрозам являются регулярно проводимые по инициативе ФСБ России совещания руководителей спецслужб, органов безопасности и правоохранительных органов. Данный формат доказал свою востребованность. Это чрезвычайно полезные встречи, в ходе которых удаётся напрямую обсуждать самые актуальные вопросы по противодействию терроризму и экстремизму. До пандемии они проходили в России ежегодно; всего состоялось восемнадцать таких встреч, в них участвовали представители восьмидесяти государств[286].

Несмотря на достаточно консервативный характер структуры «силового блока»[287], в ответ на гибридные угрозы и вызовы всё равно случилась существенная трансформация правоохранительной системы страны в виде переоформления и учреждения ряда специализированных органов. Так, только в структуре МИДа были созданы три департамента по данной тематике, к тому же, образова-

---

[285] Федоренко А. В. Общая характеристика органов государственной власти по вопросам обеспечения национальной безопасности в Российской Федерации // Молодой ученый. – 2022. – № 5 (400). – С. 237–239.

[286] Снегирев В. Н. Каким оружием в борьбе с вызовами глобального характера располагает МИД РФ [Электронный ресурс] // Российская газета. 2021. URL: https://rg.ru/2021/11/18/kakim-oruzhiem-v-borbe-s- vyzovami-globalnogo-haraktera-raspolagaet-mid-rf.html (дата обращения: 20.10.2022).

[287] Чепрасов К. В. Создание национальной гвардии как ответ на гибридные вызовы безопасности России // Вопросы безопасности. – 2016. – № 2. – С. 8–19.

ние Национальной гвардии также послужило хорошим примером реагирования Россией на новые угрозы гибридного типа.

Глобальный характер нетрадиционных вызов и угроз обусловил необходимость объединения усилий всех государств мира для их решения. Для расширения международного сотрудничества по противодействию новым вызовам и угрозам, в начале 2000-х годов в МИДе РФ был учреждён Департамент по вопросам новых вызовов и угроз. Основные направления работы данного департамента включают координирование внешнего сотрудничества России по борьбе с терроризмом и трансграничной преступностью и т.п. Благодаря образованию данного департамента дипломаты России смогли наладить деловые и профессиональные контакты между спецслужбами и службами безопасности, советами национальной безопасности, национальными антитеррористическими службами, полицией и органами внутренних дел различных стран, а также между ведомствами по борьбе с незаконным оборотом наркотиков. Сотрудники данного департамента выполняют функцию по созданию атмосферы доверия и взаимопонимания, помогающей осознанию различными государствами общности интересов в борьбе с трансграничной преступностью, без чего национальным спецслужбам бывает иногда трудно перешагнуть через устоявшиеся стереотипы и пойти на сотрудничество в столь деликатных областях, поэтому их координирующая работа является одной из предпосылок для того, чтобы правоохранительные органы различных стран приступили к практическому взаимодействию на уровне профессионалов.

В декабре 2019 года президент России В. В. Путин подписал указ о создании нового департамента МИД РФ – Департамента международной информационной безопасности. Подразделение занимается международной информационной безопасностью (МИБ), в том числе борьбой с использованием информационных технологий в военно-политических, террористических и других преступных целях. До этого этой темой занималось подразделение департамента новых вызовов и угроз. Новая структура разрабатывает и реализовывает государственную политику в области международной информационной безопасности, кури-

рует деятельность международных организаций и форумов по МИБ, а также занимается разработкой и согласованием национальных мер по информационной безопасности в сфере международного сотрудничества и международных отношений[288].

За последние годы в России предпринималось уже несколько шагов по обновлению инструментов «мягкой силы». При этом Россия активно использует во внешнеполитическом инструментарии элементы «мягкой силы». В контексте усложняющихся геополитических реалий, когда Коллективный Запад своим главным противником назначил Россию и сдерживает её самыми нечистоплотными методами[289], в МИД России сформировался новый департамент, который бы взял на себя разработку стратегии и координацию действий России в области «мягкой силы»[290].

Согласно Указу президента РФ от 20 мая 2022 года[291], в структуре дипведомства создан новый департамент – по многостороннему гуманитарному сотрудничеству и культурным связям (ДМГК) и определены новые полномочия МИД России по участию в разработке и реализации государственной политики в области многостороннего гуманитарного сотрудничества и обеспечения гуманитарного влияния РФ в мире[292]. Несмотря на то, что у министерства давно есть все эти полномочия и связанные с их реализацией подразделения, например, Россотрудничество, созданное в 2000-х годах и призванное продвигать российскую «мягкую силу» за рубежом, в его структуре нет подразделения, которое бы централизовало их: они частично распределены между рядом департаментов МИДа, не являясь для них основными. А появление нового подразделения ДМГК пред-

---

[288] МИД РФ назвал задачи нового 42-го департамента [Электронный ресурс]// Интерфакс. 2019. URL: https://www.interfax.ru/russia/689780 (дата обращения: 01.11.2022).

[289] Лавров обвинил Запад в «нечистоплотности» в отношении России и КНР [Электронный ресурс]// NEWS. 31.10.2022. URL: https://news.ru/vlast/lavrov-obvinil-zapad-v-nechistoplotnosti-v-otnoshenii-rossii-i- knr/ (дата обращения: 01.11.2022).

[290] Черненко Е. Использование Россией «мягкой силы» // Газета «Коммерсантъ». 06.10.2021. – №181. – С. 6.

[291] Указ Президента Российской Федерации от 20.05.2022 № 295 «О внесении изменений в Указ Президента Российской Федерации от 11 июля 2004 г. № 865 «Вопросы Министерства иностранных дел Российской Федерации" и в Положение, утвержденное этим Указом» [Электронный ресурс] // Официальный интернет-портал правовой информации. 2022. URL: https://news.ru/world/v-mid-rf-poyavitsya-departament-myagkoj-sily/ (дата обращения: 10.11.2022).

[292] Рустамова С. В МИД РФ появится департамент «мягкой силы» [Электронный ресурс] // NEWS. 2022. URL: https://news.ru/world/v-mid-rf-poyavitsya-departament-myagkoj-sily/ (дата обращения: 01.11.2022).

ставляет собой один из важнейших шагов для реализации национальной политики по обеспечению культурного суверенитета, которое неоднократно подчеркивалось в «Стратегии-2021» как одно из приоритетных направлений обеспечения национальной безопасности.

Механизм воздействия любой диверсионной деятельности, в частности, цветных революций, показывает, что наличие в государстве национально ориентированной и лояльной главе государства политической элиты, особенно элиты «силовой», является одним из ключевых факторов успешности противодействия политической дестабилизации. Как отметила Е. Г. Пономарева, «сила законной власти в целом и национального лидера, в частности, заключается в наличии верных и преданных силовых структур, которых нельзя ни запугать, ни перекупить»[293]. Извлекая урок из украинского «Майдана», президент России в 2016 году создал новую структуру – Федеральные войска национальной гвардии РФ (Росгвардия)[294]. В структуру национальной гвардии, «кроме внутренних войск, вошли специальные отряды быстрого реагирования территориальных органов МВД, ОМОН, Центр специального назначения оперативного реагирования и авиации, а также авиационные подразделения МВД РФ»[295]. По сути, Росгвардия является полноценным «силовым» министерством, призванным обеспечивать государственную и общественную безопасность. Таким образом, Росгвардия, вместе с МВД, стала «структурой, специально «заточенной» не столько на борьбу с преступностью, сколько на противодействие гибридным вызовам. Причём показателен тот факт, что директором образованной Росгвардии был назначен В. В. Золотов – один из давних соратников В. В. Путина с начала 1990-х годов и одно из наиболее доверенных лиц из команды Президента РФ »[296].

---

[293] Пономарева Е. Г. Секреты «цветных революций» [Электронный ресурс] // Свободная мысль. 2012. № 1/2. URL: http://svom.info/entry/208-sekrety-cvetnyh-revolyucij/ (дата обращения: 15.10.2022).

[294] Указ Президента РФ от 5 апреля 2016 № 157 «Вопросы Федеральной службы войск национальной гвардии Российской Федерации» [Электронный ресурс] // Президент России. 05.04.2016. URL: http://www.kremlin.ru/acts/bank/40689 (дата обращения: 20.09.2022).

[295] Чепрасов К. В. Создание национальной гвардии как ответ на гибридные вызовы безопасности России // Вопросы безопасности. – 2016. – № 2. – С. 8–19.

[296] Чепрасов К. В. Создание национальной гвардии как ответ на гибридные вызовы безопасности России // Вопросы безопасности. – 2016. – № 2. – С. 17.

Неотъемлемой частью Стратегии национальной безопасности Российской Федерации является её государственная культурная политика. Исторический опыт показывает, что культурное самосознание, духовные, ценностные коды стали сферой жёсткой конкуренции, и на сегодняшний день уже объектом открытого информационного противоборства, хорошо срежиссированных пропагандистских атак. Попытки Запада влиять на мировоззрение целых народов мишени-страны, стремление подчинить их своей воле, навязать свою систему ценностей и понятий стали печальной реальностью, с которой сталкиваются многие страны, в том числе и Российская Федерация[297]. Россия в своём руководящем документе по национальной безопасности «Стратегия-2021» подняла культурную безопасность на небывалый уровень в системе обеспечения безопасности всей нации. Для защиты традиционных российских духовно-нравственных ценностей, культуры и исторической памяти предпринимаются комплексные меры, такие, как:

1) духовно-нравственное и патриотическое воспитание граждан;

2) защита исторической правды, сохранение преемственности и сложившегося единства российской истории;

3) развитие системы образования, обучения и воспитания.

Патриотизм – прочный фундамент будущего России[298]; это чрезвычайно важно, поскольку именно молодёжь является основным ресурсом «цветных революций», и именно она выступает объектом манипуляций и средством достижения целей со стороны «режиссёров» «цветных» государственных переворотов. От того, как сегодня воспитана молодёжь, зависит, сможет ли Россия сберечь и приумножить себя; сможет ли она быть перспективной и эффективно развивающейся страной во все более усложняющейся современной международной обстановке. С распадом СССР молодёжные патриотические организации и движения (такие, как комсомол и пионерия) прекратили своё существование, что по-

[297]Встреча с представителями общественности по вопросам патриотического воспитания молодёжи[Электронный ресурс] // Президент России. 12.09.2012 URL: http://www.kremlin.ru/events/president/news/ 16470 (дата обращения: 20.10.2022).

[298] Путин В. «Патриотизм – прочный фундамент будущего России» [Электронный ресурс] // Кубанское Казачье Войско. 2012. URL: http://www.slavakubani.ru/p-service/military-service/patriotic-education/ vladimir-putin-patriotizm-prochnyy-fundament-budushchego-rossii/ (дата обращения: 25.10.2022).

влияло на нравственные и патриотические ценности общества. Патриотическое воспитание в условиях современной России признано властью ключевым в обеспечении устойчивого развития и национальной безопасности Российской Федерации[299]. О важности патриотического воспитания неоднократно упоминали глава РФ и представители органов власти разных уровней[300]. С 2009 года в Стратегии национальной безопасности Российской Федерации стало позиционироваться создание системы патриотического воспитания граждан России как условие решения задач обеспечения национальной безопасности [301]. Фактически, ещё с 2000 годов в России предпринимаются активные меры по развитию патриотических ценностей у подрастающего поколения.

Начиная с 2001 года, когда была принята первая Государственная программа «Патриотическое воспитание граждан Российской Федерации на 2001-2005 годы», постановлениями Правительства Российской Федерации каждые пять лет вводится в действие обновлённая Государственная программа патриотического воспитания граждан[302], предусматривающая единый комплекс мероприятий, направленных на дальнейшее совершенствование системы патриотического воспитания граждан России.

Для эффективной реализации политики патриотического воспитания и укрепления руководства патриотическим воспитанием в стране были образованы различные профильные организации на этом направлении. В 2005 году, всего через три месяца после «оранжевой революции» на Украине, в России возникло молодёжное общественное политическое движение «Наши», для того чтобы противостоять проникновению идей враждебных сил в российскую молодёжь и уг-

[299]Фетисов В. В. Правовая основа патриотического воспитания граждан Российской Федерации [Электронный ресурс] // Росвоенцентр . 2014. URL: http://www.rosvoencentr-rf.ru/press-tsentr/pravovaya-baza/osnova-patrioticheskogo-vospitaniya.php (дата обращения: 25.10.2022).

[300] Путин В. В. Программа патриотического воспитания должна основываться на базовых ценностях [Электронный ресурс] // ТАСС. 2019.URL: https://tass. ru/obschestvo/7325009 (дата обращения: 20.10.2022); Стенографический отчёт о встрече В. В. Путина с представителями общественности по вопросам патриотического воспитания молодёжи // Президент России. 2012. URL: http://www.kremlin.ru/events/ president/news/16470 (дата обращения 20.10.2022).

[301] Стратегия национальной безопасности Российской Федерации до 2020 года [Электронный ресурс] // Президент России. 2009.URL: http://www.kremlin.ru/supplement/424 (дата обращения: 25.10.2022).

[302] Бахтин Ю. К. Патриотическое воспитание как основа формирования нравственно здоровой личности // Молодой учёный. – 2014. – № 10 (69). – С. 349.

розе «цветных революций» в РФ. В контексте очередной цветной революции на Украине – «Евромайдана» – в 2016 году по инициативе Министерства обороны РФ и поддержке президента Российской Федерации было создано всероссийское детско-юношеское военно-патриотическое общественное движение «Юнармия», которая стала одним из важнейших элементов государственной программы по патриотическому воспитанию молодого поколения России. Среди молодёжных организаций следует отметить и Российский союз молодёжи (РСМ): данная организация быстро развивается при поддержке правительства РФ. Сегодня одним из приоритетных направлений работы РСМ является воспитание гражданственности и патриотизма молодёжи и ориентация их на повышение чувства социальной ответственности.

К тому же, 20 октября 2012 года президент РФ В. В. Путин подписал Указ «О совершенствовании государственной политики в области патриотического воспитания», согласно которому в структуре Администрации Президента РФ было создано Управление по общественным проектам, призванное оказать всестороннее содействие работе по патриотическому воспитанию молодёжи. В задачи Управления, в частности, вошло информационно-аналитическое и организационное обеспечение основных направлений государственной политики в области патриотического воспитания, подготовка материалов и предложений по укреплению духовно-нравственных основ российского общества, совершенствованию работы по патриотическому воспитанию молодёжи, разработке и реализации общественных проектов в этой области[303].

Отечественная история представляет собой основу национальной идентичности, культурно-исторического кода страны[304]. Россия – государство со сложной историей, где вопрос внедрения единого учебника истории давно обсуждается. В связи с тем, что после распада Советского Союза учителя могли сами выбирать пособия по истории для преподавания предмета, в школах появилась широкая

[303] Образовано Управление по общественным проектам// Президент России. 2012 URL: http://www.kremlin.ru/events/president/news/16692 (дата обращения: 25.10.2022).

[304]Стенографический отчёт о встрече с разработчиками концепции нового учебно– методического комплекса по отечественной истории // Президент России. 2014 URL: http://www.kremlin.ru/events/ president/news/20071 (дата обращения: 20.10.2022).

вариативность учебников. В 2000-е годы попытки фальсификаций истории России «становятся все более жёсткими, злыми, агрессивными»[305]. На этом фоне в 2003 году «вопрос о содержании учебников по истории был поднят президентом В. В. Путиным, высказавшимся в пользу сохранения в исторической учебной литературе темы патриотизма и необходимости воспитания у учащихся чувства гордости за свою страну. С тех пор вопрос о содержании учебников по истории вошёл в повестку дня государственной политики»[306].

В июне 2007 года на Всероссийской конференции преподавателей гуманитарных и общественных наук В. В. Путин в своём выступлении особо подчеркнул необходимость повышения ответственности правительства за качество издаваемых учебников по истории[307]. Впоследствии Указом Президента Российской Федерации от 15 мая 2009 года № 549 была создана Комиссия Российской Федерации по противодействию попыткам фальсификации истории в ущерб интересам России, чтобы выявить информацию о фальсификации исторических фактов и событий, направленной на умаление международного престижа Российской Федерации и выработать рекомендации по реагированию на эти попытки и по нейтрализации их возможных негативных последствий[308]. Для развития национального исторического просвещения на основе объективного изучения, освещения и популяризации отечественной и мировой истории в 2012 году было основано «Российское историческое общество» (РИО), перед которым поставлены приоритетные задачи создания нового «переосмысленного» учебника истории для школьников. В 2013 году президент В. В. Путин выступил с инициативой создания единых учебников истории России для школы, которые будут лишены внутренних противоречий и двойных толкований, и поручил соответствующую работу РИО. В результате чего изучение российской истории в школах по учеб-

[305] РФ создаёт комиссию по противодействию попыткам фальсификации истории [Электронный ресурс]// РИА НОВОСТЬ. 2009. URL: https://ria.ru/20090519/171517015.html (дата обращения: 20.10.2022).
[306] Гузь Е. Школьный учебник по истории в условиях трансформации государственной образовательной политики рубежа xx–xxi вв. // История. – 2019. –1 (21). – С. 114–115.
[307] Выступление Президента РФ В. В. Путина на встрече с делегатами Всероссийской конференции преподавателей гуманитарных и общественных наук 21 июня 2007 г. // Преподавание истории в школе. – 2007. – № 6. – С. 4–7.
[308] Указ о Комиссии при Президенте Российской Федерации по противодействию попыткам фальсификации истории в Ущерб интересам России [Электронный ресурс]// Президент России. 2009. URL: http://www.kremlin.ru/acts/bank/29288 (дата обращения: 20.10.2022).

никам, переформатированным под новый историко-культурный стандарт, было начато в 2016/2017 учебном году и на 2022 год к использованию в школах одобрены три линейки учебников истории от трёх разных издательств.

Будущее России зависит от того, как воспитать её молодёжь[309]. Власть России обращает высшее внимание не только на формирование системы ценностей у молодёжи, нравственного фундамента, необходимого для воспитания достойных, любящих свою Родину россиян, но и обеспечение страны квалифицированными кадрами, тем более что Россия заметно опередила в этом деле страны Запада. В России формируется система подготовки специалистов по противодействию гибридным войнам, одним из признаков которой является появление профильных образовательных программ (высшего образования).

В июле 2022 года «Министерство науки и высшего образования РФ опубликовало официальное заявление о поддержке введения курсов по гибридным войнам в ВУЗах»[310], считая данную инициативу актуальной в связи со сложившейся международной ситуацией. На самом деле, ещё до появления официального заявления Минобрнауки такие программы уже были созданы в ряде российских вузов. Так, новая магистерская программа «Информационные и гибридные войны», призванная научить разрабатывать и реализовывать операции по противодействию информационной и гибридной войнам, открылась на базе факультета политологии МГУ им. Ломоносова[311].

«В России первой из таких программ стала магистерская программа «Информационные и гибридные конфликты», открытая в 2019 году в Севастопольском государственном университете (СевГУ) по инициативе профессора МГУ А. В. Манойло»[312], которая явилась прообразом программы «Информационные и

[309]Владимир Путин. «Патриотизм — прочный фундамент будущего России»[Электронный ресурс] // Кубанское Казачье Войско. 2012.URL: http://www.slavakubani.ru/p-service/military-service/patriotic-education/vladimir-putin-patriotizm-prochnyy-fundament-budushchego-rossii/ (дата обращения: 25.10.2022).

[310] В Минобрнауки поддержали введение курса по изучению гибридных войн в вузах[Электронный ресурс] // ТАСС. 2022. URL: https://tass.ru/obschestvo/15212025?utm_source-google.com&utm_medium-organic&utm_campaign-google.com&utm_referrer-google.com (дата обращения: 25.07.2022).

[311]В МГУ открылась магистерская программа «Информационные и гибридные войны» [Электронный ресурс] // ТАСС. 2022. URL: http://www.kremlin.ru/acts/bank/29288 (дата обращения: 25.07.2022).

[312]Манойло А. В. «Гибридная дипломатия»: о подготовке кадров в сфере противодействия современным информационным и гибридным войнам // Дипломатическая служба. – 2023. – № 2. – С. 130–139.

гибридные войны», созданной в 2022 году в МГУ. Программа в СевГУ предназначена для обучения профессионалов в сферах международных медиа и аналитических структур на уникальном материале Севастополя и Крыма, находящихся на переднем крае обороны против гибридных угроз в адрес России. Запуск программы «Информационные и гибридные конфликты» стал первым опытом организации подготовки специалистов по гибридным войнам на системном уровне[313]. Вместе с тем «в октябре 2019 года Московское городское отделение «Молодой гвардии Единой России» (МГЕР) запустило новый проект по обучению специалистов противодействия информационным операциям». «На курсах активистов МГЕР учили владеть вирусными технологиями, отрабатывали с ними тактику и приёмы противодействия фейкам, враждебной пропаганде, спекуляциям и популизму и после окончания обучения специалисты МГЕР стали обладать реальными званиями и навыками»[314] того, как обеспечивать политическую стабильность в сетях и чем ответить массовые протесты даже при активной раскачке оппозиционерами, вследствие чего данная программа даже назвали в социальных сетях и мессенджере «Телеграмм» «подготовкой информационного спецназа ЕР». В контексте СВО подобные программы по изучению гибридных войн умножились в вузах России. Так, в конце июня 2022 года в Российском государственном социальном университете прошёл апробацию краткий интенсивный курс «Гибридная война» и создаётся новая административная единица – Центр противодействия гибридным угрозам[315]. В этом же году в Московском техническом университете связи и информатики началась разработка программы по информационному противоборству (борьбе с дезинформацией и фейками). Таким образом, такие программы, как «Информационные и гибридные войны», создают кадровую ос-

[313]Информационные и гибридные войны: как совершить прорыв в области гуманитарных технологий и противодействовать угрозам [Электронный ресурс] // Россия Сегодня. 2019. URL: http://pressmia.ru/ pressclub/ 20190606/952378627.html (дата обращения: 25.07.2022).

[314]Манойло А. В. «Гибридная дипломатия»: о подготовке кадров в сфере противодействия современным информационным и гибридным войнам // Дипломатическая служба. – 2023. –№ 2. – С. 130–139.

[315] В Минобрнауки поддержали введение курса по изучению гибридных войн в вузах [Электронный ресурс] // ТАСС. 2022. URL: https://tass.ru/obschestvo/15212025?utm_source-google.com&utm_medium-organic&utm_campaign-google.com&utm_referrer-google.com (дата обращения: 25.07.2022).

нову для формирования в Российской Федерации общегосударственной системы противодействия гибридным угрозам.

С развитием информационно-коммуникативных технологий (ИКТ) цифровая дипломатия становится необходимым современным средством для реализации международных отношений[316]. Практика почти всех «цветных революций» показывает, что одной из основных предпосылок успешной подрывной деятельности «стал тотальный контроль над ключевыми СМИ, позволяющий донести до массового адресата любым образом искажённую «картинку реальности»[317]. Типичными примерами можно назвать операции НАТО в Ливии, когда глобальные СМИ предъявляли миру фальсифицированные фото и ролики «зверств войск Муамара Каддафи против собственного народа».

В отношении расширенного информационного воздействия противника на международное мнение и деятельности по демонизации образа России, с 2000 года Россия начала разрабатывать и осуществлять активную коммуникативную стратегию для целенаправленного формирования имиджа страны и продвигать ее, в том числе, посредством СМИ нового типа[318]. К середине 2000-х годов идея интеграции России в мировое сообщество новым образом стала одним из важнейших направлений внешнеполитической деятельности России [319]. Власть России придаёт большое значение информационной поддержке СМИ в деле защиты национальной безопасности и интересов, о чем свидетельствуют как правовое, так и организационное обеспечение в данной сфере. С вступлением в новый XXI-й век все пять опубликованных версий стратегических документов по национальной безопасности России касаются информационной безопасности и вопросов, связанных со СМИ. Так, в 2000 году была принята первая версия «Доктрины ин-

[316] Рябиченко А. Цифровая дипломатия вчера и сегодня [Электронный ресурс] // РСМД. 16.11.2018. URL: http://russiancouncil.ru/analytics-and-comments/columns/digitaldiplomacy/tsifrovaya-diplomatiya-vchera-i-segodnya/ (дата обращения: 17.12.2022).

[317] Чепрасов К. В. Создание национальной гвардии как ответ на гибридные вызовы безопасности России // Вопросы безопасности. – 2016. –№ 2. – С. 8–19.

[318] Рожков И. Я., Кисмерешкин В. Г. Имидж России. Ресурсы. Опыт. Приоритеты. – М.: РИПОЛ классик, 2008. – С. 60.

[319] Лебедева М. М. «Мягкая сила»: понятие и подходы // Вестник МГИМО. – 2017. – №3 (54). –С. 212– 223; Булгаров М. А., Тонян М. Н., Кутовая А. А. К вопросу о сущности понятия «Имидж страны» // Word Science: Problems and Innovations: сб. ст. победителей IX Междунар. науч.– практ. конф. в 2 ч. Ч. 2. – Пенза: Наука и Просвещение, 2017. – С. 110–113.

формационной безопасности Российской Федерации», согласно которой информационная безопасность впервые включена в основные аспекты национальной безопасности, при этом была поставлена задача укреплять государственные СМИ для защиты национальных интересов РФ в информационной сфере[320]. В последней редакции Стратегии национальной безопасности («Стратегия-2021») сказано, что «укрепление позиций российских средств массовой информации и массовых коммуникаций в глобальном информационном пространстве» и «расширение использования инструментов сетевой дипломатии» входили в состав приоритетных задач для достижения целей внешней политики Российской Федерации[321].

В организационном аспекте в 2000-х годах был проведён ряд масштабных реорганизаций ведущих СМИ России. В том числе, открытие телеканала Russia Today в 2005 году стал «первым шагом на пути создания российских СМИ нового типа, ориентированных на зарубежную аудиторию»[322]. Впоследствии, в 2007 году официальным печатным органом правительства «Российской газетой» был запущен медиапроект Russia Beyond the Headlines (RBTH) с целью «лучше понять Россию». На этой основе с 2013 года в России началось систематическое планирование внешней коммуникации государственных СМИ. 9 декабря 2013 года президент России В. В. Путин подписал Указ «О мерах по повышению эффективности деятельности государственных СМИ», согласно которому были ликвидированы одно из крупнейших в России средств массовой информации – «РИА Новости» и государственная радиовещательная компания «Голос России» (как самостоятельное учреждение). Вместо «РИА Новости» было образовано международное информационное агентство «Россия сегодня», а вместо «Голоса России» в октябре 2014 года было создано агентство Sputnik[323]. В 2016 году Проект RBTH перешёл в ведение компании АНО «ТВ-Новости», управляющей теле-

[320]Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // Контур Норматив. 2000.URL: https://normativ.kontur.ru/document?moduleId=1&documentId=40613 (дата обращения: 20.09.2022).
[321]Стратегии национальной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от02.07.2021 г. № 400 [Электронный ресурс] // Президент России. 2021. URL: http://www. kremlin.ru/acts/bank/47046 (дата обращения: 20.09.2022).
[322] Толоконникова А. В., Будакова Д. О. Роль телеканала RT в формировании международного имиджа России // Вестник Московского университета. Серия 10: Журналистика. – 2019. – № 5. –С. 89– 119.
[323] Указ о мерах по повышению эффективности деятельности государственных СМИ [Электронный ресурс] // Президент России. 2013. URL: http://www.kremlin.ru/events/president/news/19805 (дата обращения: 20.09.2022).

каналом RT и имеющей успешный опыт работы на международном медиарынке и в области новых медиа, чтобы эффективнее доносить до международной аудитории информацию о России. Нововведения были ведены не только в организационных структурах крупнейших внешнеорентированных СМИ, но и в формате и механизме их функционирования. Так, переориентируясь на синдикацию контента, с 2014 года планомерно сокращали количество печатных вкладок RBTH, который с 2017 года окончательно перестаёт выходить в печатной версии, перейдя на цифровые платформы и распространение материалов в зарубежных изданиях по модели синдикации[324]. Таким образом, на данный момент в России сформировалась «Большая Тройка» в сфере СМИ нового типа как мощная система проводника бренда страны за рубеж – телеканал «Russia Today», Международное информационное агентство и радио «Sputnik» и проект новых медиа «RB»[325], что стало ключевым информационным ресурсом усиления собственного информационного воздействия на зарубежную аудиторию и продвижением положительного имиджа России. В частности, сегодня телеканал RT уже стал «абсолютным лидером среди международных телеканалов» [326]. По данным SimilarWeb за октябрь 2022 года, сайт RT Arabic занимает первое место по числу посещений среди сайтов иностранных для арабского региона арабоязычных новостных телеканалов, опережая, в том числе, CNN Arabic, Sky News Arabia и Euronews Arabic. Сайт RT на испанском языке обходит по посещаемости испаноязычные версии BBC, Euronews, France 24 и teleSUR. Между тем, RT входит в пятерку самых популярных международных телеканалов в 10 странах Латинской Америки. Кроме того, на новых медиаплатформах, монополизируемых Западом, аккаунты RT показали хорошие результаты, и в 2020 году RT стал первым в мире новостным телеканалом с более чем 10 миллиардами просмотров

[324] RussiaBeyondTheHeadlines передали управляющей телеканалом RT компании [Электронный ресурс] // РБК .2017. URL: https://www.rbc.ru/technology-and-media/09/01/2017/587399da9a7947c7cccd70f3 (дата обращения: 20.09.2022).

[325] Примечание: после перезапуска в сентябре 2017 года название RBTH было сокращено на RB (RussiaBeyond).

[326] Толоконникова А. В., Будакова Д. О. Роль телеканала RT в формировании международного имиджа России // Вестник Московского университета. Серия 10: Журналистика. – 2019. – № 5. – С. 89–119.

на видеохостинге YouTube[327]. Реализуя свою деятельность и глубоко интегрируясь в международное общество, канал RT продолжает приобретать аудиторию, неравнодушную к происходящему в мире, и, тем самым, увеличивает влияние на мировой арене. В этом отношении RT France добилась больших успехов. Во время акции протестов «жёлтых жилетов» во Франции франкоязычные каналы местных и западных мейнстримных СМИ в подавляющем большинстве подчёркивали ущерб и вред, нанесённый французскому правительству данным движением. Вместе с тем выдвигаясь в места беспорядков, RT France своим беспристрастном освещением и самоотверженностью изменил стереотип западной аудитории о «пропагандистском характере» российских СМИ и завоевал одобрение французской аудитории. Многие демонстранты отказались общаться с официальными французскими СМИ, RT France стал единственным телеканалом, пользующимся доверием, как противников «желтых жилетов», так и самих активистов движения[328]. Согласно данным американской некоммерческой организации Avaaz, RT France стал абсолютным лидером по числу просмотров видео о протестах на YouTube, вдвое обогнав по показателям пять крупных французских СМИ вместе взятых[329].

В эпоху глобализации много гибридных угроз имеют общий характер и выходят далеко за рамки национальных границ, что требует коллективного подхода к противодействию этим новым вызовам от членов международного сообщества. В данном контексте установление широкого международного сотрудничества при решении указанных проблем также стало приоритетными задачами внешней политики РФ.

Среди международных организаций в Евразийском регионе Союзное государство Беларуси и России занимает особое место, являясь одной из наиболее

---

[327] См.: https://www.rt.com/about– us/

[328] «Merci, RT»: активисты «жёлтых жилетов» не доверяют французским СМИ [Электронный ресурс] // RT. 04.01.2019. URL: https://russian.rt.com/press_releases/article/589428-rt-france-zhyoltye-zhilety (дата обращения: 17.11.2022).

[329] Исследование показало рост влияния RT во Франции [Электронный ресурс] // RT. 21.06.2019. URL: https://russian. rt.com/world/news/643260-rt-france-issledovanie (дата обращения: 17.11.2022).

успешных интеграционных структур в данном регионе и «фундаментом» строящегося здания евразийской интеграции[330].

Так, 2 апреля 1996 года был подписан «Договор о создании Сообщества Беларуси и России», который запустил процесс интеграции России и Белоруссии и предусматривал, что обе стороны должны сотрудничать в таких сферах, как обеспечение национальной безопасности и борьба с преступностью. Уже через несколько лет Сообщество было преобразовано в надгосударственное образование – Союзное государство Беларуси и России (СГ).

Фундаментальным шагом стало подписание Договора о создании Союзного государства России и Беларуси в 1999 году, который включал в себя перечень приоритетных направлений сотрудничества двух стран, включая гарантию национальной безопасности участников Союза и наращивание усилий по борьбе с преступностью[331].

Военно-политическая составляющая сотрудничества РБ и РФ является одной из наиболее гармонично развивающихся. Механизм взаимодействия, отработанный министерствами обороны двух стран, является примером для других структур, прежде всего, с организационной точки зрения: наличие региональной группировки войск, которая охватывает всю территорию Беларуси и часть территории России, реализация программ по созданию инфраструктуры Региональной группировки войск, регулярное проведение совместных коллегий, оперативно-штабных и полевых учений[332].

26 декабря 2001 года была утверждена первая Военная доктрина СГ, которая является системой официально принятых единых взглядов и установок на обеспечение военной безопасности государств-участников. Однако, спустя 16 лет после ее принятия сильно изменились военно-политическая обстановка в регио-

[330]Союзное государство Белоруси и России. От сообщества к построению единого государства / под. ред. Г. А. Рапоты，Р. А. Курбанова. – М.: Юнити–Дана. – 2017. – С. 18.

[331] Договор от 8 декабря 1999 года о создании союзного государства[Электронный ресурс] // Посольство Республики Беларусь в Российской Федерации. 1999. URL: https://russia.mfa.gov.by/ru/bilate ral_relations/sojuz/legal_acts/a8c7dec6793bf47e.html (дата обращения: 15.09.2022).

[332] Тиханский А. Новая военная доктрина Союзного государства Беларуси и России: «гибридные войны» и «цветные революции» [Электронный ресурс] // Аналитический портал «Евразия. Эксперт» .2017. URL: https://eurasia.expert/novaya-voennaya-doktrina-soyuznogo-gosudarstva-belarusi-i-rossii-gibridnye-voyny-i-tsvet-nye-evolyuts/ (дата обращения: 15.09.2022).

не и на международном уровне и характер самой вооружённой борьбы: в сегодняшних конфликтах выделяется гибридный характер – помимо классических насильственных средств, типичными стали использование непрямых действий, предусматривающих ведение военных действий «чужими руками», массовое задействование негосударственных акторов, в том числе, протестующих, частных военных кампаний и даже нелигитимных организаций. В новых политических реалиях основной опасностью для СГ стали спровоцированные внешними силами вооружённые конфликты и локальные войны, способные при определённых условиях перерасти в региональную или крупномасштабную войну[333].

С учётом особенностей и новых факторов военно-политической обстановки, в 2017 году была опубликована новая Военная доктрина, которая учитывает расширение диапазона военных угроз, обращает особое внимание на «цветные революции» и «гибридные войны», и уточняет подходы по определению военных опасностей для СГ. К тому же, в новом документе впервые упомянуты угрозы, связанные с частными зарубежными военными компаниями и впервые изложена активная позиция по предотвращению военных конфликтов путём принятия превентивных мер стратегического сдерживания.

В последние годы обе страны достигли значительных результатов по сотрудничеству в противодействии угрозам различного рода и поддержании национальной безопасности и стабильности. После кризиса в Украине 2014 года к власти в стране пришли экстремистски настроенные антироссийские группировки, представляющие серьёзную угрозу национальной безопасности России и Беларуси. Обе стороны усилили совместные меры по борьбе с организованной преступностью и «тремя силами зла» (терроризмом, экстремизмом и сепаратизмом), а также – по предотвращению угрозы национальной безопасности Союза со стороны враждебных сил путём проникновения через границу[334]. Политический кризис в Беларуси 2020 года поднял российско-белорусское сотрудничество на новый этап. После президентских выборов 9 августа 2020 года в Беларуси про-

[333] Там же.

[334] Таможня и КГБ Белоруссии помогли остановить ввоз оружия в Россию с Украины [Электронный ресурс]// РИА НОВОСТЬ. 2019 г. URL: https://ria.ru/20190917/1558754175.html (дата обращения: 15.09.2022).

изошли масштабные протесты, что вызвало серьёзный политический кризис, угрожающий положению А. Г. Лукашенко в системе власти[335]. Россия оказывала А. Г. Лукашенко полную поддержку в разведывательных, экономических, военных и других аспектах, что помогло ему преодолеть кризис. Так, когда политический кризис в Беларуси зашёл в тупик, Служба внешней разведки России опубликовала официальное заявление, раскрывая, что данный кризис, по сути, является «цветной революцией», осуществляемой при поддержке Пентагона, а также поделилась информацией о нечистоплотных методах США для раскачивания ситуации в Беларуси[336]. В деле А. Навального Беларусь вовремя обнародовала перехватанную аудиозапись разговора об «отравлении» Навального, чтобы помочь России справиться с обвинениями со стороны США и Европы и с возможной «цветной революцией»[337]. В качестве другого типичного примера эффективного сотрудничества по защите национальной безопасности можно указать то, что 17 апреля 2021 года Федеральная служба безопасности Российской Федерации совместно с Комитетом государственной безопасности Республики Беларусь пресекли противоправную деятельность имеющего двойное гражданство США и Республики Беларусь Зянковича Ю. Л. и гражданина РБ Федуты А. И., планировавших осуществление военного переворота в Белоруссии по отработанному сценарию «цветных революций» с привлечением местных и украинских националистов, а также физическое устранение президента А. Г. Лукашенко[338].

Взаимодействие России и Китая в области обеспечения безопасности имеет глубокие исторические корни[339]. Обе страны активно взаимодействуют по

---

[335] Эскалация кризиса в Белоруссии: Особенности протеста и трагедия Лукашенко [Электронный ресурс] // EurAsiaDaily. 2020. URL: https://eadaily.com/ru/news/2020/08/17/eskalaciya-krizisa-v-belorussii-osobennosti-protesta-i-tragediya-lukashenko (дата обращения: 15.09.2022).

[336] О ситуации в Белоруссии [Электронный ресурс]/ / СВР РФ. 2020. URL: http://www.svr.gov.ru/smi/2020/09/o-situatsii-v-belorussii-2.htm (дата обращения: 15.09.2022)

[337] В Минске опубликовали «перехваченный разговор Варшавы и Берлина» [Электронный ресурс] // РБК. 2020. URL: https://www.rbc.ru/politics/04/09/2020/5f527c719a7947ab31a92a85 (дата обращения: 15.09.2022).

[338] ФСБ России совместно с КГБ Республики Беларусь пресечена противоправная деятельность граждан Республики Беларусь Зянковича Юрия Леонидовича и Федуты Александра Иосифовича， планировавших осуществление военного переворота в Белоруссии [Электронный ресурс]// ФСБ РФ. 2021. URL: http://www.fsb.ru/fsb/press/mes sage/single.htm%21id%3D10439220%40fsbMessage.html (дата обращения: 15.09.2022).

[339]Патрушев призвал Россию и Китай усилить готовность к взаимной поддержке [Электронный ресурс] // РИА НОВОСТЬ. 2022. URL: https://ria.ru/20220919/kitay-1817822340.html (дата обращения 20.09.2022).

проблемам безопасности и развития, как в двустороннем, так и в многостороннем форматах.

Согласно «Совместному заявлению Китайской Народной Республики и Российской Федерации о развитии всеобъемлющего стратегического сотрудничества в новую эпоху», подписанному в июне 2019 года, обе страны осуществляют широкий диапазон сотрудничества, направленного на эффективное противостояние различного рода вызовам и угрозам в сфере безопасности, в том числе самые актуальные направления включают: военно-техническое сотрудничество, совместную борьбу с терроризмом и экстремизмом, взаимодействие в киберпространстве и т.д.

Китай и Россия активно сотрудничают в области обеспечения безопасности киберпространства. Так, в 2016 году обе стороны подписали совместное заявление об усилении взаимодействия по обеспечению безопасности информационного пространства. К тому же, в рамках уже существующего механизма соответствующих консультаций уполномоченных ведомств были назначены «высокопоставленные представители двух стран, ответственные за проведение регулярных встреч и консультаций по вопросам, представляющим взаимный интерес, определение новых взаимовыгодных направлений сотрудничества в информационном пространстве, продвижение инициатив и обеспечение координации межведомственного сотрудничества»[340].

В аспекте укрепления «мягкой силы» Китай и Россия провели ряд мероприятий в сфере СМИ с целью совместного противодействия медиавойне «Коллективного Запада». Поскольку Китай и Россия бросают вызов гегемонии Запада в области глобального управления и ценностей, «лагерь Запада» во главе с США старается дискредитировать Китай и Россию с использованием гегемонии в общественном мнении и посредством распространения дезинформации. На этом фоне Китай и Россия активизируют сотрудничество в области СМИ, особенно после 2016 года, когда лидеры двух стран объявили 2016 и 2017 годы Китайско-

[340] Совместное заявление Президента Российской Федерации и Председателя Китайской Народной Республики о взаимодействии в области развития информационного пространства [Электронный ресурс] // Президент России. 2016. URL: http://www.kremlin.ru/supplement/5099 (датаобращения 15.09.2022).

российскими медиагодами. Во время протестов в Гонконге против законопроекта об экстрадиции крупнейший российский телеканал RT выпустил специальный репортаж под названием «Hong Kong unmasked», посвященный разбору настоящих причин беспорядков в Гонконге и роли Вашингтона в них[341], что привлекло широкое международное внимание и стало классическим примером совместной работы СМИ двух стран для оказания влияния на международное общественное мнение.

В качестве знаменательной части российского и китайского ответа на американское сдерживание Россия и Китай разрабатывают платежный механизм, альтернативный системе SWIFT. Таким образом, торгово-экономическое сотрудничество будет обходить доллар США и систему SWIFT, что позволит срывать американский контроль в сферах международных платежей и торговли. Совместные военные учения также стали регулярной формой сотрудничества между Россией и Китаем. Так, с 2005 года Китай и Россия проводили крупномасштабные военные учения «Мирная миссия», организованные под эгидой ШОС, которые стали одним из важных символов сотрудничества в области безопасности и антитерроризма в рамках ШОС и важным каналом для продвижения военных контактов между странами-членами ШОС. С 2012 года вне рамок ШОС проводятся ежегодные специализированные военно-морские учения «Морское взаимодействие», направленные на укрепление боеспособности России и Китая по совместному противостоянию нетрадиционным угрозам на море.

На международной арене Россия и Китай постоянно координируют усилия по поддержанию региональной и международной безопасности и содействию решению острых проблем. Так, для смягчения международной напряжённости, вызванной ядерной проблемой Корейского полуострова, обе стороны разработали российско-китайскую дорожную карту и совместно предложили проект резолюции Совета Безопасности ООН по данной проблеме, хотя данные предложе-

[341] Hong Kong unmasked: The real reasons & instigators behind anti– Beijing riots [Электронный ресурс] // RT.. 2019. URL: https://www.rt.com/news/474756-hong-kong-protests-china-us/ (дата обращения 15.07.2021).

ния столкнулись с противодействием Вашингтона[342]. Россия и Китай предприняли значительные усилия по координированию конфликтов в Афганистане, способствуя заключению соглашения и проведению консультаций заинтересованных сторон, благодаря чему в 2019 году было опубликовано совместное заявление на решение афганской проблемы[343]. В рамках ООН Россия и Китай продолжили дипломатическое сотрудничество для балансирования политики западных стран. Так, на заседаниях Совета Безопасности по ситуации на Ближнем Востоке и в Африке Россия 16 раз накладывала вето на проекты резолюций, а Китай – девять раз, причём обе стороны согласовывали свои действия. По сирийскому вопросу Москва и Пекин совместно использовали право вето восемь раз[344]. Как минимум совместные дипломатические усилия обеих сторон увеличивают цену вмешательства Западом в региональные дела.

Россия также проводит линию по борьбе с гибридными угрозами в рамках региональных и международных организаций, в частности, существующих на постсоветском пространстве организаций ОДКБ，ЕАЭС и СНГ, в рамках ШОС и ООН также существуют подходящие механизмы для совместного противодействия угрозам различного толка.

С момента основания ОДКБ и СНГ деятельность организаций в основном нацелена на реагирование на угрозы военной безопасности, однако со временем в рамках обоих организации стала активизироваться и деятельность по совместному противодействию нетрадиционным угрозам. В рамках ОДКБ действует «Центр кризисного реагирования», который может стать базой для любой антикризисной деятельности. В апреле 2020 года в Центре состоялись внеплановые консультации руководителей военно-медицинских служб министерств обороны соответствующих государств по вопросам борьбы с распространением корона-

[342] China, Russia propose lifting some U.N. sanctionson North Korea, U.S. says not the time [Электронный ресурс]// Reuters. 2019. URL: https://www.reuters.com/article/us-northkorea-usa-un/china-russia-propose-lifting- of-some-u-n-sanctions-on-north-korea-idUSKBN1YK20W (дата обращения 15.08.2022).

[343] U.S., Russia, China and Pakistan Joint Statement on Peace in Afghanistan [Электронный ресурс]// U.S. Department of State. 20 URL: https://ru.usembassy.gov/u-s-russia-china-and-pakistan-joint-statement-on-peace-in- afghanistan/ (дата обращения 15.08.2022).

[344] Лузянин С. Г. (рук.) и др.; Чжао Х. (рук.). Российско–китайский диалог: модель 2020: доклад. – М.: НП РСМД. – 2020. –С. 42–43.

вирусной инфекции нового типа[345]. В январе 2022 года по запросу президента Казахстана Касым-Жомарта Токаева в связи с массовыми протестами и наличием «террористической угрозы» ОДКБ направила в Казахстан «коллективные миротворческие силы» и помогла стабилизировать обстановку в стране и возвратить её в правовое поле[346].

В рамках СНГ с начала 2000-х годов активизировалась деятельность по совестной борьбе с незаконной миграцией и экономическим преступлениям. Так, в 2000 году «было принято Положение о создании общей базы данных незаконных мигрантов и лиц, которым въезд в СНГ запрещён. В 2004 году была одобрена Концепция сотрудничества государств-участников СНГ в противодействии незаконной миграции, после чего с 2005 года регулярно принимались соответствующие многолетние программы»[347]. В 2007 году был принят «Договор о противодействии легализации (отмыванию) преступных доходов и финансированию терроризма, чтобы укреплять сотрудничества в этой сфере»[348]. Сегодня Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ), созданная в 2004 году, ведёт довольно активную деятельность в рамках сотрудничества с Группой разработки финансовых мер по борьбе с отмыванием денег (ФАТФ)[349]. В 2012 году начал работать «Совет руководителей подразделений финансовой разведки государств-участников СНГ с широкой повесткой дня»[350].

Деятельность ЕАЭС скорее направлена на противодействие угрозам эко-

---

[345] Представители оборонных ведомств государств-членов ОДКБ обсудили вопросы профилактики и борьбы с коронавирусной инфекцией COVID–19 [Электронный ресурс] // ОДКБ. 2020. URL: https://odkb-csto.org/news/news_odkb/predstaviteli-oboronnykh-vedomstv-gosudarstv-chlenov-odkb-obsudili-voprosy-profilaktiki-i-borby-s-ko/#loaded (дата обращения 11.10.2022).

[346] Выступление Главы государства Касым– Жомарта Токаева на внеочередной сессии Совета коллективной безопасности ОДКБ [Электронный ресурс] // Официальный сайт Президента Республики Казахстан. 2022. URL: https://akorda.kz/ru/vystuplenie-glavy-gosudarstva-kasym-zhomarta-kemelevicha-na-vneocherednoy-sessii-soveta-kollektivnoy-bezopasnosti-odkb-1002245 (дата обращения 11.10.2022).

[347] Погорельская А. М. Противодействие нетрадиционным угрозам безопасности на постсоветском пространстве // Евразия. Эксперт. – 2020. – № 1– 2. – С. 47–53.

[348] Там же.

[349] Мероприятия. Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма [Электронный ресурс] // Евразийская группа. 2019. URL: https://eurasiangroup.org/ ru/events/2019 (дата обращения 11.10.2022).

[350] Погорельская А. М. Противодействие нетрадиционным угрозам безопасности на постсоветском пространстве // Евразия. Эксперт. – 2020. – № 1– 2. – С. 47–53.

номического характера, чем другим видам нетрадиционных угроз. В частности, в 2021 году было принято Соглашение об обмене информацией в сфере противодействия легализации доходов, полученных преступным путём, и финансированию терроризма при перемещении наличных денежных средств и (или) денежных инструментов через таможенную границу Евразийского экономического союза, согласно которому информационное взаимодействие может осуществляться с использованием интегрированной информационной системы Союза при условии, что указанная информационная система будет обеспечивать меры по защите предоставляемой информации. В состав органов РФ, участвующих в реализации данного Соглашения, входят Федеральная таможенная служба, Министерство внутренних дел, Следственный комитет РФ, Федеральная служба безопасности и Федеральная служба по финансовому мониторингу[351]. В сегодняшних условиях военно-политического кризиса в Европе, когда Россия изолирована от глобализации, монополизируемой Западом, для самой России участие в ЕАЭС сейчас становится скорее необходимостью, чем экспериментальным выбором. Механизмы взаимной торговли в рамках ЕАЭС позволяют решать проблемы на фоне экономической войны Запада против России[352].

Другим важным механизмом для противодействия нетрадиционным угрозам является ШОС，которая в своё время поставила на приоритетное место своей деятельности борьбу с «тремя силами зла»: экстремизмом, сепаратизмом и терроризмом. Во-первых, Россия активно подталкивает государства-члены ШОС к совместному реагированию на общие угрозы национальной безопасности. Так, на саммите в ноябре 2020 года по инициативе России лидеры ШОС приняли пакет совместных заявлений по обеспечению международной информационной безопасности, противодействию наркоугрозе и борьбе с «тремя силами зла»[353]. Во-вторых, ШОС также стала важной платформой для России при сохранении

[351] Президент подписал Указ об органах, участвующих в обмене информацией в сфере противодействия легализации доходов, полученных преступным путем [Электронный ресурс] // Федеральная служба по финансовому мониторингу. 2022. URL: https://www.fedsfm.ru/special/releases/5945 (дата обращения 20. 08. 2022).

[352] Bordachev T. Trenches and Bridges of Eurasian Integration [Электронный ресурс] // Valdai . 2022. URL: https://valdaiclub.com/a/highlights/trenches-and-bridges-of-eurasian-integration/ (дата обращения 20.10.2022).

[353] Лидеры ШОС приняли пакет документов по итогам саммита [Электронный ресурс] // РИА НОВОСТЬ. 2020. URL: https://ria.ru/20201110/shos-1583945748.html (дата обращения 11.10.2022).

стабильности в Евразийском регионе и предотвращении иностранного вмешательства. Например, после первого раунда «цветных революций» в Евразийском регионе Россия использовала ШОС в качестве платформы для противодействия вмешательству внешних сил во внутренние дела под предлогом прав человека. Соответственно, в документе ШОС отмечается, что «в области прав человека необходимо строго и последовательно уважать исторические традиции и национальные особенности народов каждой страны, отстаивать суверенное равенство всех стран»[354] и что «конкретные модели общественного развития не могут стать «экспортными»»»[355].

Кроме того, Россия также активизирует сотрудничество в области информационной безопасности в рамках ШОС. Соглашение между правительствами стран-участниц ШОС о сотрудничестве по обеспечению международной информационной безопасности является одним из первых документов подобного рода в мировой практике[356]. Начиная с 2007 года, когда в Бишкеке на заседании СГГ ШОС был утверждён План действий по обеспечению международной информационной безопасности, в последние десятки лет в рамках ШОС активно обсуждаются вопросы информационной безопасности. В 2011 году четыре государства-члена ШОС (Россия, Китай, Таджикистан, Узбекистан) представили ООН разработанный ими проект «Правила поведения в области обеспечения международной информационной безопасности» с целью стимулирования обсуждения данной проблематики на мировой арене, после которого в 2015 году обновлённая версия «Правил», разработанных в 2011 году, была внесена в качестве официального документа ООН, как «Правила поведения в области обеспечения междуна-

[354] Декларация глав государств Шанхайской организации сотрудничества[Электронный ресурс] // Центральное народное правительство КНР. 2005. URL: http://www.gov.cn/gongbao/content/2005/content_64324.htm (дата обращения 20. 08. 2022) (《上海合作组织成员国元首宣言》//中华人民共和国中央人民政府官网.2005 年 7 月 5 日).

[355] Декларацияпо случаю пятой годовщины Шанхайской организации сотрудничества государств Шанхайской организации сотрудничеств [Электронный ресурс] // Официальный сайт МИД КНР. 2006. URL: https://www.fmprc.gov.cn/chn/pds/ziliao/1179/t346575.htm (дата обращения 20.08.2022) (《上海合作组织五周年宣言》 // 中华人民共和国外交部官网.2006 年 6 月 15 日).

[356]Екатеринбургская декларация глав государств – членов Шанхайской организации сотрудничества [Электронный ресурс] // Президента России. 2009. URL: http: //archive.kremlin.ru/text/docs/2009/06/217868. shtml (дата обращения 11.10.2022).

родной информационной безопасности (МИБ)»[357]. В инициативе «Правил поведения» зафиксированы следующие важные положения об обязательствах государств: «неприменение информационно-коммуникационных технологий с целью нарушения международного мира и безопасности, невмешательство во внутренние дела других государств, неприменение силы или угрозы силой при разрешении международных споров, возникающих в цифровой сфере»[358], что, в свою очередь, заложило основу для разработки международным сообществом правил ответственного поведения в информационном пространстве.

Значительные позитивные сдвиги в сфере внешнего сотрудничества России с другими странами наблюдаются и на треке совместного противодействия киберпреступности в рамках разных переговорных площадок, в частности, ООН. Внешняя политика России основана на продвижении правил международной информационной безопасности (МИБ)[359]. Согласно «Основам государственной политики России в области международной информационной безопасности на период до 2020 года», российская позиция на этом направлении продвигается в основном под эгидой ООН. В 2018 году по российской инициативе был запущен принципиально новый переговорный формат по МИБ – Рабочая группа ООН открытого состава (РГОС), объединяющая экспертов из разных стран для обсуждения вопросов управления интернетным пространством и поиска общего понимания к ним. В июне 2021 года с подачи России была запущена «РГОС по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025», одним из приоритетов деятельности которой является «выработка универсальных правил, норм и принципов ответственного поведения государств в информационном про-

[357]Об инициативе стран– членов ШОС «Правила поведения в области обеспечения международной информационной безопасности» [Электронный ресурс] // МИД РФ. 2015. URL: https://www.mid.ru/ru/ foreign_policy/news/ 1582268/?lang=ru(дата обращения 11.10.2022).

[358]Письмо постоянных представителей Казахстана, Китая,Кыргызстана, Российской Федерации, Таджикистанаи Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря [Электронный ресурс] // МИД РФ. 2015. URL: https://www.mid.ru/upload/iblock/507/50773c33e891c2b04c4a1e795eed 9470.pdf (дата обращения 11.10.2022).

[359]Pasha Sharikov. Understanding the Russian Approach to information Security [Электронный ресурс] // The European Leadership Network (ELN). 2018. URL: https://www.europeanleadershipnetwork.org/commentary/ understanding-the-russian-approach-to-information-security/ (дата обращения: 05.11.2022).

странстве»[360]. Формируя основные концептуальные подходы и передовые идеи, Россия создала новый алгоритм переговорного процесса по вопросам МИБ. К настоящему времени Россией заключено 11 межправительственных соглашений о сотрудничестве в области МИБ, а также 6 совместных двусторонних и многосторонних заявлений глав государств в данной сфере[361].

Кроме того, Россия наращивает сотрудничество по этим вопросам с партнёрами в других международных организациях: идёт выработка плана первоочередных мероприятий по реализации профильной инициативы в СНГ – Стратегии обеспечения информационной безопасности, продолжается активная работа в рамках ОДКБ, ШОС и БРИКС, Россия активно и успешно продвигает глобальные инициативы по МИБ под эгидой ООН. На сегодняшний день разнузданная кибер- и информационная преступность уже стала глобальной проблемой, требующей согласованного ответа всего мира. Однако международное сотрудничество в данной сфере далеко от идеала и нуждается в серьёзной международно-правовой настройке. Российские инициативы по МИБ как раз реагируют на эти актуальные вызовы.

[360]Об итогах организационной сессии Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 [Электронный ресурс] // МИД РФ. 2021. URL: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1423780/ (дата обращения 13.10.2022).

[361]Глобальная киберповестка: дипломатическая победа. Интервью директора Департамента международной информационной безопасности МИД России А. В. Крутских [Электронный ресурс] // Международная жизнь. 2021.URL: https://interaffairs.ru/news/show/30374 (дата обращения: 26.10.2022).

2.3. Основные принципы организации, формы и методы противодействия информационным операциям США (как ключевому компоненту современной гибридной войны)

После событий Евромайдана на Украине в 2014 году информационные атаки США против России перешли в открытую фазу. С обострением американско-российских отношений Коллективный Запад ведёт беспрецедентно ожесточённую информационную войну против России, пользуясь абсолютным преимуществом в СМИ и Интернет-технологиях. По словам А. В. Крутских, «всего за первое полугодие 2021 года общее число кибератак на критическую инфраструктуру России и мира выросло на 150 %, в том числе 40 % атак на объекты критической инфраструктуры России совершили «классические» киберпреступники, остальные 60 % – хакеры, которые работают на проправительственные структуры других государств»[362].

14 марта 2022 года «The Guardian» также признала, что только в кибервойне против России участвуют больше 300 тыс. хакеров по всему миру[363]. Это свидетельствует, что киберпространство уже стало одним из наиболее активных фронтов гибридной войны Запада против России.

«Система обеспечения информационной безопасности, представляющая собой совокупность сил, органов, методов и средств обеспечения информационной безопасности» является частью системы обеспечения национальной безо-

[362]Аналитики заявили о росте кибератак на критическую инфраструктуру на 150% [Электронный ресурс] // РБК. 2021. URL: https://www.rbc.ru/technology_and_media/12/07/2021/60eb7ca69a7947b2f91f6_a8d (дата обращения: 20.11.2022).

[363] 'It's the right thing to do': the 300,000 volunteer hackers coming together to fight Russia [Электронный ресурс] // The Guardian. 2022. URL: https://www.theguardian.com/world/2022/mar/15/volunteer-hackers-fight-russia (дата обращения: 01.02.2023).

пасности страны. Следовательно, их правовые и организационные основы частично пересекаются.

Кроме основополагающих документов, касающихся вопросов общей национальной безопасности, существуют и руководящие документы специального характера, ориентированные на ИБ РФ и формулирующие базовые положения по ее укреплению. Так, в 2000 году был принят первый в истории современной России национальный стратегический документ по обеспечению информационной безопасности – Доктрина информационной безопасности (далее – Доктрина), согласно которому «состояние национальной безопасности Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет только возрастать»[364]. С тех пор информационную безопасность официально признали одним из важнейших элементов национальной безопасности РФ.

Согласно действующей Доктрине, утверждённой Президентом РФ 5 декабря 2016 года, под информационной безопасностью понимается «состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ, оборона и безопасность государства»[365].

Органы управления и обеспечения ИБ РФ составляют организационную основу системы обеспечения информационной безопасности Российской Федерации (СОИБ РФ). Обобщённая структура СОИБ РФ изображена на схеме 5. В состав основных специальных государственных органов, обеспечивающих информационную безопасность РФ, входят:

1) Комитет Государственной думы по безопасности;
2) Совет безопасности России (СБ России);
3) Федеральная служба по техническому и экспортному контролю (ФСТЭК

[364] Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // Российская газета. 2016.URL: https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 20.10.2022).
[365] Там же.

России);

4) Федеральная служба безопасности Российской Федерации (ФСБ России);

5) Федеральная служба охраны Российской Федерации (ФСО России);

6) Служба внешней разведки Российской Федерации (СВР России);

7) Министерство обороны Российской Федерации (Минобороны России);

8) Министерство внутренних дел Российской Федерации (МВД России);

9) Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);

10) Центральный банк Российской Федерации (Банк России).

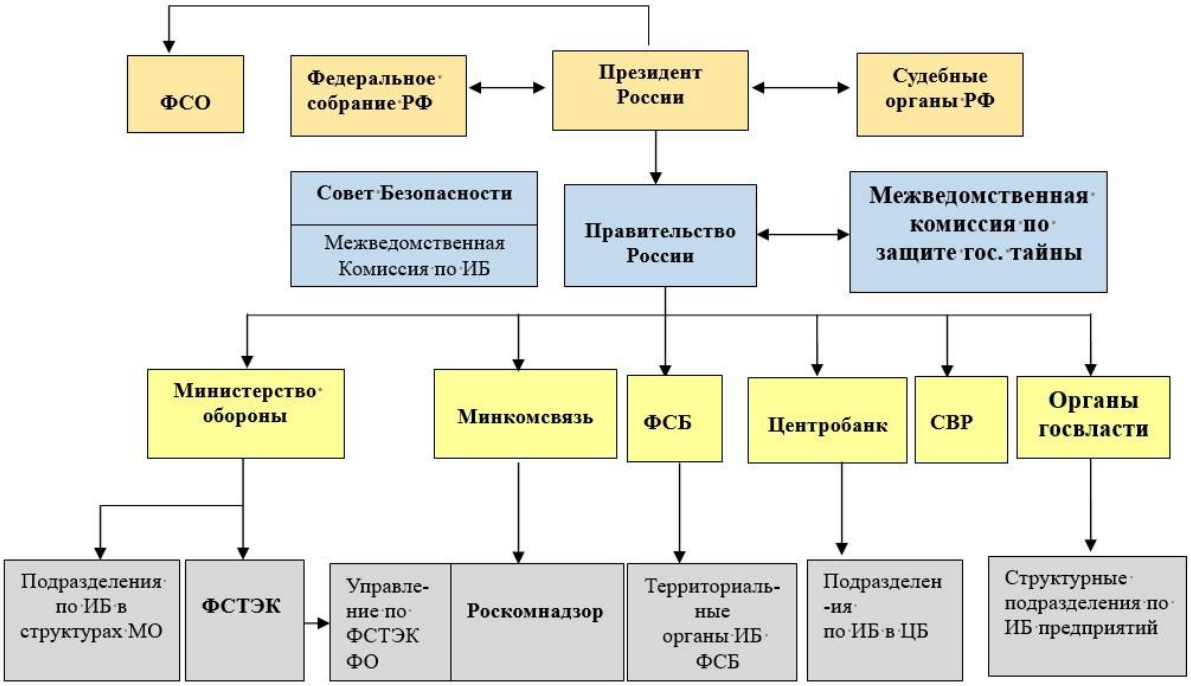


Схема 5. Структура органов обеспечения ИБ России

В этой системе Президент РФ руководит деятельностью органов и сил, ответственных за информационную безопасность. Федеральное собрание РФ создаёт необходимую нормативную базу. Координация деятельности органов, отвечающих за информационную безопасность, а также их финансовое обеспечение, находятся в компетенции Правительства РФ, в частности, Совет безопасности, Роскомнадзор, ФСБ, ФСТЭК.

Любая информационная операция выполняется неким актором – индивидом, общественной группой, государственным органом или другими субъектами,

осуществляющими информационные операции[366]. Хотя мало открытых источников подробно описывают мощь информационных операций (ИО) России, доступные данные позволяют утверждать, что в целом силы ведения ИО России состоят из трех типов акторов: государственные акторы, зависимые от государства акторы и независимые от государства акторы. Государственные акторы состоят из чиновников и сотрудников госорганов. Зависимые от государства акторы – это акторы, которые формально не принадлежат к госорганам, но регулярно действуют по их указанию. Чаще всего к данному типу акторов относятся контролируемые государством СМИ (такие, как RT и Sputnik), госкорпорации (такие, как Газпром) и другие учреждения. Сюда также входят различные группы и отдельные лица, которые, судя по всему, работают на фрилансе, но действуют также по государственным указаниям[367]. Независимые от государства акторы – это различные внештатные сотрудники, такие, как блогеры, хакеры, активисты и бизнесмены, которые, как правило, совершают действия в сфере ИО без указания государства, но могут координировать действия с государством или зависимыми с ним акторами на специальной основе.

Имеющиеся в открытом доступе данные свидетельствуют о том, что Министерство обороны (в частности, ГРУ[368]) после российско-грузинской войны 2008 года стало ключевым государственным актором в области ИПО[369]. Российские военные исторически были ключевым субъектом в наступательных информационно-психологических операциях: незадолго до Второй мировой войны в Красной Армии было создано управление «специальной пропаганды», которому поручались весьма деликатные задания под общим названием «политическая ра-

---

[366] Устинова М. Новые термины на русском языке. Глоссарий конфликтологических терминов. – М.: Каллиграф, 2008. – 96 с.

[367] Туровский Д. Пришло наше время послужить России [Электронный ресурс] // Meduza. 2018. URL: https://meduza.io/feature/2018/08/07/prishlo-nashe-vremya-posluzhit-rossii (дата обращения: 10.01.2023); Пришло наше время послужить России: как война в Грузии вдохновила спецслужбы на вербовку хакеров– патриотов [Электронный ресурс] // Вестник К. 2018. URL: https://vestnikk.com/society/crucial/32201- prishlo-nashe-vremya-posluzhit-rossii-kak-voyna-v-gruzii-vdohnovila-specsluzhby-naverbovku-hakerov-patriotov.html (дата обращения: 10.01.2023).

[368] ГРУ было реорганизовано в 2010 г. и сейчас называется «ГУ ГШ».

[369] Russia Military Power: Building a Military to Support Great Power Aspirations. – Defense Intelligence Agency (Washington, D.C.). – 2017. – P. 74.

бота»[370]. В 1991 году эти подразделения спецпропаганды были переподчинены ГРУ под эгидой Центра иностранной военной информации и связи[371]. Считается, что подразделение ГУ ГШ 54777 (72-й центр ГУ ГШ), 26165 (85-й центр ГУ ГШ) и в/ч 74455 являются главными центрами по организации и ведению наступательных информационно-психологических операций[372]. Среди негосударственных акторов Агентство Интернет-исследований (Internet Research Agency, далее – IRA) является самой известной организацией, которая может укомплектовать российские ряды троллей[373]. Кроме того, важно, что российское правительство имеет способность пополнять свой боевой отряд по ведению ИО обширной сетью негосударственных акторов. Впервые о необходимости создания в российской армии киберкомандования в марте 2012 года заявил тогдашний Вице-премьер РФ Д. Г. Рогозин, который потом объявил о планах по созданию кибервойск[374]с как техническими, так и психологическими боевыми задачами, и способностью заниматься всем – от сетевой безопасности до информационных операций[375]. В 2013 году министр обороны С. К. Шойгу открыл «большую охоту» на программистов для российских Вооруженных сил, ранее приказав Главному оперативному управлению (ГОУ) Генштаба создать киберкоманду «как можно скорее». Вероятно, в период с 2014 по 2017 годы в России уже были созданы такие силы, назван-

[370]Особый фронт [Электронный ресурс] // Аргументы времени. 01.10.2018. URL: https://svgbdvr.ru/voina/osobyi–front (дата обращения: 10.01.2023).

[371] Пушкарев Н. ГРУ: вымысли и реальность. – М: Яуза: Эксмо, 2004.– С. 31– 35.

[372] Troianovski A., Ellen N. How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's duels with the West [Электронный ресурс] // Washington Post. 2018. URL: https://www.washingtonpost. com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/ 2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html (датаобращения: 10.01.2023); U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations [Электронный ресурс] // U.S. Department of Justice, Office of Public Affairs . 2018. URL: https://www.justice.gov/ opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and (дата обращения: 20.01.2023).

[373] Soldatov Andrei, Irina Borogan. The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries. – New York: Public Affairs, 2015. – 384 p.

[374] Кибервойска появятся в армии до конца года [Электронный ресурс] // Москва24. 2013 URL: https://www.m24.ru/ articles/Minoborony/05072013/20906 (дата обращения: 15.12.2022); Ма Цзяньгуан, Ся Пэн. Россия создает кибервойска [Электронный ресурс] // Военное обозрение. 2013. URL: https://topwar.ru/31668-rossiya-sozdaet-kibervoyska-stdailycom-kitay.html (дата обращения: 15.12.2022).

[375] В Вооружённых силах создают войска информационных операций [Электронный ресурс] // Независимое военное обозрение. 2014. URL: https://nvo.ng.ru/concepts/2014– 05– 16/2_red.html (дата обращения: 15.12.2022); Минобороны России прорабатывает вариант создания гуманитарных научных рот [Электронный ресурс] // ТАСС. 2013. URL: https://nauka.tass.ru/nauka/631973 (дата обращения: 15.12.2022).

ные Войсками информационных операций[376]. Как эти силы вписываются в существующую военную структуру, остается неясным. Войска информационных операций участвовали в масштабных военных играх в 2016 году, где В. В. Герасимов отметил, что ГОУ Генштаба будет функционировать как координирующий орган информационного противоборства[377]. По словам начальника Генштаба, подчиненные ему Центры информационного противоборства (ЦИП), созданные в каждом из четырех основных военных округов России, дополненные войсками информационных операций, подразделениями радиоэлектронной борьбы и специалистами по информационной безопасности, будут вести информационное противоборство в составе российских вооруженных сил, которое имеет такое же значение, как и подразделения, занимающиеся планированием кинетических ударов по потенциальному противнику[378].

Многие из российских ИО осуществляются различными акторами, часто на разовой основе (схема 6). Большинство осуществлённых ИО исходит от инициативы отдельных лиц, руководствующихся скорее своим пониманием желаний Кремля, чем каким-либо детальным генеральным планом[379]. То есть, проведение информационных операций чаще всего слабо организованно и делегировано широкому кругу субъектов, некоторые из которых тесно связаны командной цепочкой, другие связаны с государственными органами гораздо более непрочно[380].

---

[376] В Минобороны РФ создали войска информационных операций [Электронный ресурс] // Интерфакс. 2017. URL: https://www.interfax.ru/russia/551054 (дата обращения: 15.12.2022).; Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций [Электронный ресурс] // ТАСС. 2014. URL: https://tass.ru/politika/1179830 (дата обращения: 15.12.2022).

[377] Russia Military Power: Building a Military to Support Great Power Aspirations. Defense Intelligence Agency (Washington, D. C.). 2017. p. 38; Информационное противоборство отработали на «Кавказе–2016» [Электронный ресурс] // Известия. 2016. URL: https://iz.ru/news/632393 (дата обращения: 15.12.2022).

[378] На учениях «Кавказ– 2016» впервые отработали «информационное противоборство» [Электронный ресурс] // РИА НОВОСТИ. 2016. URL: https://ria.ru/20160914/1476902330.html (дата обращения: 15.12.2022).

[379] Galeotti M. Controlling Chaos: How Russia Manages its Political War in Europe [Электронный ресурс] // London, United Kingdom: European Council on Foreign Relations. 2017. URL: https://ecfr.eu/publication/ controlling_chaos_how_russia_manages_its_political_war_in_europe/ (дата обращения: 15.12.2022).

[380] Подробнее см.: Constanze Stelzenmüller. The Impact of Russian Interference on Germany's 2017 Elections [Электронный ресурс]// Brookings Institute. 2017 URL: https://www.brookings.edu/testimonies/ the-impact-of-russian-interference-on-germanys-2017-elections/ (дата обращения: 01.02.2022); Naja Bentzen. Foreign Influence Operations in the EU [Электронный ресурс] // European Parliamentary Research Service. 2018. URL: https://www.europarl. europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf (дата обращения 28.07.2022).

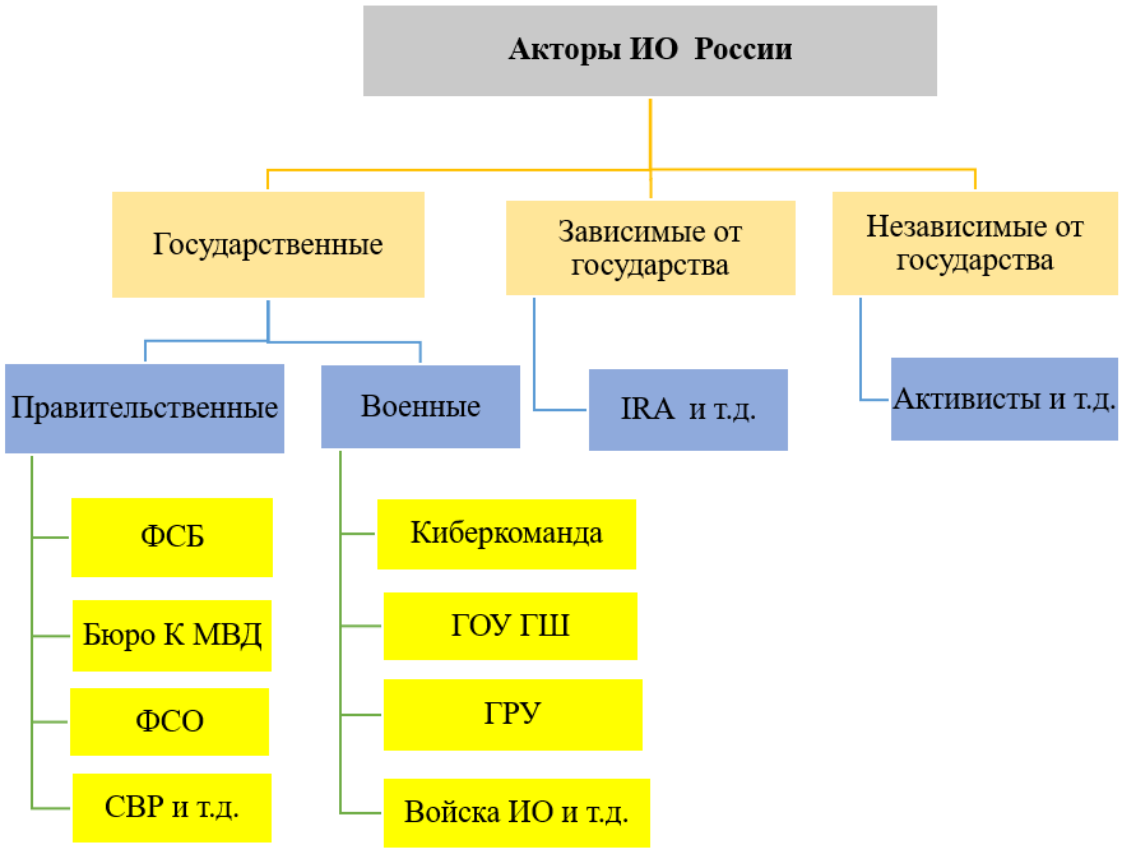


Схема 6. Типология акторов ИО России

Хотя озабоченность информационной войной, наряду с другими нетрадиционными инструментами международной борьбы, такими, как гибридным войнам, появилась сравнительно недавно, подход России к информационному противоборству уходит корнями в её историю, начиная с XV века, через институционализацию пропаганды в советское время до современных форм информационного противостояния.

Существуют несколько терминов в российской и зарубежной литературе для описания деятельности конфронтационных сторон в информационной сфере – информационные операции, информационная война, информационные кампании, психологическая война и т.д. Несмотря на то, что все эти термины слабо соответствуют российскому пониманию информационного противоборства, которое охватывает все «враждебные действия с использованием информации в качестве инструмента», с учётом того, что различие между этими терминами имеет мало практического значения для подходов к их исследованиям, чтобы не ввязы-

ваться в ненужные терминологические дебаты, в данной диссертации эти термины используются как взаимозаменяемые (синонимы).

Российский подход к «информационному противоборству» в общих чертах аналогичен западным идеям Information operation или Information warfare, но с явными отличиями, которые проявляются, как минимум, в следующих аспектах: во-первых, в российском понимании размыта грань между кибернетическими, психологическими и информационными войнами, и широкий диапазон действий, направленных на кражу, подбрасывание, перехват, манипулирование, искажение или уничтожение информации и т.д., рассматривается как инструменты информационного противостояния[381]. Во-вторых, в российских терминах информационное противостояние объединяет два аспекта: «информационно-техническую (блокирование работы технических средств системы государственного и военного управления противника) и информационно-психологическую (информационно-психологическое воздействие – ИПВ – на его руководителей, личный состав вооружённых сил и население) составляющую»[382]. В-третьих, информационные операции «не ограничиваются военным временем – они проводятся и в мирное время, задолго до перехода к боевым действиям, и постепенно активизируются по мере эскалации конфликта, чтобы создать благоприятные условия для стороны – инициатора информационного воздействия, а в ходе конфликта полностью парализовать функционирование инфраструктуры управления противника»[383]. При этом участники ИО не ограничиваются действиями между «враждебными сторонами», они «могут быть направлены на союзников и нейтральные государства с целью вовлечения их в ИВ на своей стороне»[384].

Таким образом, ИО в России стали широкоохватываюшим понятием, включающим широкий диапазон деятельности с преднамеренной, систематиче-

[381] Giles K. Handbook of Russian Information Warfare. – Rome, Italy: NATO Defense College, 2016. – P. 4; Selhorst T. Russia's Perception Warfare: The Development of Gerasimov's Doctrine in Estonia and Georgia and Its Application in Ukraine // Militaire Spectator. – 2016. – Vol. 185, No. 4. – P. 151.

[382] Колесов П. Информационная война Грузии против Южной Осетии и Абхазии// Зарубежное военное обозрение.– 2008.– No. 10. – С. 18– 21.

[383] Бартош А. А. Адаптивные стратегии информационной войны (часть 1) // Вестник Академии военных наук. – 2016. – № 2(55). – С. 85– 93.

[384] Колесов П. Информационная война Грузии против Южной Осетии и Абхазии // Зарубежное военное обозрение. – 2008. – No. 10. – С. 18– 21.

ской попыткой сформировать восприятие, манипулировать когнациями и направлять поведение для достижения реакции, которая способствует желаемым намерениям их инициатора.

Следовательно, понятие «информационной безопасности» в российском обществе также гораздо шире, чем на Западе. В западном понимании информационная безопасность в целом относится к конфиденциальности, целостности и доступности систем, сетей и данных, то есть подчёркивается аспект информационной технологии информационной безопасности. Вместо этого обсуждение российским правительством информационной безопасности широко охватывает интересы режима в информационной сфере, включая безопасность режима и контроль государства над информационными потоками и общественным мнением. Хотя в западном понимании существует и нетехнологический аспект информационной безопасности, например, она может пониматься как защита государственных секретов, включая «меры по пресечению иностранного шпионажа» внутри страны и «меры по защите военных и дипломатических сообщений от иностранного перехвата и эксплуатации»[385], трактовка же данного понятия в России еще шире и охватывает такие аспекты, как репортажи в прессе и общественное восприятие.

Разные подходы по данным вопросам обусловили разницу в проведении политики по обеспечению информационной безопасности: Западные страны делают ставку на поддержание свободного обмена информации через безопасную техническую инфраструктуру, обеспечивающуюся правительством; российский же подход основан на ответственности правительства не только за обеспечение безопасности инфраструктуры, но и за обеспечение безопасности самой информации, что отражает традиционное понимание Россией национального суверенитета. В то же время российское правительство понимает информационный суверенитет как нераспространение «вредоносной» иностранной информации среди российских граждан и обмен соответствующей информацией о России с ино-

[385] Подробнее, см.: Michael Herman. Intelligence Power in Peace and War. – Cambridge: Cambridge University Press,1996.– P. 165.

странными партнёрами[386]. Соответственно, Россия выступает за усиленный государственный контроль над информацией, что подвергается острой критике Запада, который воспринимает такой подход как угрозу политической стабильности демократических стран.

В информационном противоборстве с США и их союзниками Россия придерживается следующего основного принципа: информационная безопасность неотделима от национальной безопасности, для обеспечения которой необходимо комбинировать оборонительные и наступательные подходы и осуществлять достойные контратаки асимметричными средствами.

Российские методы по противодействию ИО базируются на её восприятии данного феномена. С одной стороны, российские военные и политические эксперты рассматривали развитие Интернета и, в частности, социальных сетей, как угрозу безопасности страны; с другой стороны, они также приняли их как потенциально высокоэффективное наступательное оружие с низкими затратами, которое может помочь России устранить дисбаланс в военных возможностях между ней и США и их союзниками.

Российское руководство считает, что его национальная безопасность находится под угрозой информационной агрессии со стороны Запада. По мнению Москвы, с 1990-х годов Россия и Запад все больше втягивались в «цивилизационную борьбу», что поставило России актуальную задачу защищать своё мировоззрение и культуру от агрессивного вторжения западного либерализма[387]. В частности, информационная агрессия против России рассматривалась как неотъемлемая часть этой борьбы[388].

Этому восприятию способствовал ряд политических реалий. Прежде всего, часть этой новой реальности заключалась в том, что развитие Интернета неиз-

---

[386] Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // Российская газета. 2016. URL:https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 20.10.2022).

[387] Robinson L., Helmus T.C., Cohen R.C. et al. Modern Political Warfare: Current Practices and Possible Responses [Электронный ресурс] // RAND Corporation. 2018. URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1772/RAND_RR1772.pdf (дата обращения: 05.01.2023).

[388] Подробнее. См.: Стрельцов А. А. Основные задачи государственной политики в области информационного противоборство // Военная мысль. – 2011. – No. 5.– С.18– 25; Модестов С. А. США готовы к информационной войне с Россией // Независимое военное обозрение. – 1997. – No. 25.

бежно даёт Западу огромное преимущество над Россией. Как заявил президент В. В. Путин, Интернет был «проектом ЦРУ», и Россия должна была быть защищена от него[389].

Ряд политических событий ещё больше подогрел это восприятие. Первыми среди них были цветные революции в бывших советских республиках в начале 2000-х годов, которые рассматриваются Москвой как инструмент западной (прежде всего, американской) политики с целью свергнуть законные правительства, которые проводили политику, противоречащую интересам США[390]. При этом считается, что Соединенные Штаты в немалой степени организовали эти «восстания» с помощью коммуникационных технологий – в частности, Интернета и социальных сетей. Так, многие российские авторы указывали на способность Запада влиять и организовывать массовые движения через Интернет во время цветных революций на Украине и в Грузии[391].

Восприятие российскими военными несдерживаемого развития Интернета как уязвимого места национальной безопасности продолжало развиваться на фоне растущей напряжённости в отношениях с Западом. В частности, движение «арабской весны» и протесты в Москве в 2011-2012 годах оказывают исключительно глубокое влияние для укрепления взглядов на социальные сеть как на серьёзную угрозу национальной безопасности[392]. В московских протестах 2011-2012 годов, представляющих собой самый серьёзный вызов российскому режиму с момента вступления В. В. Путина на пост президента, российские протестую-

---

[389] Soldatov A., Borogan I. The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries.– NewYork: Public Affairs, 2015. – P. 238; Отец Всемирной паутины поспорил с Путиным об интернете как проекте ЦРУ [Электронный ресурс] // РБК. 2014. URL: https://www.rbc.ru/technology-and-media/11/12/2014/5489 a91d2ae5960852e224e9 (дата обращения: 05.01.2023).

[390] Charap S., Colton T.J. Everyone Loses: The Ukraine Crisis and the Ruinous Contest for Post–Soviet Eurasia. – New York: Routledge for the Intern. Inst. for Strategic Studies, 2017. – 211 p.

[391] Например, см. Кузьмин В. Роль США в осуществлении «цветных революций» в зарубежных странах [Электронный ресурс] // Зарубежное военное обозрение. 2008. URL: https://militaryarticle.ru/ zarubezhnoe-voennoe-obozrenie/2008-zvo/7658-rol-ssha-v-osushhestvlenii-cvetnyh-revoljucij-v (дата обращения: 05.01.2023); Тимофеев В. Про информшаблону [Электронный ресурс] // Красная звезда. 2005. URL: http://old.redstar.ru/2005/01/1901/303.html (дата обращения: 05.01.2023).

[392] Несмеянов В. Эта тихая смертельная война [Электронный ресурс] // Флаг Родины. 2017. URL: https://sc.mil.ru/files/morf/military/archive/%5B«Flag_Rodini»%5D%5B2017-03-10%5D.pdf (дата обращения: 15.01.2023); Сивков К. «Мудрость» Януковича [Электронный ресурс] // Военное обозрение. 2014. URL: https://topwar.ru/54802-mudrost-yanukovicha.html (дата обращения: 05.01.2023); Alissa de Carbonnel. Insight: social media Makes Anti–Putin Protests 'Snowball,' [Электронный ресурс] // Reuters. 2011. URL: https://www.reuters.com/article/us-russia-protests-socialmedia-idUSTRE7B60R720111207 (дата обращения: 15.01.2023).

щие позаимствовали из социальных сетей репертуар протестующих в США[393]. Как и сам В. В. Путин, российские военные эксперты часто приписывают эти события преднамеренному влиянию Запада, действовавшего через спецслужбы, разведку и подразделения PSYOPS Вооруженных сил США[394]. Считается, что за «арабской весной» стоят те же силы. Таким образом, некоторые российские политологи и военные эксперты пришли к выводу, что национальная система СМИ заменяется международной, которая все больше опирается на Интернет-ресурсы и соцсети, с управлением которых могут провести быструю смену власти внутри стран противника[395]. Угрозы соцмедиа могут быть даже более разрушительными, чем «танковые прорывы» прошлых дней[396].

Размышляя об этом опыте с начала 2000-х годов, в 2013 году начальник Генерального штаба ВС РФ В. В. Герасимов, выступая с известной речью, впервые выразил официальную позицию России к угрозам, созданным Западом с использованием технологий информационных сетей для воздействия на государственные структуры и население страны-мишени[397]. Впоследствии в 2016 году В. В. Герасимов более конкретно раскрыл механизм действия гибридных войн США в отношении их противников, в которых, по мнению Герасимова, Интернет используются как оружие, «цветные революции» – как основное средство гибридных войн, что может привести к «внешне ненасильственной» смене правительства в стране противника. Суть любой «цветной революции» заключается в смене режима, организованной извне. В ее основе лежат информационные технологии,

---

[393]Например, см.: Elder M. Russian Protests: Thousands March in Support of Occupy Abay Camp [Электронный ресурс] // The Guardian. 2012. URL: https://www.theguardian.com/world/2012/may/13/russian-protests-march-occupy-abay (дата обращения: 15. 01.2023).

[394] Кудряшов А. Использование за рубежом сети Интернет в интересах ведения информационных войн [Электронный ресурс] // Зарубежное военное обозрение. 2011. URL: https://militaryarticle.ru/zarubezhnoe– voennoe-obozrenie/2011-zvo/8028-ispolzovanie-za-rubezhom-seti-internet-v-interesah (дата обращения: 05.01.2023); Микрюков В. Победа в войне должна быть достигнута еще до первого выстрела [Электронный ресурс] // Независимое военное обозрение. 2016. URL: https://nvo.ng.ru/concepts/2016-01-15/10infowar.html (дата обращения: 05.01.2023); Несмеянов В. Сумеем ли защитить великую победу? [Электронный ресурс] // Флаг Родины. 2013. URL: https://sc.mil.ru/files/morf/military/archive/%5B «Флаг%20Родины»%5D%5 B2013-06-04%5D. pdf (дата обращения: 05.01.2023).

[395] Белозеров В., Копылова Д. СМИ: Информационное противоборство [Электронный ресурс] // Ориентир. 2014. URL: http://milportal.ru/smi-informatsionnoe-protivoborstvo/ (дата обращения: 05.01.2023).

[396] Новик А. Оружие будущего по–британски [Электронный ресурс] // Страж Балтики. 2019. URL: https://ric.mil.ru/upload/site173/3smeFty8fn.pdf (дата обращения: 20.01.2023).

[397] Герасимов В. Ценность науки в предвидении [Электронный ресурс] // Военно–промышленный курьер. 2013. URL:https://vpk.name/news/85159cennost-nauki-v-predvidenii.html (дата обращения: 20.01.2023).

манипулирующие протестным потенциалом населения, и другие невоенные средства. Важной частью данного механизма является массовое, целенаправленное воздействие на сознание граждан (объектов агрессии) посредством глобальной сети Интернет[398]. Данные высказывания начальника Генштаба России ошибочно распространяют на Западе для описания «новой теории России по ведению современной войны» под названием «Доктрина Герасимова»[399].

Согласно российской военной литературе, Россия смутно представляла себе наступательные возможности развивающихся коммуникационных технологий в 1990-х годах, но начала воспринимать наступательный потенциал социальных сетей только в начале 2000-х годов[400]. Например, в учебнике ГРУ 1999 года по психологической войне неоднократно отмечается роль телевидения в поддержке военных операций, а Интернет упоминается лишь дважды. В тоже время существует преувеличенное представление о потенциале технологии «вируса», влияющей на психологическое состояние пользователей сетей[401]. Вплоть до 2000-х годов, благодаря собственной практике России и опыту других стран, российские эксперты были осведомлены о том, что новые коммуникационные технологии, в частности, Интернет и соцсети, могут быть хорошим инструментом против превосходящего противника, благодаря использованию асимметричных возможностей[402].

Восприятие Россией того, что она не может напрямую конкурировать с Западом в обычных вооружённых силах, повысило значение информационного противостояния для российских военных и чиновников администрации президента. По словам В. В. Путина, российские ответы на развитие вооружённых сил других стран «должны быть основаны на интеллектуальном превосходстве, они

---

[398] Герасимов В. По опыту Сирии [Электронный ресурс] // Военно–промышленный курьер. 2016. URL: https://vpk.name/news/150974_po_opytu_sirii.html (дата обращения: 20.01.2023).
[399] Galeotti M. I'm Sorry for Creating the 'Gerasimov Doctrine [Электронный ресурс] // Foreign Policy . 2018. URL: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ (дата обращения: 20.01.2023).
[400] Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт). – Минск: Харвест,1999. – С. 9.
[401] Там же; Kovalev A., Bodner M. The Secrets of Russia's Propaganda War, Revealed [Электронный ресурс] // Moscow Times. 2017. URL: https://www.themoscowtimes.com/2017/03/01/welcome-to-russian-psychological-warfare-operations-101-a57301 (дата обращения: 20.01.2023).
[402] Модестов С., Сокут С. Байты вместо пуль // Независимое военное обозрение. – 1999. – No. 13.

будут асимметричными и менее затратными» [403]. Вместе с тем в российских военных кругах распространено мнение о том, что потенциал информационного оружия настолько велик, что можно достигать победы в операциях и конфликтах исключительно с его применением, без применения традиционных средств вооружённой борьбы.[404] То есть, Москва увидела перспективу того, чтобы информационная война стала дублером вооружённых сил, а не просто их сервисом. Следовательно, к 2010 году в Военной доктрине России была утверждена растущая роль информационного противостояния «для достижения политических целей без применения традиционных вооружённых сил»[405]. Как отметил российский учёный А. М. Евдокимов, согласно историческому опыту, только с оборонительным подходом, без решительных и наступательных операций, победа в информационном противоборстве не достигается[406]. Таким образом, ведение Западом информационной войны сыграло значительную роль в том, чтобы заставить Россию выработать собственный наступательный арсенал информационной конфронтации.

Эволюция российских представлений о ИКТ как инструменте международного противоборства и защиты внутренней стабильности завершилась в ходе украинского конфликта 2014 года, когда Россия тщательно добавила эти технологии в свой арсенал ИВ. С тех пор российские военно-политические акторы стали более откровенно говорить об активном использовании социальных сетей в ИО для нанесения ответных ударов по противнику. Так, военный аналитик из известного российского военного журнала предупредил, что американские информационные войска распространяют пропаганду в социальных сетях, в то время

---

[403] Путин В. В. Солдат есть звание высокое и почётное. Выступление с ежегодным Посланием Федеральному Собранию [Электронный ресурс] // Красная звезда. 2006. URL: http://old.redstar.ru/ 2006/05/11 05/1 01.html (дата обращения: 06.02.2023).

[404] Буренок В. М., Ивлев А. А., Корчак В. Ю. Развитие военных технологий XXI века: проблемы планирование, реализация. – М.: Тверь: КУПОЛ, 2009. – С. 224; Чекинов С. Г., Богданов С. А. // Прогнозирование характера и содержания войн будущего: проблемы и суждения // Военная мысль. 2015.– No. 15.– С. 44–45.

[405] Указ Президента Российской Федерации от 05.02.2010 г. №146 О Военной доктрине Российской Федерации [Электронный ресурс]/ / Президент России. 2010. URL: http://www.kremlin.ru/acts/bank/30593 (дата обращения: 01.10.2022).

[406] Евдокимов А. М. Об активных информационных мероприятиях на южном стратегическом направлении// Защита и безопасность. – 2010. – № 4(55). – С. 27.

как российская армия только учится владеть этим оружием[407]. Другой аналитик отметил преимущества в использовании ИКТ для достижения асимметричных военных целей против противников, превосходящих в вооружённых силах[408].

Эволюция российской военной мысли о ИО как об угрозе и оружии, переплетается с широкой озабоченностью последствиями развития ИКТ для национальной безопасности и внутренней стабильности[409]. Собственный опыт российских военных в Чечне, Грузии и Украине в сочетание с международным уроком в ряде показательных событий, таких, как «арабская весна», «Панамское досье», сформировал российское стратегическое мышление о современном информационном противостоянии с использованием ИКТ. Более того, информационные атаки США, как угрожают России, так и фактически косвенно содействуют развитию собственного информационного арсенала России. Так, постоянная фиксация на возможности того, что НАТО и США могут использовать платформу социальных сетей для разжигания народных волнений против России, породила российский инстинкт самозащиты путем разработки собственных контрмер и включения социальных сетей в свой арсенал информационного противостояния.

Прежде всего, в целом ответные меры России на ИО можно разделить на два вида – оборонительные и наступательные.

Оборонительные контрмеры включают в себя меры по уничтожению или нейтрализации эффекта злонамеренных ИО противника с целью защиты безопасности собственной инфраструктуры киберпространства и информационного суверенитета от посягательств (российское понимание информационной безопасности и информационного суверенитета было подробно проанализированы в

---

[407] Мухин В. Ставка на информационный спецназ [Электронный ресурс]// Независимое военное обозрение. 2015. URL: https://nvo.ng.ru/realty/2015-04-17/1specnaz.html (дата обращения: 05.12.2022).

[408] Антонович П. Ключевые аспекты информационной войны [Электронный ресурс] // Армейский сборник. 2014. URL:https://sc.mil.ru/files/morf/military/archive/1012014.pdf (дата обращения: 05.12.2022).

[409] Подробность о принятых Кремлем мерах по вопросам интернета и национальной безопасности см.: Soldatov A., Borogan I. The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries.– New York: Public Affairs, 2015. – 384 p.

начале данного раздела). К оборонительным операциям, типология которых была подробно разработана А. Манойло[410], относятся следующие методы:

1) перехват информационной повестки – «глушить» вброс противника собственным инфоповодом с более резонансным эффектом в самые первые минуты или часы после его обнаружения (при помощи разведки или других источников). Типичным примером такого рода операций являются «Скрипальские чтения», организованные в первую годовщину инцидента в Солсбери. Выброс информации о конференции на уровне профессора университета за несколько часов распространился на уровень международной повестки, перехватив на 48 часов информационную повестку у западных и российских СМИ с 3 по 4 марта 2019 года, что полностью разрушило установленный план по ИО зарубежных спецслужб к годовщине отравления С. Скрипаля;

2) перехват оперативной инициативы (или операции прямого действия) – данный тип операции реализовывается также как в операциях перехвата информационной повестки, но отличается в основном объектом воздействия. Перехват прямо направлен на срыв негласных действий противника, тем самым, разрушая его план ИО;

3) отвлечение на негодный объект – переключение внимания противника на стороннюю тему с целью маскировки истинных целей и задач ИО;

4) «информационные прививки – операции, предназначенные для выработки у целевых аудиторий коллективного иммунитета на негативное информационное воздействие (ожидаемого содержания)»[411];

5) «операции возвратного типа» (или операции класса «бумеранг») – информационные контроперации, рассчитанные на использование инерции, набранной операцией противника (как в айкидо или тхэквондо). В качестве примера можно привести оперативную комбинацию, разыгранную с США в марте 2020 года – сразу после объявления Д. Трампа о начале «антинаркотеррористической

[410] См. подробнее Манойло А. В. Информационные войны и психологические операции. Руководство к действию. – М.: Горячая линия– Телеком, 2018. – 496 с.
[411] Манойло А. В. Стратегические информационные операции и оперативные игры спецслужб. – М.: Горячая линия – Телеком, 2021. – С. 75.

операции» в Венесуэле. Данная операция получила название «Предупреждение Трампу: главное – не выйти на самого себя»[412].

Наступательные контрмеры к ИО также можно назвать превентивными контрмерами – то есть, на основе существующего опыта или усвоения «сигнала» о потенциальном информационном нападении противника нанести удар на упреждение. В отличие от вышеописанных контрмер защитного характера, данный тип операций носит наступательный характер (из-за этого его иногда называют агрессивным, об этом мы будем говорить ниже) и дают возможность вскрыть и пресечь враждебную деятельность на самой ранней стадии ее возникновения, заставить противника действовать в невыгодных условиях. К нему можно отнести: кибероперации, операции по коррекции восприятия и активные мероприятия спецслужб.

Кибероперации – это набор наступательных действий, направленный против компьютерных информационных систем, компьютерных сетей, инфраструктур с попыткой получить несанкционированный доступ к данным, функциям или другим ограниченным областям вычислительной системы. В соответствии с прямым объектом воздействия можно выделить кибероперации трёх типов действия: физические, логические и семантические. Физические кибероперации непосредственно воздействуют на компьютеры и каналы связи. Логические кибероперации направлены на программное обеспечение, сайты и иные технические цифровые данные. Одним из распространённых видов данных кибероераций является DDoS-атака, направленная на ограничение доступа к сайтам. Внедрение вредоносного программного обеспечения также является наиболее используемым методом в данном типе операций, так же как и внедрение вирусов-вымогателей NotPetya или Stuxnet. Семантические кибероперации направлены на получение персональных данных, сохраняющихся в Интернет-пространстве. К данному типу операций можно отнеси широкий круг действий несанкционированного сбора личной и секретной информации в киберпространстве, таких как

[412] Манойло А. В. Стратегические информационные операции и оперативные игры спецслужб. – М.: Горячая линия – Телеком, 2021. – С. 75.

взломы ящиков электронной почты, аккаунтов в социальных сетях, облачных хранилищ и т.д. Самыми яркими примерами такого типа действий можно назвать взлом электронной почты экс-госсекретаря США Хиллари Клинтон в 2016 году и утечки электронной почты кандидата в президенты Франции Эммануэля Макрона в 2017 году[413]. Стоит отметить, что подобные действия чаще всего направлены на осуществление психологического давления на противника и манипуляцию общественного мнения путем публикации полученной информации в кибероперациях.

Операции по коррекции восприятия – целенаправленные действия по улучшению имиджа собственной стороне и изменению восприятия целевых аудиторий к определённым событиям в свою пользу. Для достижения данной цели принято заменять неблагоприятную информацию для своей стороны, как объективную, так и сфабрикованную противником, новой информационной повесткой. Типичным примером коррекции восприятия можно назвать попытки США фальсифицировать историю Второй мировой войны, в то же время российские усилия по «переосмыслению» истории также можно отнести к данной категории операций. Стоит отметить, что, хотя суть операций по коррекции восприятия двух стран совпадает – заключается в манипуляции сознанием и оказании влияния на действия противника с оружием информации (это тоже суть самой ИО), применяемые средства для достижения цели данных операций различны. Собственно, в американской методике по коррекции восприятия, как привило, используются массовые сфабрикованные фейки, которые могут вызвать ажиотаж в краткосрочной перспективе, но могут также легко потерять свою достоверность и авторитет в случае их раскрытия аудиторией. В российской практике операции по коррекции восприятия реализуются в основном с помощью вбросов информации, благоприятной для собственной стороны или вредной для имиджа противника, с фактическим основанием, хотя иногда и с умышленным умолчанием части фактов.

[413] Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations [Электронный ресурс] // Booz Allen Hamilton. 2020.URL: https://www.boozallen.com/content/dam/home/docs/cyber/bearing-witness-uncovering-the-logic-behind-russian-military-cyber-operations-2020.pdf (Дата обращения: (10.02.2023).

Третьем видом наступательных контрмер можно назвать «активные мероприятия» – секретные или открытые специфические операции (мероприятия) спецслужб, направленные на оказание влияния на общественное мнение и действия противника с целью извлечь из этих мероприятий выгоду, например, заставить направить действия противника в выгодное русло, ослабить его позиций, сорвать его замыслы и т.д. К данной категории относятся как стратегические операций, так и оперативные игры разведки (как это понимается в методах информационных операций США против России). В качестве примера использования активных мероприятий российской стороной можно привести возможное, по утверждению ЦРУ, вмешательство российской разведки в выборы США 2016 года, что, как ошибочно считалось в разведсообществе США, повлияло на результат выборов[414].

Когда речь идёт о наступательных информационных операциях, наблюдаются противоположные взгляды среди российских и западных учёных. По словам российских учёных, российские информационные операции носят преимущественно оборонительный характер, в то время как западная литература сосредоточена на описании наступательных ИО России. Несмотря на это, по немногочисленным открытым российским источникам можно утверждать, что в Москве все же накоплен определённый опыт проведения наступательных ИО, в том числе в форме активных мероприятий (информационных контроопераций). Так, «типичным примером такого рода операций является «Дело Диосдадо Кабельо» августа 2019 года – операция по разоблачению агента ЦРУ в ближайшем окружении Президента Венесуэлы Н. Мадуро и продолжение данного инцидента «Поиск крота» в ЦРУ»[415]. Всего один «информационный вброс, опубликованный российским экспертом в венесуэльском издании «Medium» 17 августа 2019 года, вызвал настоящую панику в ЦРУ и «эффект домино», который, как следствие,

[414] Assessing Russian Activities and Intentions in Recent US Elections [Электронный ресурс] //Office of the Director of National Intelligence..2017.URL: https://www.dni.gov/files/documents/ICA_2017_01.pdf (дата обращения: 10.02.2023).
[415] Манойло А. В. Современная практика информационных войн и психологических операций. Вирусные технологии и «эпидемии» каскадного типа на примере операции по разоблачению агента влияния ЦРУ, бывшего вице–президента Венесуэлы Диосдадо Кабельо [Электронный ресурс] // Национална сигурност (Nacionalna sigurnost). 2019. URL: https://nacionalna-sigurnost.bg/broi-3 (дата обращения: 15.10.2022).

привёл не только к провалу тщательно готовившихся и законспирированных тайных операций»[416] по проникновению в ближайшем окружении Н. Мадуро, но и к ряду неожиданных результатов, нанёсших США прямые потери, в том числе, в кадровом составе разведки. Так, сразу после разоблачения секретной инициативы США в операции «Дело Диосдадо Кабельо», Д. Болтон был уволен с поста помощника президента США по национальной безопасности. Наряду с этим, считая, что внутри разведсообщества США сидит «крот» (точнее, российский информатор), преемник Болтона Роберт О'Брайен «провёл в структурах разведсообщества «чистку», в результате чего СНБ США, аппарат директора национальной разведки и оперативный директорат ЦРУ покинули несколько десятков сотрудников – в основном специалистов по Латинской Америке и славистов»[417].

Согласно западным авторам, первые наступательные информационные операции современной России на ОТКС были проведены в конце 1990-х годов во время чеченского конфликта, когда как российские государственные, так и пророссийские негосударственные акторы атаковали чеченские электронные СМИ и другие сайты. Хотя эти действия лучше всего назвать хакерскими, они были направлены и на то, чтобы спровоцировать информационно-психологическое воздействие[418]. Впоследствии россияне также развивали свой инструментарий социальных сетей внутри страны: например, приблизительно с 2011 года стали выявляться такие методы, как перехват разговоров в Twitter и Facebook с целью препятствия координации деятельности оппозиции[419]. По сообщениям высокопоставленных чиновников разведки, после переизбрания В. В. Путина в контексте масштабных протестов 2011-2012 годов, российский президент поручил тогдашнему главе ГУ ГШ начать «перепрофилирование кибероружия, ранее использо-

[416] Там же.
[417] Там же.
[418] ФСБ не видит нарушения закона в действиях томских хакеров против сайта «Кавказцентр» [Электронный ресурс] // Newsroom. 2002. URL: https://www.newsru.com/russia/04feb2002/tomsk.html (дата обращения: 10.01.2023); Туровский Д. Пришло наше время послужить России [Электронный ресурс] // Meduza. 2018. URL: https://meduza.io/feature/2018/08/07/prishlo-nashe-vremya-posluzhit-rossii (дата обращения: 10.01.2023).
[419] Calabresi M. Inside Russia's Social Media War on America [Электронный ресурс] // Time. 2017. URL:https://translated.turbopages.org/proxy_u/en-ru.ru.69103ea1-63f8638d-b52db1f4–74722d776562/https/time.com/4783932/ (дата обращения: (10.02.2023); Elder M. Russians Fight Twitter and Facebook Battles over Putin Election [Электронный ресурс] // The Guardian. 2012. URL: https://www.theguardian.com/world/ 2012/may/13/russian-protests-march-occupy-abay (дата обращения: 15. 01.2023).

вавшегося для ПО в зонах боевых действий, для использования в предвыборной борьбе». После чего российские спецслужбы начали финансировать «фермы троллей» для расширения ИПО в киберпространстве [420].

Предполагается, что самые ранние онлайновые ИО России в отношении иностранных стран случились в период между 2005 и 2008 годами в контексте напряженных отношений с Эстонией и российско-грузинской войны[421]. Эти усилия, которые включали в себя DDoS-атаки на целевые веб-сайты, проводились сочетанием государственных акторов и патриотических хакеров[422]. По данным Исследовательского проекта вычислительной пропаганды (Computational Propaganda Research Project) Оксфордского университета, получившего доступ к аккаунтам IRA в Facebook, Twitter и Instagram, вдали от границ России ИО IRA в отношении англоязычных стран начались в 2013 году, но на «низком уровне»[423]. При этом американские авторы, в частности, разведчики и другие официальные лица, «почти единодушно» считают, что российские ИО 2016 года по так называемому вмешательству в американские выборы остались самым заметными ИО современной России в отношении демократических стран. По мере расследования данного инцидента разведка и другие официальные лица обнаружили, что Москва разработала изощренную тактику по ведению ИО[424].

Считается, что наиболее экспансивные и агрессивные ИО России произошли после кризиса на Украине 2014 года, когда российские государственные

[420] Calabresi M. Inside Russia's Social Media War on America [Электронный ресурс] //Time. 2017. URL: https://time.com/magazine/us/4783906/may-29th-2017-vol-189-no-20-u-s/ (дата обращения: 20.01.2023).

[421] Pomerantsev P., Weiss M. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money: A Special Report Presented by the Interpreter, a Project of the Institute of Modern Russia [Электронный ресурс]// Institute of Modern Russia. 2014. URL: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev_The_Menace_of_Unreality.pdf (дата обращения: 10.02.2023.); Timberg C. Russian Propaganda Effort Helped Spread 'Fake News' During Election, Experts Say [Электронный ресурс] // Washington Post. 2016. URL: https://www.washingtonpost. com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election–experts-say/2016/11/24/ 793903b6-8a40-4ca9-b712-716af66098fe_story.html (дата обращения: 20.01.2023).

[422] Pomerantsev P., Weiss M. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money: A Special Report Presented by the Interpreter, a Project of the Institute of Modern Russia [Электронный ресурс] // New York: Institute of Modern Russia. 2019. URL: https://imrussia.org/media/pdf/Research/Michael_ Weiss_and_Peter_ Pomerantsev__The_Menace_of_Unreality.pdf (дата обращения: 20.01.2023); Timberg C. Russian Propaganda Effort Helped Spread 'Fake News' During Election, Experts Say [Электронный ресурс] // Washington Post. 2016.URL: https://www.washingtonpost.com/business/economy/russian-propaganda-effort- helped-spread-fake-news-during-election–experts-say/2016/11/24/793903b6-8a40-4ca9-b712-716af66098fe_story.html (дата обращения: 20.01.2023).

[423] Howard Philip, Bharath Ganesh, Dimitra Liotsiou et al. The IRA, Social Media and Political Polarization in the United States, 2012–2018. – University of Oxford: Computational Research Project, 2018.– P. 9.

[424] Calabresi M. Inside Russia's Social Media War on America [Электронный ресурс] //Time. 2017. URL: https://time.com/magazine/us/4783906/may-29th-2017-vol-189-no-20-u-s/ (дата обращения: 20.01.2023).

акторы начали масштабное использование социальных сетей в своих ИО. Исследования проекта Computational Propaganda Research Project показали, что количество твитов от российской стороны несколько увеличилось в начале 2014 года, а затем резко возросло в конце 2014 года и в 2015 году. В то же время, сообщения российских акторов по ведению ИО распространились с Twitter на YouTube, Instagram и Facebook[425]. В одной из своих самых первых заметных кампаний IRA посеяла панику в городе Луизиана, распространяя через Twitter заявления о якобы имевшем место взрыве на заводе Columbia Chemicals[426]. А ГУ ГШ обнаружило ведение ИО в отношении лидера Украины через Facebook [427].

Основные причины широкого расхождения взглядов на наступательные ИО России между американскими и российскими учёными кроются в следующем: прежде всего, в большинстве ИО размыта граница между атакующими и защищающимися. Для достижения успеха в ИО требуются комбинации оборонительных и наступательных действий, а последние позволяют защитникам составить профиль противника после успешной атаки на него и использовать эти знания для совершенствования своей системы защиты, в данном случае первоначальный защитник превратится в атакующего. К тому же, хотя удачные информационные операции могут обеспечить стороне-инициатору значительное преимущество перед противником, но их применение осталось спорным, поскольку ИО могут быть актом агрессии, вызывающей возможные технические и этические последствия. Таким образом, будучи наиболее известными игроками в ИО на международной арене, и США, и Россия пытаются представлять себя жертвами, а другую сторону – агрессором с целью завоевать преимущество в общественном мнении. Так, в западной версии о российских ИО, по собственному мнению автора, кроме

---

[425] Howard P., Bharath G., Dimitra L. et al. The IRA, Social Media and Political Polarization in the United States, 2012–2018. – University of Oxford: Computational Research Project, 2018. – P. 9.

[426] Smith R. Columbia Chemical Hoax Tracked to ‘Troll Farm’ Dubbed the Internet Research Agency [Электронный ресурс] // News. 2015. URL: https://www.news.com.au/technology/online/social/columbia–-chemical-hoax-tracked-to-troll-farm-dubbed-the-internet-research-agency/newstory/128af54a82b83888158f7430136bcdd1 (дата обращения: 05.02.2023).

[427] Nakashima E. Inside a Russian Disinformation Campaign in Ukraine in 2014 [Электронный ресурс] // Washington Pos t. 2017.URL: https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html (дата обращения: 05.02.2023).

некоторых необоснованных обвинений с политизацией собственной информации для демонизации противника, в её фактологической части с, видимо, достаточными доказательствами, не исключается возможность того, что усиление информационного наступления Запада вызвало адекватные ответные действия России в форме ИО (как оборонительных, так и наступательных). Ведь США по-прежнему остались мировым лидером в области ИКТ, владея абсолютной инициативой в ведении информационной войны. Таким образом, западный нарратив типа ведения Россией «экспансивных» и «агрессивных» ИО после 2014 года можно понять – с некоторой долей скепсиса; однако он в большой степени игнорирует или преднамеренно скрывает предпосылки и контекст активности ИО России. Более того, исходя из своих собственных политических позиций и желаемых политических целей, западные учёные пришли к совершенно противоположным, даже искажённым выводам о природе событий, чем российские, рассматривая «активные ответные меры» (по мнению российских учёных) как агрессивную информационную войну. Такой контраст нетрудно понять после всего – между Россией и Западом давно существует непримиримый (пусть и временно смягчённый) конфликт.

Важно также отметить, что, хотя позиции и взгляды российских и западных учёных на вопрос о том, кто является «агрессором» и «жертвой» информационной войны, существенно различаются, вместе с тем существует поразительное совпадение определённых мыслей, событий и доводов в аргументах обеих сторон. Это доказывает, что эти события действительно были ключевыми моментами в развитии информационной войны, показывающими процесс эволюции формы, методов и интенсивности информационного противоборства.

Схема 7. Типология контрмер России к ИО

Целая цепочка ИО состоит из трех звеньев: производства контента (путём фабрикации, кражи, взлома и т.д.), распространения контента по каналам ОТКС и потребления контента целевой аудиторией. Таким образом, мы также можем рассматривать контрмеры к ИО с точки зрения этапов их осуществления (схема 7). В таблице 3 представлены эти категории контрмер с отдельными примерами каждого типа. Стоит отметить, что контрмеры могут быть направлены на любой один или несколько этапов этой цепочки, при этом они могут также выполнять логически предшествующие функции повышения осведомлённости или институционального строительства.

Таблица 3. **Типология контрмер к ИО с точки зрения жизненного цикла дезинформации**

Звено ИО	**Контрмеры**	**Пример**	**Дополнение**
Производство	Препятствовать субъектам ИО производить или заказывать производство контента	Сдерживание наказанием Сдерживание воспрещением Блокирование субъектов	Повышение осведомлённости: 1) выявление и анализ исполнителей и меха-

		ИО	низмов в жизненном цикле дезинформации; 2) повышение осведомлённости об угрозе среди лиц, принимающих решения и целевой аудитории. Организационное строительство: создание институтов с полномочиями и возможностями для борьбы с дезинформацией
Распространение	Ограничить субъектов от распространения контента	Сдерживание наказанием Сдерживание воспрещение Блокирование субъектов ИО Запрет или ограничение каналов социальных сетей Алгоритмические, правовые и ручные ограничения на распространение дезинформации	
Потребление	Повышение устойчивости аудитории, снижение восприимчивости к контенту	Развенчание Медиаграмотность Проактивная публичная дипломатия Позитивная стратегическая коммуникация Снижение доверия к информации противника	

Контрмеры, направленные на стадию производства – это меры, которые направлены на предотвращение производства или заказа инициаторами ИО продукции контента, например фабрикации информации или получения защищённой информации путём кибероперацій.

Предотвращение может осуществляться следующим образом:

- сдерживание наказанием – уведомление возможных (потенциальных) агрессоров ИО о серьёзных последствиях своей деятельности по ИО против России, чтобы они осознали, что стоимость своих действий намного превышает их ценность, и далее отказались от ИО. Повлеченные наказания из-за ИО агрессора, включая экономические санкции, дипломатическую изоляцию и уголовное преследование, могут быть направлены как на государство в целом, так и на кон-

кретных лиц. Типичным примером контрмер такого типа можно назвать недавнюю деятельность внешнеполитического ведомства России: в начале февраля 2023 года МИД России передало ноту Посольству США с требованием прекратить злонамеренную активность в информационном пространстве против России, которая «относится к уголовно наказуемым деяниям», пригрозив высылать всех причастных к такой деятельности из страны, вне зависимости от занимаемых постов[428];

- сдерживание воспрещением – повышение порога для совершения информационных атак, чтобы заставить их исполнителей поверить в трудность или невозможность достижения своих целей. Для этого конкретные меры могут быть техническими и правовыми, например публикация ряда законов по усилению контроля над деятельностью в информационном пространстве России, в частности, Закон об иноагентах. Другим примером можно назвать ведённый в эксплуатацию с 2019 года «суверенный Рунет», сочетающий технические и правовые аспекты сдерживания воспрещением;

- блокирование акторов ИО – лишение способности производителей размещать дезинформацию в Интернете, например, через блокирование учётных записей потенциальных акторов ИО, требование проверки личности, выведение троллей из сети или блокирование сайтов. Последним примером можно назвать блокирование Роскомнадзором сайтов ЦРУ и ФБР на территории России из-за обнаружения на этих ресурсах деятельности по распространению дезинформации и дискредитации российской армии[429].

Меры для этапа распространения информации направлены на препятствие распространению дезинформации или злонамеренной пропаганды. Такие меры включают выявление и пресечение деятельности аккаунтов в соцсетях, распространяющих дезинформацию, ограничение каналов, доступных для потенциальных акторов ИО, и прикрытие контента злонамеренных дезинформации и пропа-

[428] МИД вручил посольству США ноту с требованием не вмешиваться в дела России[Электронный ресурс] // РИА НОВОСТИ. 2023. URL: https://ria.ru/20230207/ssha01850326734.html (дата обращения: 20.01.2023).
[429] Роскомнадзор объяснил блокировку сайтов ЦРУ и ФБР дискредитацией армии [Электронный ресурс] // РБК. 2023. URL: https://www.rbc.ru/politics/27/01/2023/63d3b5e69a79479d2da90fd2 (дата обращения: 20.01.2023).

ганды. Те же виды контрмер, которые направлены на стадию производства, доступны и для звена распространения информации, например, угроза судебного преследования или повышение сложности распространения контента на платформах соцсетей путём блокировки аккаунтов. Кроме того, распространение дезинформации также может быть ограничено с помощью алгоритмов, отсеивающих фальшивые материалы, законов и нормативных актов, запрещающих или цензурирующих определённый контент или его создателей, а также ручных процессов, отсеивающих дезинформацию или пропаганду.

Контрмеры для этапа потребления информации направлены на создание устойчивости, снижение восприимчивости или прививку аудитории от ИО агрессора. Для реализации этих целей помогают развенчание (т.е. разоблачение дезинформации или манипулируемой информации) и обучение, в частности воспитание медиаграмотности. К тому же, ознакомление аудитории с проактивной публичной дипломатией или стратегической коммуникацией также может снизить восприимчивость к дезинформации по соответствующим вопросам. Другие меры, такие, как предупреждения, пометки информации, которая подозревается как ложная, или идентификация конкретных источников как подозрительных также помогают снизить доверие аудитории к соответствующей информации.

К тому же попытки и усилия по организационному строительству и повышению осведомлённости пронизывают всю цепочку «производства-потребления». Организационное строительство подразумевает создание организаций с необходимыми полномочиями и возможностями для проведения информационных операций оборонительного и наступательного характера. Меры по повышению осведомлённости целевой аудитории о дезинформационной и пропагандистской деятельности могут быть достигнуты путём обнаружения сотрудников профильных органов, а также с помощью исследований и анализа компетентных экспертов, как это сделали на антифейковом сайте «Вбросам. нет»[430]. Обнаружение означает идентификацию тайных акторов ИО и является предпо-

[430]Антифейк–кафе «Вбросам.нет!» [Электронный ресурс] // «Вбросам.нет!» URL: http://vbrosam.net/about/ (дата обращения: 20.09.2022).

сылкой для ряда других мер. Исследование и анализ намного сложнее обнаружения и направлены на лучшее понимание природы ИО и на разработку возможных контрмер. Доведение результата обнаружения, исследования и анализа до сведения пользователей Интернет-сети также влияет на потребление информации, потенциально снижая восприимчивость аудитории к дезинформации.

В основном, межправительственные и неправительственные контрмеры к ИО были направлены на повышение осведомлённости и потребление информации. Более того, поскольку угроза манипулирования информацией в соцсетях возникла недавно, в отличие от западных стран, которые приложили значительные усилия для организационного строительства, российское правительство осталось на стадии исследования. Контрмеры, направленные на стадию распространения информации, как правило, находятся в компетенции компаний соцсетей.

2.4. Оценка эффективности российского противодействия гибридной агрессии США в информационном пространстве

Представление России об информационной войне во многом обусловлено информационными атаками на Советский Союз Западом во время холодной войны, что стало одним из основных факторов распада СССР[431]. С распадом Советского Союза информационные операции Запада продолжаются на огромном, слабо защищённом российском пространстве и превращаются в открытую информационную агрессию против России. Так, после «оранжевой революции» в 2004 году главнокомандующий европейскими силами НАТО Филип Бридлав подчеркнул, что Запад должен вести информационную войну против России в ответ на события в Украине[432]. В 2016 году Центр анализа европейской политики (CEPA) опубликовал доклад «Победа в информационной войне», предсказавший антироссийские стратегии в информационном поле[433]. На данный момент информационная стратегия Запада против России давно созрела.

Основная цель ИВ Запада против современной России заключается в осуществлении контроля над ней путём организации цветной революции, с помощью которой проамериканские силы получат абсолютное господство в российском правительстве. Реализация данной цели выполняет две основные функции: привести к упадку России, превратив её в потенциально «разделённую» страну (как Советский Союз в 1991 году) с возможностью инициации гражданской войны; изолировать её от международного сообщества путем дискредитации, ведь

[431] Григорьев Ю. П. Антироссийские информационные войны // Россия: тенденции и перспективы развития. – 2015. – Выпуск 10.– Часть I. – С. 255– 259.
[432] Breedlove P. West Must Fight Russia in Information War [Электронный ресурс] // Military Times. 2015. URL: https:// www.militarytimes.com/2015/03/22/breedlov-west-must-fight-russia-in-information-war (дата обращения: 06.01.2023).
[433] Крылова И. А. Информационные войны и безопасность России// Россия: тенденции и перспективы развития. – 2016. – Выпуск 11. – Часть Ⅱ. – С. 116–121.

сформированный Западом образ России как «отсталой», «авторитарной» и «агрессивной» проникает в СМИ и массовое сознание по разным каналам[434].

Как именно осуществляются информационные операции против России, показано в работах А. В. Манойло – он впервые системно раскрыл эту схему[435]. В контексте СВО структура ИО, проводимых США в отношении России, состоит из четырёх ярусов: стратегические информационные операции, оперативные игры, фейки и спецпропаганда[436]. Первые три приёма являются типичными в практике США в их противостоянии современной России в информационной сфере, а спецпропаганда, давно известная еще со времён Холодной войны форма информационной борьбы, стала с началом СВО доминировать.

Стратегические информационные операции – это оперативные комбинации иностранных разведок, направленные на обвинения в совершении руководством страны-противника особо тяжких преступлений с предположительной целью в перспективе посадить его на скамью международного трибунала. Прежде, в период «после Крыма» (2016-2021 годы), эта форма информационных операций (делящихся на стратегические и тактические) была доминирующей в ИВ против России: к ним относится и «дело Скрипалей», и «Допинговый скандал с WADA», и «дело об аргентинском кокаине» и даже так называемое «дело об отравлении Навального»[437]. Но с началом СВО их число резко сократилось, вместо них на пике популярности оказалась спецпропаганда.

Оперативные игры ведутся иностранными разведками с лицами, близкими к власти (например, политическая и экономическая элита, особенно российские олигархи), которые имеют крупные активы на Западе и могут оказывать значительное влияние на политические решения своей страны. Данный вид операций предназначен, прежде всего, для организации насильственной смены власти в РФ с помощью внутренней оппозиции типа «пятой колоны» по сценарию так назы-

---

[434] Там же.
[435] Манойло А. В. Стратегические информационные операции и оперативные игры спецслужб. – М.: Горячая линия – Телеком, 2021. – С. 59–75.
[436] Манойло А. В. Информационные диверсии в конфликте на Украине // Вестник МГОУ. – 2022. – №4.
[437] Манойло А. В. Информационная война и новая политическая реальность: Ч. II // Вестник МГОУ. Электронный журнал. Серия Политология. – 2021. – № 2. – С. 110– 148.

ваемого «Венесуэльского прецедента»[438].

Фейки – это специфическая форма дезинформации. Цели фейковых атак варьируются от конкретных – насаждения страха, ажиотажа, разжигания ненависти, до отвлечения сил и средств противника на негодный объект: чем больше кадров и ресурсов направляют на разоблачение фейков, тем меньше внимания уделяется настоящим стратегическим информационным операциям – таким, например, как инцидент в Буче.

Спецпропаганда – это методы, направленные на дискредитацию лидеров, деморализацию армии противника, подрыв политической стабильности внутри государства. Данный приём очень старый, давно известный еще по «холодной войне», но порядком подзабытый в эпоху монополии на информационные операции специальных служб, ведущих свои оперативные игры на каналах ОТКС (2014-2021 годы), стал основным по интенсивности в информационной борьбе в сегодняшнем украинском конфликте. С этой точки зрения можно сказать, что с началом СВО наблюдается определённый регресс в технологиях информационной войны: на передний план выдвинулись классические приемы спецпропаганды и примитивные фейки, временно «вытеснив собой с ТВД более тонкие инструменты организации идеологических диверсий – оперативные комбинации и оперативные игры спецслужб»[439].

Предполагается, что рост боеспособности информационных операций современной России начался после «первой чеченской войны» 1994 года, когда российские военные проиграли информационную войну чеченским сепаратистам[440]. Извлекая уроки из «первой чеченской войны», бывший начальник штаба СКВО пришёл к выводу, что ГРУ должно создать учебный центр для воспитания технических специалистов и развивать современные технологии повышения эф-

[438] Манойло А. В. Современная практика информационных войн и психологических операций. Вирусные технологии и «эпидемии» каскадного типа на примере операции по разоблачению агента влияния ЦРУ, бывшего вице–президента Венесуэлы Диосдадо Кабельо [Электронный ресурс] // Национална сигурност (Nacionalna sigurnost). 2019. URL: https://nacionalna-sigurnost.bg/broi-3 (дата обращения: 15.10.2022).
[439] Манойло А. В. Информационные диверсии в конфликте на Украине // Вестник МГОУ. – 2022. – №4.
[440] Pain P. (Translated by Robert R. Love). The Second Chechen War: The Information Component. – Fort Leavenworth: Foreign Military Studies Office, 2000. – P. 8.

фективности психологических операций (ПО)[441]. Однако с тех пор и до «российско-грузинской войны» 2008 года ситуация ненамного улучшилась, когда в распоряжении российских военных было всего 50 специалистов по ПО, и лишь немногие из них обладали техническими навыками, такими, как проведение телевизионных трансляций[442]. Таким образом, когда Грузия изображала Россию как агрессора, успешно воздействуя на мировое общественное мнение через СМИ, российские специалисты по связям с общественностью не смогли развернуть убедительную контрпропаганду[443], что заставило Россию переосмыслить свою способность к проведению ИО[444]. К началу «Евромайдана» 2014 года технологии и боевые силы России по ведению ИПО претерпели качественное изменение – на базе классических советских теорий об ИПО, таких, как рефлексивный контроль[445], и опыта информационного противоборства с США, Россия стала менять ситуацию в ИО в свою пользу. В отличие от Грузии, на Украине Россия задействовала многочисленные акторы и инструментарии для влияния на общественное мнение в своей стране и за рубежом, сочетая военные операции, деятельность контролируемых государством СМИ, социальные сети, официальную риторику и неофициальную тайную деятельность, такую, как IRA и другие «фермы троллей»[446]. После вхождения Крыма в состав России наблюдаются участившиеся обвинения Запада в ведении Россией ИВ в глобальном масштабе с целью укре-

---

[441]Потапов В. Действия соединений, частей и подразделений СВ при проведении специальной операции по разоружению НВФ в 1994–96 гг. на территории Чеченской республики. Доклад бывшего начальника штаба СКВО генерал– лейтенанта В. Потапова [Электронный ресурс] // Вестник ПВО. (дата не известна). URL: http://pvo.guns.ru/book/chechnya_pvo.htm (дата обращения: 06.01.2023).

[442] Цыганок А.Д. Первые жертвы оружия нового поколения [Электронный ресурс] // Независимое военное обозрение. 2018. URL: https://nvo.ng.ru/armament/2018-11-16/8_1022_victim.html (дата обращения: 06.01.2023).

[443] Овчинников В. В., Новиков М. П. Информационное противоборство в современной геополитике // Защита и безопасность. – 2011. – № 2. – С. 10–11.; Василенко И. Формирование нового образа России «после Крыма»: парадоксы информационной войны // Власть. – 2014. – № 10. – С. 207–208.

[444] Iasiello E.J. Russia's Improved Information Operations: From Georgia to Crimea // Parameters.– 2017. – Vol. 47, No. 2. – P. 51.

[445] Snegovaya M. Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare. Russia Report I [Электронный ресурс] // Institute for the Study of War. 2015. URL: https://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf (дата обращения: 10.02.2023 г.); OlikerOlga.Russia's New Military Doctrine: Same as the Old Doctrine, Mostly // Washington Post. 15.01.2015. URL:https://www.washingtonpost. com/news/monkey-cage/wp/2015/01/15/russia-snew-military-doctrine-same-as-the-old-doctrine-mostly/ (дата обращения: 06.01.2023).

[446]Treyger Elina, Joe Cheravitch, Raphael S. Cohen. Russian Disinformation Efforts on Social Media [Электронный ресурс] // RAND Corporation. 2022. URL: https://www.rand.org/pubs/research_reports/RR4373 z2.html (дата обращения: 06.01.2023)

пить стабильность российского режима и международное положение путём подрыва Запада[447]. Таким образом, «Крымская весна» считается успешной практикой российских ИПО (как оборонительных, так и наступательных) с использованием Интернета как оружия, в частности, возможностей социальных сетей. При этом Кремль рассматривает Интернет как угрозу безопасности режима и эффективное оружие в борьбе с противником России. Как отметил бывший глава Администрации президента России Сергей Иванов: «Сеть – палка о двух концах: может и пользу сослужить, и быть откровенной помойкой»[448].

С 2008 года Россия выпустила две последовательные стратегии по развитию «информационного общества». По мере публикации этих документов, предназначенных для стимулирования цифрового развития и технологических инноваций, наблюдалось введение, в том числе, все более жёстких мер цензуры и надзора. В последующее десятилетие данная стратегия была дополнена целым рядом законов с целью установления «суверенитета» над инфраструктурой, контентом и данными информационного пространства России, в частности, RuNet является кульминацией этих усилий[449].

С начала нового 21-го века российские ученые, политики и военные специалисты неоднократно писали об информационных угрозах стране. Так, в марте 2000 года тогдашний министр иностранных дел И. Иванов назвал сообщения западных СМИ о коррупции Б. Ельцина «настоящей информационной войной» против России, отмечая, что западные СМИ стремятся «нарисовать крайне негативную, однобокую картину современной России» с целью очернить Россию, отодвинуть ее на второстепенные роли и лишить её независимого голоса в миро-

---

[447] Costello K. Russia's Use of Media and Information Operations in Turkey. Santa Monica, Calif.: RAND Corporation. 2018; Scott Jasper. Russia's Ultimate Weapon Might Be Cyber [Электронный ресурс] // The National Interest. 2018. URL: https://nationalinterest.org/profile/scott-jasper (датаобращения: 06.01.2023); Kovacs E. Russian Cyberspies Shift Focus from NATO Countries to Asia [Электронный ресурс] // Security Week. 2018. URL: https://www.securityweek.com/ russian-cyberspies-shift-focus-nato-countries-asia/ (дата обращения: 06.01.2023).

[448] Руководитель администрации президента России – в спецпроекте ТАСС «Первые лица» [Электронный ресурс] // ТАСС. 2015. URL: https://tass.ru/top– officials/2356242 (датаобращения: 20.10.2022).

[449] Sherman J. Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior [Электронный ресурс] // Atlantic Council. 2021. URL: https://www.atlanticcouncil.org/wp-content/uploads/ 2021/07/RuNet-Issue-Brief-2021.pdf (дата обращения: 20.10.2022).

вых делах[450].

В первые два срока В. В. Путина и в президентство Д. А. Медведева лидеры России не стали «массовым проявлением идеологического и аллегорического мышления»[451]. Хотя СМИ страны утратили большую часть своей «независимости», вмешательство правительства в культуру было ограниченным. Однако, после избрания В. В. Путина президентом в 2012 году, когда Россия оказалась в осаде объединённых усилий Европы и США, направленной на стратегическую изоляцию страны и ее культурное разрушение, «конспирология» (концепт «осажденной крепости») постепенно стала мейнстримом.

Катализаторов этой эволюции было несколько. Прежде всего, протесты против так называемой «фальсификации выборов» осенью 2011 года в России, организованные под руководством предполагаемых американских спецслужб с использованием новой телекоммуникационной технологии[452] (в частности, благодаря использованию соцсетей – через Facebook и российский VK), заметно укрепили решимость российского правительства усилить контроль над внутренним информационным пространством. К тому же ряд ключевых событий на международной арене также усилили опасения относительно дальнейшего развития Интернета и обострили восприятие угрозы со стороны ИПО для государственной безопасности, чему способствовали, в частности, движение «арабской весны» в 2011 году[453], утечки Сноудена в 2013 году[454], скандал «Панамских документов» в 2016 году[455] и даже инциденты в самой России, когда граждане публиковали ро-

---

[450] Hoffman D. Yeltsin's Immunity Up held by Duma Vote [Электронный ресурс] // Washington Post. 2000. URL: https://www.washingtonpost.com/wp-srv/WPcap/2000-03/30/090r-033000-idx.html (дата обращения: 05.02.2023).

[451] Borenstein E. Plots against Russia: Conspiracy and Fantasy After Socialism. – Cornell University Press, 2019. – P. 27.

[452] Gutterman S., Bryanski G. Putin Says U.S. Stoked Russian Protests [Электронный ресурс] // Reuters. 2011. URL: https://www.reuters.com/article/uk-russia-idUKTRE7B70H720111208 (дата обращения: 10.01.2023).

[453] Exporting Revolution [Электронный ресурс] // RT. 2012. URL: https://www.rt.com/usa/ revolution-activists-world-people-297 (дата обращения: 10.01.2023).

[454] Soldatov A., Borogan I. How Edward Snowden In advertently Helped Vladimir Putin's Internet Crackdown [Электронный ресурс] // BuzzFeedNews. 2015. URL: https://www.buzzfeednews.com/article/andreisoldatov/ how-edward-snowden-inadvertenly-helped-vladimir-putins-inter (дата обращения: 05.01.2023).

[455] Russia's Putin: Panama Papers Area 'Provocation [Электронный ресурс] // Reuter. 2016. URL: https://www.reuters.com/article/us-russia-putin-panamapapers/russias-putin-panama-papers-are-a-provocation-idUSKCN0XB16D (дата обращения: 05.01.2023); Taylor A. Putin Saw the Panama Papers as a Personal Attack and May Have Wanted Revenge, Russian Authors Say [Электронный ресурс] // Washington Post. 2017. URL: https://www.washingtonpost.com/news/worldviews/wp/2017/08/28/putin-saw-the-panama-papers-as-a-personal-attack-and-may-have-wanted-revenge-russian-authors-say (дата обращения: 05.01.2023).

лики об «обысках» у лидеров оппозиции и проявления «жестокости полиции» в Интернете[456]. Таким образом, реальные вызовы режиму в сочетании с конспиративным мышлением привели к решению усилить контроль над информацией и сфокусировать усилия на информационной войне, которая все чаще ведётся именно в пространстве Интернет.

В частности, кризис на Украине 2013-2014 годов оказался важным переломным моментом, подвигавшим российские власти ужесточить контроль над внутренним информационным пространством. После украинского Майдана информационные кампании все больше были направлены на гораздо более сложные геополитические события. В качестве важных составляющих сил ИО России выступили пророссийские силы и пропагандистские СМИ, которые переключили свое внимание с отечественных оппозиционеров на «клеймение» лидеров Украины как «фашистов», которых «США и их союзники используют в качестве оружия против Москвы»[457]. Впервые за последние семнадцать лет высокопоставленные политики, включая самого президента В. В. Путина, начали регулярно озвучивать такие идеи публично[458].

Таким образом, информационная война воспринималась Россией как «оружие» для сохранения статуса великой державы и внутриполитической стабильности:

- во-первых, российское руководство и элиты, как политические, так и военные, проецируют важное положение России в мире с помощью антироссийских информационных операций;

- во-вторых, повышается сплочённость российского общества с помощью подчёркивания или даже преувеличения угроз информационных операций «недружественных» государств-агрессоров (переключение внимания с внутренних конфликтов на внешние угрозы);

---

[456] Franke U., Pallin C.V. Russian Politics and the Internet in 2012.– Stockholm: Defense Research Agency, 2012. –P. 44.
[457] Seddon M. Documents Show How Russia's Troll Army Hit America [Электронный ресурс] // Buzzfeed News. 2014. URL: https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army- hit-america (дата обращения: 05.01.2023).
[458] Yablokov I. Fortress Russia: Conspiracy Theories in Post–Soviet Russia. – Medford: MA; Polity, 2018. – P. 183– 184.

- в-третьих, достаточно просто узаконивать при этом новые меры по усилению контроля государством над общественными мнениями и потоком информации. Наряду с реальными угрозами, метод по созданию воображаемого представления об иностранных информационных угрозах внутренней стабильности России, который бывший сотрудник службы национальной безопасности США и эксперт по вопросам России Фиона Хилл называет «искусством наступательной обороны», стал неотъемлемой частью российской внешней политики[459].

Эффективность российских контрмер относительно ИО США и их союзников можно анализировать со следующих точек зрения: 1) конкретных кейсов по ИВ; 2) оценки или мнений представителей в данной области исследования; 3) применяемых конкретных средств в ИВ.

По открытым источникам из классических примеров успешных ИО современной России исключительно выделяются так называемые «Скрипальские чтения» (в марте 2019 года) и «Дело Диосадо Кабельо» (в августе 2019 года), а также его продолжение – «поиск «крота» с Р. О'Брайеном, помощником Президента США по национальной безопасности (в октября 2019 года)»[460], с которыми уже довольно подробно разобрались, и которые представлены как в публикациях СМИ [461], так и в различных научных источниках[462].

В том числе, оперативная комбинация «Скрипальские чтения» на сегодняшний день «продолжает оставаться одной из самых эффективных (а возможно, даже самой эффективной) операций по перехвату информационной повестки»[463]. О её эффективности говорят статистические данные: так, «в период про-

[459] Hill F. Mr. Putin and the Art of the Offensive Defense: Approaches to Foreign Policy (Part Two) [Электронный ресурс] // Brookings Institution. 2014. URL: https://www.brookings.edu/articles/mr-putin- and-the-art-of-the-offensive-defense-approaches-to-foreign-policy-part-two (дата обращения: 05.01.2023).

[460] Манойло А. В. Современная практика информационных войн и психологических операций. Вирусные технологии и «эпидемии» каскадного типа на примере операции по разоблачению агента влияния ЦРУ, бывшего вице–президента Венесуэлы Диосдадо Кабельо [Электронный ресурс] // Национална сигурност (Nacionalna sigurnost). 2019. URL: https://nacionalna-sigurnost.bg/broi-3 (дата обращения: 15.10.2022).

[461] Manoilo A.V. Skripal Readings as an Example of a Special Operation to Intercept the Information Agenda. The Latest Practice of Modern Information Warfare and Psychological Operations [Электронный ресурс] // Medium. 2020. URL: https://medium.com/@andreimanoilo/skripal-readings-as-an-example-of-a-special-operation-to-intercept-the-information-agenda-dd55b3dab908 (дата обращения: 10.10.2022).

[462] Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно–психологической войны. 4–е изд., перераб. и доп. – М.: Горячая линия – Телеком, 2020. – С. 344–345.

[463] Манойло А. В. Стратегические информационные операции и оперативные игры спецслужб. – М.: Горячая линия – Телеком, 2021. – С. 67.

ведения операции (с 3 по 4 марта 2019 года) только в одном Telegram информационный повод захватил внимание аудитории более чем в один миллион триста тысяч (1304640) человек. Совокупный же охват в СМИ только за время проведения операции составил более 50 млн. человек (101 материал)»[464]. Но в то же время стоит отметить, что, по мнению некоторых российских авторов, само «Дело об отравлении Сергея и Юлии Скрипалей» 2018 года в Солсбери – пример «филигранно проведённой американскими и британскими спецслужбами стратегической операции информационной войны», как бы к ней при этом не относились[465].

Также стоит отметить, что примеры успешных ИО в российской практике пока являются только «явлениями единичными и не могут заменить собой систему информационного противодействия, которая уже есть у США»[466], но отсутствует до сих пор в России, хотя потребность в ней давно назрела. После истории с «Панамским досье» силовые ведомства России стали проявлять повышенный интерес к теме информационного противоборства. В отличие от США, где действует система планирования и проведения информационных операций, «у России каждое ведомство действует само по себе, пытается проводить как операции, так и контроперации, однако в 90 % случаев эти сотрудники не знают стратегии и тактики развёртывания данной работы»[467],что с большой степенью вероятности ведёт к тому, что «на системные действия США Россия отвечает практикой запаздывающих импровизаций»[468]. В этом плане типичным примером такой «хаотичности» послужили неудачные ответы российской стороны на первых этапах в «Деле об отравлении Скрипалей» 2018 года, когда наблюдалась практически

[464] Манойло А. В. Информационная война и новая политическая реальность: Ч. II // Вестник МГОУ. Электронный журнал. Серия Политология. – 2021. – № 2. – С. 110–148.
[465] Манойло А. В. Дело Скрипалей как операция информационной войны // Вестник Московского государственного областного университета (электронный журнал). – 2019. –№ 1. – С. 72– 96.
[466] Манойло А. В. Информационная война и новая политическая реальность: Ч. II // Вестник МГОУ. Электронный журнал. Серия Политология. – 2021. – № 2. – С. 110–148.
[467] Триггеры информационной схватки [Электронный ресурс] // Независимое военное обозрение. 2020. URL: https://nvo.ng.ru/nvo/2020-11-12/1_1117_triggers.html (дата обращения: 10.11.2022).
[468] Манойло А. В. Стратегические информационные операции и оперативные игры спецслужб. – М.: Горячая линия – Телеком, 2021. – С. 74–75.

полная несогласованность действий российских министерств и ведомств в деле реагирования на продолжение истории со Скрипалями.

Поскольку большинство информационных операций ведётся негласно, в частности, стратегических информационных операций и оперативных игр спецслужб, это не позволило оценить их эффективность по открытым источникам; для решения этого вопроса возможен анализ мнений ведущих экспертов в данной области исследования (включая российских, западных и китайских учёных) с попыткой дать как можно всестороннюю, объективную оценку эффективности противодействия Россией информационной войны.

Как отметил директор Национальной разведки США Дэниел Коутс, «без сомнения, Россия считает свои прошлые усилия по ИО успешными» [469]; «представители различных кругов России не скупятся на восхищение от достигнутых своей страной результатов в информационном противостоянии с противниками». Так, Андрей Крутских, главный советник президента РФ по вопросам информационной безопасности, в 2017 году сравнил возможности России в информационной войне с получением ядерного оружия, заявив, что Россия получит «нечто на информационной арене, что позволит нам разговаривать с американцами на равных[470]». Вместе с тем комментируя действия России в Сирии, командующий Южным военным округом генерал-полковник Александр Дворников подчеркнул важность информационных операций в арсенале России: «информационные ресурсы стали одним из наших самых эффективных видов оружия», и «без информационных операций у нас не было бы успеха в Алеппо, Дейр-эз-Зоре и Гуте»[471].

Взгляды американских учёных на эффективность российских ИО можно анализировать как с позиции их прямых оценок, так и с позиции выдвигаемых

---

[469] Rosenberg M., Savage G., Wines M. Russia Sees Midterm Elections as Chance to Sow Fresh Discord Intelligence Chiefs Warn // New York Times. 13.02.2018. URL: https://www.nytimes.com/2018/02/13/ us/politics/russia-sees-midterm-elections-as-chance-to-sow-fresh-discord-intelligence-chiefs-warn.html (дата обращения: 20.12.2022).

[470]«Информационная битва». Как Россия создавала фейковых американцев, чтобы повлиять на выборы [Электронный ресурс] // Главк. 2017. URL: https://glavk.net/news/265042-informatsionnaja_bitva._kak_rossija_sozdavala_fejko vyh_amerikantsev_chtoby_povlijatj_na_vybory (дата обращения: 20.12.2022); Ignatius D. Russia's Radical New Strategy for Information Warfare [Электронный ресурс] // Washington Post. 2017. URL: https://www.washingtonpost.com/ blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/ (дата обращения: 20.12.2022).

[471] Дворников А. Штабы для новых войн [Электронный ресурс] // Военно–промышленный курьер. 2018. URL: https://vpk.name/news/222202_shtaby_dlya_novyh_voin.html(дата обращения: 20.09.2022).

ими обвинений о ИО против США и их союзников. По мнению бывшего заместителя АНБ Криса Инглиса, Россия опережает США на 10 лет в желании использовать социальные сети для влияния на общественное мнение[472]. Наряду с этим, другие американские эксперты считают, что российские ИО уже нанесли реальный и значительный ущерб США даже только из-за их «вещательных операций» в течение американских выборов 2016 года. Так, как отметил Джаред Эндрю Коэн, старший исследователь Совета по международным отношениям (CFR), «вызывая сомнения в достоверности результатов голосования 2016 года и уязвимости будущих выборов, Россия достигла своей самой важной цели: подорвала доверие к американской демократии»[473]. По мере расследования российских операций в инциденте так называемого «вмешательства в выборы США» 2016 года десятки высокопоставленных сотрудников разведки и других организаций, занимающихся расследованием российских операций влияния утвердили, что Москва разработала сложную тактику для расширения своего влияния в киберпространстве. Соединив столетний опыт операций влияния с новой праформой социальных сетей, Россия, возможно, получила возможность, к которой долго стремилась, но так и не смогла полностью реализовать в годы холодной войны: изменять ход событий в США манипулированием общественным мнением[474].

Повсеместное обвинение России со стороны западных авторов в ведении информационной войны выражает опасение и тревогу США и их союзников о развитии информационного влияния, но одновременно также свидетельствует о том, что российские контрмеры к ИО имели определённый эффект «бумеранга» – если трудно сказать, в какой степени это реально повлияло на действия США, как минимум, его психологическое воздействие очевидно. Западное общество настолько оценило информационное влияние России, что некоторым специалистам пришлось напоминать, что сила российской ИО переоценена, публично призывая не уделять слишком много внимания так называемой «российской ин-

[472] Calabresi M. Inside Russia's Social Media War on America [Электронный ресурс] // TIME. 2017. URL: https://cs.brown.edu/people/jsavage/VotingProject/2017_05_18_Time_InsideRussia'sSocialMediaWarOnAmerica.pdf (дата обращения: 20.01.2023).
[473] Там же.
[474] Там же.

формационной войне». Так, Марк Галеотти, ведущий эксперт в области русской политики, считает опасения Запада перед российской ИО «панической реакцией». По его мнению, вместо реакции на реальное российское информационное поле боя, такие опасения являются отражением политической неуверенности и противоречий Запада, которые могут быть использованы Россией[475]. К данному мнению добавились другие учёные и чиновники, предупреждая, что страх перед российскими ИО может быть более разрушительным, чем сами операции. «Стремясь казаться более могущественными, чем они есть на самом деле, русские сочтут успехом, если вы усомнитесь в правдивости ваших источников новостей, зная, что Москва может скрываться в вашей ленте Facebook или Twitter»[476].

Китай намного отстаёт от США и России в плане исследований гибридных войн, в частности, такой ее составляющей как информационная война. Исследования китайских учёных основаны на исследованиях российских и западных (прежде всего американских) учёных при отсутствии своих инноваций[477]. Вместе с тем в отличие от западных авторов, которые фокусируются на наступательной или так называемой «агрессивной» информационной войне России, с заметными обвинениями, критикой и идеологическим подтекстом, исследования китайских учёных о ИО, связанных с Россией, более объективны и нейтральны, охватывая как оборонительные, так и наступательные аспекты российских контрмер к ИО. При рассмотрении активной ИО китайские учёные уделяют больше внимания анализу тактики в конкретных кейсах и в основном дают положительные оценки, рассматривая информационную и гибридную войну как гибкое и умное средство защиты Россией своей национальной безопасности и интереса с использованием асимметричных преимуществ, которое заслуживает постоянного внимания Китая, чтобы извлечь из него полезные опыт и уроки. Другими словами, до СВО в целом китайские учёные считают Россию довольно успешной в использовании

[475]MarkGaleotti. The West is too paranoid about Russia's 'infowar' [Электронный ресурс] // The Moscow Times. 2015.URL:http://connections– qj.org/article/west– too– paranoid– about– russias– infowar (дата обращения: 20.10.2022).
[476] Calabresi M. Inside Russia's Social Media War on America [Электронный ресурс] //Time. 2017. URL: https://time.com/magazine/us/4783906/may-29th-2017-vol-189-no-20-u-s/ (дата обращения: 20.01.2023).
[477] См. подробнее: Го Ф. Гибридная война в исследованиях ученых китайской народной Республики // Гражданин. Выборы. Власть.– 2022. –№ 1(23). –С. 140–151.

комбинации гибридных (прежде всего информационных) операций как оборонительного, так и наступательного характера[478].

Эффективность российских контрмер к ИО также можно проанализировать с точки зрения анализа мощности конкретных применяемых средств. Так, американские аналитики потратили много усилий на исследования эффективности российских ИО с помощью социальных сетей[479], а китайские учёные уделяют пристальное внимание коммуникативной стратегии, в частности использованию СМИ, в арсенале ИО России[480]. В этом плане считается, что после масштабной реорганизации в ряде крупнейших компаний СМИ, в России сформировалась мощная коммуникационная стратегия. В частности, в качестве одного из главных ресурсов цифровой дипломатии и инструмента оказания информационного воздействия на мировой арене «телеканал RT резко выделяется нестандартным контентом»[481], ключевой особенностью телеканала считается «подача информации о мировых событиях под альтернативным углом»[482] на фоне монополии западных СМИ.

---

[478] См. например: Цзя Юаньпей, Сун Цюн. Методы ведения информационных войн Запада против России и российские контрмеры // JournalofJournalismStudies.–2020.–№ 22. –С. 233–234.（贾渊培，宋琼.西方对俄罗斯舆论战方式及其应对策略研究,载《新闻研究导刊》2020 年第 22 期，第 233 至 234 页.）;Хан Кеди. «Гибридная война» России в Украине // Исследование стратегических решений. –2021. –№ 6. – С. 51–80. （韩克敌. 俄罗斯在乌克兰的“混合战争”,载《战略决策研究》2021 年第 6 期，第 51 至 80 页. ）;Гао Кай, Чжао Линь. Гибридная война – новый подход России к стратегической игре// JournalofJournalismStudies. –2019. – № 117. – С. 10–13.（高凯，赵林. “混合战争”— 俄罗斯新战略博弈手段，载《新闻研究导刊》2019 年第 7 期，第 10 至 13 页.）;Шэн Шилян. Как Россия ответила на гибридную войну от США // Военный сборник. –2016. –№ 11. – С.20–23. (盛世良.俄罗斯如何应对美国的 «混合战争» 军事文摘 2016 年第 11 期第 20 至 23 页.);Дуань Цзюньцзе. Практика российской «гибридной войны» и ее последствия // Современные международные отношения. – 2017. – № 3. – С. 31– 36. (段君泽. 俄式"混合战争" 实践及其影响, 载现代国际关系 2017 年第 3 期第 31 至 36 页.)

[479] Treyger E., Cheravitch J, Cohen R.S. Russian Disinformation Efforts on social media [Электронный ресурс]/ / RAND Corporation. 2022. URL: https://www.rand.org/pubs/research_reports/RR4373z2.html (дата обращения: 15.01.2023).

[480] Лю Сяофэн, Ма Цзяньгуан, Лю Янъюэ. Международная коммуникация российских СМИ и национальная безопасность: структура, стратегии, вдохновение // RussianStudies. – 2023. – № 3. – С. 78–100.（刘箫锋,马建光,刘杨钺. 俄罗斯媒体国际传播与国家安全：布局、策略、启示,载《俄罗斯学刊》2022 年第 3 期，第 78 至 100 页.; Тянь Фэнцзюань. Формирование и коммуникация образа российского государства в киберпространстве // Siberian Studies. – 2021. – № 4. – С. 31–48.（田凤娟.俄罗斯国家形象在网络空间的塑造与传播,载《西伯利亚研究》2021 年第 4 期，第 31 至 48 页.; Го Цзиньфэн. Международная коммуникационная стратегия российских СМИ в свете телеканала RT // Современные международные отношения. – 2022. – № 3. – С.52–62. (郭金峰.从 RT 电视台看俄罗斯媒体国际传播战略,载《现代国际关系》 2022 年第 3 期，第 52 至 62 页）.

[481] Толоконникова А. В., Будакова Д. О. Роль телеканала RT в формировании международного имиджа России // Вестник Московского университета. Серия 10: Журналистика. – 2019. – № 5. – С. 89–119.

[482] Там же.

Говоря о достигнутых результатах российских СМИ во главе RT и их роли в информационной борьбе, гендиректор МИА «Россия сегодня» Дмитрий Киселев отметил, что Россия выигрывает информационную борьбу у западных стран, а «то (они) не преследовали бы RT и Sputnik». «Мы выигрываем информационно, и мы более привлекательны по нашим идеям. Мы предоставляем альтернативную информацию по отношению к западному мейнстриму»[483]. К тому же директор Службы внешней разведки РФ Сергей Нарышкин также отметил, что, опираясь на колоссальный опыт действовавшего в СССР агентства печати и информации, агентство эффективно обеспечивает защиту России в информационном пространстве, позволяя непредвзятому читателю понять, что правда на российской стороне: «Доступным и нешаблонным слогом блестящие журналисты АПН рассказывали зарубежной аудитории, чем живёт Советский Союз, по-настоящему творчески и аргументированно доказывали читателю правоту своего государства на фоне информационных нападок на него со стороны западных стран»[484].

Со всеми основаниями можно утверждать, что развитие ведущих СМИ России находится на передовых позициях среди мировых медиа, оптимизируя контент и подстраиваясь под новшества социальных сетей постоянно[485]. Играя важную роль в разрушении гегемонии западного дискурса и формировании благоприятного образа России, государственные СМИ России достигли значительных успехов в информационных противоборствах с Западом. В качестве примера можно привести изменение отношения зарубежной общественности к телеканалу RT: от первоначальной настороженности и критики до постепенных частично положительных отзывов: «Как это ни парадоксально, миссия представить западной публике альтернативный взгляд на происходящее выпала на долю России.

[483]Россия выигрывает информационную борьбу у Запада, заявил Киселев [Электронный ресурс] // РИА НОВОСТЬ. 12.09.2018. URL: https://ria.ru/20180912/1528348402.html (дата обращения: 10.05.2021).
[484]Нарышкин поздравил МИА «Россия сегодня» с 80–летием [Электронный ресурс] // РИА НОВОСТЬ. 2021. URL: https://ria.ru/20210624/yubiley-1738356654.html (дата обращения: 10.05.2021).
[485] Глебов М. С. Элементы и механизмы новой публичной дипломатии во внешней политике государства // Государственное управление. – 2018. – № 68. – С. 275–293.

Наконец, появилось нечто действительно отличное от наших каналов, контролируемых либо правительством, либо крупными корпорациями...»[486].

Однако стоит отметить, что украинский конфликт 2022 года можно считать переломом, проявившим слабость России в информационном противоборстве с противником. Широко известно, что Россия не демонстрирует явные преимущества в ИО в контексте СВО. Так, на Западе считают, что Украина сейчас соперничает с Россией и намного опередила ее в области, в которой Москва считается мировым лидером. В отличие от прошлых ИО Москвы, направленных на укрепление внутренней поддержки власти внутри страны, в сегодняшних конфликтах В. Зеленский руководит чрезвычайно эффективной коммуникационной кампанией, которая оказалась решающей в привлечении глобальной поддержки борьбы Украины против России. Старший научный сотрудник Атлантического совета Шон Макфей считает, что «Россия, возможно, выигрывает войну стрельбой, но Украина выигрывает информационную войну»[487]. В то же время в научно-академическом сообществе Китая также появилось сомнение в эффективности российских ИВ. Однако, в отличие от «азартного» мнения Запада о российском провале в нынешних ИВ с Украиной, китайские аналитики склоны считать, что информационная кампания России в данном конфликте проходит «с большим трудом и ограничениями»[488]. На примере применения самых популярных средств ИВ – СМИ и социальных сетей, можно сказать, что:

---

[486] Баулз У. RussiaToday: СМИ нового образца? [Электронный ресурс] // ИноСМИ. 2011. URL: http://www.inosmi.ru/politic/20110705/171615730.html (дата обращения: 16.10.2022).

[487] Ryan M., Nakashima E., Birnbaumetal M. Outmatched in military might, Ukraine has excelled in the information war [Электронный ресурс] // Washington Post. 2022. URL: https://www.washingtonpost.com/national–security/2022/03/16/ukraine-zelensky-information-war/ (дата обращения: 20.10.2022).

[488] Фань Юнпэн, Хань Циньвэнь. Характеристики и урок информационной войны в российско– украинском конфликте // Форум по стратегии киберпространства.– 2022. – № 6. – С. 76–79. （范勇鹏，韩沁雯.俄乌冲突网络信息战的特征与启示,载《网络空间战略论坛》2022年第6期，第76至79页.; Ян Нинцун. Информационная война в российско– украинском конфликте и её просветительство // Мировые социалистические исследования.– 2022. – № 10. – С. 82–88.（杨柠聪. 俄乌冲突中的信息战及其启示, 载《世界社会主义研究》2022年第10期，第82至88页.; У Фэй, Ли Сюань. Роль СМИ в информационной войне между Россией и США в контексте геополитической борьбы, // Внешняя коммуникация.– 2022. – № 6. – С.72–76.（吴非，李旋. 地缘政治博弈下俄美信息战中的媒体角色, 载《对外传播》2022年第6期，第72至76页.; Лю Цзюнь. Анализ роль социальных сетей в российско– украинский конфликт // Народный форум. –2022. – № 13. – С. 108–111. （刘军. 社交媒体对俄乌冲突的影响分析, 载《人民论文》2022年第13期，第108至111页).

- во-первых, информационная поддержка российских СМИ до и после СВО была недостаточна, слабо согласована со стратегическими целями государства и не смогла привлечь большего понимания международных масс к решению России;

- во-вторых, российские ведущие СМИ почти не в состоянии сопротивляться западным санкциям и блокированию онлайн-платформ, несмотря на разработанную стратегию управления и механизмы реагирования на кризисы в мирное время. После начала СВО России на Украине, вещательные платформы телеканала RT в Великобритании и странах ЕС были заблокированы, при этом ряд западных онлайн-платформ, таких, как Twitter, YouTube и Instagram, объявили об ограничении или запрете аккаунтов российских СМИ. Имея заметные преимущества в технологиях, западные страны превратили медиавойну с Россией в «войну блокирования российских СМИ». Хотя в ответ Россия тоже объявила о блокировании некоторых западных соцсетей (таких как Twitter, Facebook) и СМИ (таких как BBC)[489], подобные действия еще больше отрезают Россию от международного сообщества. Это отражает фундаментальную роль онлайн-платформ в международной коммуникации, что напрямую связано с выражением национального мнения и является «узким местом» национальной безопасности России.

Очевидно, что на данный момент в России разрабатываются эффективные методики для противодействия информационным атакам, но предпринимаемых мер сейчас явно недостаточно. Существует критическая необходимость внедрения новых, эффективных и адекватных мер для повышения эффективности работы по противодействию гибридным угрозам, частью которых являются информационные операции.

[489] В России уже заблокированы Twitter и Facebook [Электронный ресурс] // Super. 2022. URL: https://super.ru/l/socialmediainrussia22 (дата обращения: 10.10.2022); Роскомнадзор уведомил «Яндекс.Музыку» о необходимости удалить подкасты BBC [Электронный ресурс] // RT. 2022. URL: https://russian.rt.com/russia/news/989886-roskomnadzor-podkasty-bi-bi-si (дата обращения: 10.10.2022).

2.5. Практические рекомендации по дальнейшему совершенствованию системы противодействия гибридным войнам в Российской Федерации

С учётом проблемных зон и угроз, реализуемых уже на данном этапе и возможных в будущем, можно предложить приведенные ниже меры для совершенствования работы по противодействию гибридным угрозам, угрожающим национальной безопасности РФ.

В сфере общественных отношений:

1) смягчение внутренних противоречий и обеспечение высокого качества жизни граждан. Острые противоречия внутри общества в России, способные породить стихийное недовольство граждан, являются органическими предпосылками для запуска процесса политической дестабилизации. Как справедливо указал В. Д. Зорькин, «взрывоопасность подобного положения дел наглядно демонстрирует ситуация в Украине (2014 года), где за лежащими на поверхности событий поводами и причинами конфликта, скрывается такой глубинный фактор, как подрыв основ социальной справедливости, обусловленный олигархической структурой экономики»[490]. В этом плане некоторые «узлы критичности» России продолжают вызывать тревогу, в частности, «тенденция снижения уровня жизни населения, сопровождаемого увеличением поляризации некоторых групп общества и социальным расслоением, разрастание масштабов коррупции»[491]. В этой связи «соблюдение социальной справедливости, уважение закрепляемых ею ценностей всеми слоями общества (в частности, политической элитой) является

[490] Зорькин В. Д. Право силы и сила права // Журнал конституционного правосудия. –2015. – № 5. –С. 1–12.
[491] Чепрасов К. В. Создание национальной гвардии как ответ на гибридные вызовы безопасности России // Вопросы безопасности. –2016. –№ 2. – С. 8–19.

основополагающим условием обеспечения национальной безопасности»[492] России в современном хаотизирующемся мире;

2) совершенствование правовой основы и создание единой внутренне согласованной системы нормативно-правовых актов по обеспечению национальной безопасности страны, имеющей строгую иерархию, чтобы утратить существующие разногласия и размывания в трактовке и понимании норм по одному и тому же вопросу. Это обусловлено тем, что, во-первых, действующие концептуальные и правовые документы по этой сфере касаются только отдельных аспектов национальной безопасности, по некоторым важнейшим направлениям отсутствуют необходимые специальные федеральные законы. Так, в России до сих пор нет официального профильного документа по обеспечению кибербезопасности. Во-вторых, в действующей правовой системе наблюдаются разногласия в трактовке и в толковании отдельных норм. Например, в отличие от Концепции национальной безопасности, в Военной доктрине РФ подчёркнуты задачи военной организации по локализации внутренних угроз, в связи с чем отчасти нивелируется главная цель обеспечения военной безопасности – предотвращение, локализация и нейтрализация военных угроз Российской Федерации[493]. Ввиду этого, собственно, считается, что есть необходимость ввести единый систематизированный нормативно-правовой акт по национальной безопасности и по её составляющим. Кстати, такой подход является весьма полезной мерой повышения эффективности государственного управления, что доказывает совсем недавно принятый Закон «О контроле за деятельностью лиц, находящихся под иностранным влиянием», объединяющий основные положения, содержащиеся в различных законах, в единый законодательный акт. Созданный новый департамент по многостороннему гуманитарному сотрудничеству и культурным связям МИД РФ, централизовавший полномочия в сфере применения «мягкой силы», также служит хорошим доказательством этого;

---

[492] Там же.

[493] Усмонова Н. Р. Правовое обеспечение национальной безопасности Российской Федерации // Молодой ученый. – 2018. – № 44 (230). – С. 189–191.

3) создание специальной организации по информационной безопасности, подчинённой напрямую президенту или его ближайшим заместителям. Хотя в существующей организационной системе информационной безопасности уже были подразделения, занимавшиеся данными темами, однако они не специализируются на проведении информационных операций и кибероперациий. Для повышения эффективности противодействия информационным операциям нужен вертикально ориентированный на главу государства орган или структура, которая координировала бы все эти функции правового и организационного обеспечения информационной безопасности в России и могла бы самостоятельно реагировать на информационные атаки в первые же часы их проявления;

4) необходимость совершенствования системы подготовки кадров по противодействию ИО и другим видом гибридных войн. Во всех операциях информационной войны лежит общий принцип – удар по эмоциям, то есть делается заведомо провокационный вброс, способный вызывать у объекта воздействия немедленную ответную реакцию на эмоциях. Когда объект воздействия на эту провокацию ведется, это заканчивается не только дискредитацией его личности, но и, нередко, дискредитацией имиджа всей страны. На любые вбросы надо реагировать мгновенно, но и безошибочно[494]. Однако, к сожалению, специалистов, способных отражать информационные операции Запада, сегодня в России единицы. В связи с этим представляется необходимым ввести знания и компетенции по противодействию информационной агрессии не только в систему подготовки госслужащих, но и в систему высшего образования. В этом ключе замечательно, что некоторые ВУЗы России во главе с МГУ уже совершили первые шаги, создав специализированную программу «Информационные и гибридные войны»;

5) наращивание поддержки к платформам или проектам по противодействию ИО. В эпоху «fake news», которые подрывают доверие и вызывают негативные общественные дискуссии, актуально создать унифицированную платформу, которая может предоставлять качественную и проверенную информацию по ак-

[494] Лебедева О. В. Роль социальных сетей в дипломатической практике России // Международная жизнь. –2021. – № 3. – С. 20–27.

туальным вопросам. Для реализации этой задачи в качестве опорного информационного ресурса может быть задействован специализированный портал «Вбросам. нет»[495], уже работающий по линии публичного разоблачения вредоносных фейков и вбросов. Но, собственно, данная платформа не получает должного внимания со стороны государства;

6) развитие сотрудничества между государственными и частными секторами по противодействию ИВ, в том числе компаниями, общественными объединениями и определёнными влиятельными лицами, в частности лидерами общественного мнения. Например, Шведское агентство по чрезвычайным ситуациям сотрудничает с компаниями социальных сетей, чтобы лучше выявлять информационные операции на их платформах. В этом плане также можно опираться на опыте Пятидневной войны 2008 года, где Южная Осетия с использованием соцсетей, онлайн-форумов и блогов вовлекала большое число своих сторонников в Интернете и одержала заметный верх в ИВ с Грузией, которая «построила свою стратегию ведения информационной войны на официальном уровне и сделала ставку на массовость»[496] в популярных англосаксонских СМИ. Это доказывает, что «использование «массовых информационных армий», ведущих прямой диалог с людьми в Интернете, более эффективно, чем опосредованный диалог руководителей государств с народами мира»[497].

В международной сфере:

1) укрепление сотрудничество между Россий и Китаем в борьбе за международный дискурс и с «цветными революциями». На данный момент отношения между Россией и Китаем находятся на рекордно высоком уровне и стали образцом сотрудничества мировых держав в XXI веке. Тесное сотрудничество между Россией и Китаем является важным фактором стабильности для всего мира. Несмотря на достигнутые результаты в осуществляемых взаимодействиях двух стран, меняющаяся мировая обстановка предъявила новые требования по усиле-

[495] См.: http://www.vbrosam.net/
[496] Колесов П. Информационная война Грузии против Южной Осетии и Абхазии // Зарубежное военное обозрение. – 2008. – No. 10. – С. 18–21.
[497] Там же.

нию сотрудничества двух стран в некоторых актуальных сферах. Прежде всего, выделяется значимость укрепления сотрудничества в борьбе за международное общественное мнение. Обе стороны сталкиваются со схожим давлением со стороны международной общественности из-за участившейся дискредитации и клеветы Запада (во главе с США). Особенно после СВО России в Украине наметилась тенденция «существенной консолидации мировых СМИ в антироссийском ключе при фактическом отсутствии альтернативных мнений»[498]. В этом контексте сугубо оборонительные меры и пассивные ответы на мощные атаки Запада неэффективны, вместо этого обе страны должны инициативно вступать в борьбу с Западом за международный дискурс и изменять неблагоприятное положение для своей страны в плане международного общественного мнения, что требует от двух стран углублять сотрудничество в СМИ, совместно высказываться по актуальным международным вопросам, совместно противостоять демонизации, атакам и проникновению в общественное мнение со стороны внешних сил.

Кроме того, деятельность двух стран по предотвращению «цветных революций» особенно актуальна. В последние годы активизировались усилия по сдерживанию и подавлению России и Китая, США пытались спланировать «цветную революцию» как вокруг России и Китая, так и внутри этих стран. Россия и Китай стали ключевыми целями США по осуществлению «цветных революций». Организуемые «цветные революции» в основном сосредоточены в странах Евразии вокруг Китая и России (например, три классические цветные революции 2003-2005 годов, «зонтичная революция» в Гонконге и т.д.). Следует отметить, что «цветные революции» на периферии России и Китая являются лишь «разминкой», а Россия и Китай – конечные мишени США и их союзников[499]. Таким образом, Китаю и России необходимо совместно противостоять угрозам «цветных революций». При этом Китай и Россия также могут наращивать совестную работу в рамках СНГ и ШОС, ШОС и ОДКБ, чтобы объединить страны Евразии в единое целое и совместно противостоять указанным и другим угрозам;

[498] Чепрасов К. В. Создание национальной гвардии как ответ на гибридные вызовы безопасности России // Вопросы безопасности. – 2016. – № 2. – С. 8–19.
[499] Соловей В. Д. «Цветные революции» и России. Сравнительная политика. – 2011(1). – С. 33–43.

2) формирование единого пространства коллективного противодействия гибридным угрозам, в частности, информационным, в рамках международных интегративных организаций с участием России, таких как БРИКС, ШОС, ЕАЭС и др. Сложность и глобальность современных гибридных угроз обусловила то, что с ними каждая страна в отдельности не справится. «При любых обстоятельствах следует поддерживать коммуникацию, проводить более взвешенную политику и дипломатию»[500]. С учётом того, что для всех участников БРИКС существует общая потребность в противодействии транснациональным кибер- и информационным атакам, идущим от зарубежных противников и конкурентов, создание единого информационного пространства коллективной безопасности стран БРИКС должно стать одной из самых актуальных и востребованных в российской внешнеполитической стратегии. В качестве одного из конкретных направлений для реализации данной идеи можно создать в БРИКС собственную систему наднациональных органов, отвечающих за обеспечение информационной безопасности объединения в целом с использованием опыта создания и функционирования соответствующих наднациональных органов ЕС[501].

[500] Штоль В. В., Задохин А. Г. США – истоки и пределы американского империализма // Обозреватель–Observer. – 2018. – № 7. – С. 13.
[501] Манойло А. В., Стригунов К. С. Технологии неклассической войны. Генезис. Эволюция. Практика.– М.: Горячая линия – Телеком, 2020. – С. 322.

Выводы по главе II.

Национальная безопасность Российской Федерации сталкивается с широким спектром гибридных угроз, что требует системного подхода для противодействия им. При исследовании российского опыта по противодействию гибридным угрозам анализируются как её ключевые меры во внутренней политике, так и основные направления внешнего сотрудничества по совместному разрешению гибридных угроз. Внешняя политика России в данной сфере основана на продвижении повестки международной информационной безопасности, в этом ключе значительные сдвиги достигнуты как на постсоветском пространстве, так и в рамках различных переговорных площадок, в частности, ШОС и ООН. Во внутренней политике для организации работы по противодействию гибридным угрозам предпринимаются следующие комплексные меры: совершенствование нормативно-правовой и организационной системы, разработка целенаправленных программ и планов, реализация конкретных образовательных, культурных и других мер в сферах общества и др. Отмечается, что публикация серии законов об иноагентах является важным аспектом сокращения иностранного влияния.

В разделе, специально посвящённом вопросам противодействия информационным операциям, раскрыты правовая основа и силы по обеспечению информационной безопасности. Отмечается, что в системе государственного управления России в сфере информационной безопасности закрепилась ведущая роль «силовых» структур. Боевые силы российских ИО состоят из трех типов акторов, при этом большинство осуществлённых ИО слабо организованно и делегировано

широкому кругу субъектов, некоторые из которых тесно связаны с командной цепочкой, другие связаны с государственными органами гораздо менее прочно.

Российский подход к «информационной безопасности» имеет большие различия с подходом коллективного Запада. В российском восприятии выделяется «двойственность» – ИО рассматривают в России как угрозу безопасности режима и эффективное оружие в борьбе с противниками России, что стало основой принятия мер по противодействию ИО. В целом ответные меры России на ИО можно разделить на два крупных вида – оборонительные и наступательные. Российские контрмеры к ИО также состоят из нескольких звеньев: производства контента, распространения контента по каналам ОТКС и потребления контента целевой аудиторией. Эффективность российских контрмер к ИО США и их союзников можно анализировать со следующих точек зрения: 1) конкретных кейсов по ИВ; 2) оценок или мнений представителей в данной области исследования; 3) применяемых конкретных средств в ИВ. Отмечаем, что на данный момент в России разрабатываются эффективные методики для противодействия информационным атакам, но предпринимаемых мер сейчас явно недостаточно. Существует критическая необходимость внедрения новых, эффективных и адекватных мер для совершенствования работы по противодействию гибридным угрозам. При этом украинский конфликт 2022 года можно считать переломным моментом, проявившим недостатки России в информационном противоборстве с противником. В отношении проблемных зон и угроз, реализуемых уже на данном этапе и возможных в будущем, даны рекомендации по увеличению эффективности работы по данному направлению, как с точки зрения российского пространства, так и в аспекте международного сотрудничества.

Заключение

Нарастающая турбулентность мировой политики и международных отношений привела к революции в концепциях и технологиях международного противоборства, в частности, на передний план выдвинулись несиловые методы борьбы, объединившиеся под общим собирательным названием неклассических войн. Для корректного описания таких изменений в новой политической реальности был выдвинут ряд новых концепций – таких, как «управляемый хаос», «неограниченная война» и т.п. Интегрировав различные концепции подобного рода под одним «зонтичным брендом», гибридная война стала адекватно описывать облик современной международной системы отношений в ее конфликтном измерении и раскрыла, настолько расширился инструментарий агрессивного воздействия на противника.

Современные гибридные войны представляют сложное конвергентное явление и выражаются в комплексном использовании широкого набора сил и средств борьбы, в основном невоенных, объединённых единым замыслом и согласованных по целям, задачам, методам и инструментам воздействия на противника. Целью таких войн, как правило, становится продвижение собственных национальных интересов в сфере международных отношений и соперничества между государствами за ресурсы, смыслы и влияние.

В отличие от классических войн, гибридные войны имеют ряд значительных преимуществ: скрытость, многообразие инструментария, полифилия, высокий уровень адаптивности её участников и т.д., что делает сегодня эту форму вооруженной борьбы, доминирующей в сфере международных отношений.

Как чрезвычайно широкая по охвату «зонтичная» концепция, «гибридная война» описывает сложное и многогранное явление в современных международных отношениях, продолжая в научном плане оставаться предметом для дискуссий. В целом, отношение к данному термину разделяется на два типа: в широком

смысле гибридных войн включает как классические военные конфликты, так и различные невоенные противоборства; в узком смысле к гибридным войным относят борьбу с комплексным использованием невоенных средств, что отличает ее от традиционного вооружённого конфликта. У большинства российских исследователей термин «гибридная война» воспринимается чаще всего в широком смысле. Однако анализ последних выступлений официальных представителей России в контексте СВО позволяет утверждать, что в дискурсе российской власти «гибридная война» используется в узком смысле.

В зависимости от содержимого фокуса исследования существующие источники по данной теме классифицированы автором на два типа. Первый тип (в теоретическом плане) посвящён теоретической дискуссии, в частности, сосредоточен на том, в какой степени новая теория ознаменовала собой перелом в военной мысли, какова связь межу теорией гибридных войн и традиционными представлениями о войне. Второй тип исследований (в практическом плане) рассматривает, как новые идеи влияют на государственную политику и реализованы на практике, в частности, в международных противоборствах. К тому же, по отношению к феномену «гибридной войны» современные научные подходы представлены двумя крупными течениями, или школами: консервативной и новаторской, каждый из которых включает в себя две платформы: умеренную и радикальную.

Проведённый сравнительный анализ о подходах Запада (прежде всего США и НАТО), России и Китая к феномену «гибридной войны» позволил выяснить, что теория гибридных войн в России имеет более широкую философско-теоретическую базу, чем на Западе, последний обращает больше внимание на практическое использование данной концепции неклассических войн. Вместе с тем к одному и тому же, по сути, феномену, китайский подход выделяется собственной спецификой. Китай играет роль наблюдателя бурной дискуссии России и Запада по тематике гибридных войн, фокусируясь на сущности, отражённой в феномене гибридных войн и практическом использовании так называемой технологии гибридных войн. А сама теория гибридных войн не приобрела до сих

пор такую популярность как в России и Западе, ведь у Китая сформировалась и развивается своя теоретическая система в процессе осмысления новых изменений в ситуациях международных конфликтов и безопасности, которая выходит за рамки российской и западной теории гибридных войн. В отличие от теории гибридных войн, подчёркивающей «внешние силы» и «угрозы», китайская теория по международной ситуации и национальной безопасности имеет яркую китайскую специфику со строгой и чёткой логикой, сосредоточенной на «внутреннем управлении» и «безопасности».

При этом мировой опыт по противодействию гибридным угрозам и войнам, в частности, опыт НАТО, а также китайский опыт по совершенствованию системы обеспечения общей национальной безопасности под руководством «Всеобъемлющей концепцией национальной безопасности» (ВКНБ), дают определенные и весьма полезные уроки для других стран, включая Россию.

В современных гибридных войнах используется широкий диапазон инструментов, в основном, невоенных, таких, как информационно-психологические операции, кибератаки, экономические инструменты давления и блокады и т.п. При этом неотъемлемой составляющей в структуре гибридных войн остаётся её военная часть, использование которой все чаще осуществляется в форме сплава традиционных общевойсковых или специальных военных операций с креативными формами и методами ведения боевых действий, осуществляемыми некомбатантами – повстанцами, диверсантами, боевиками организованных преступных группировок (ОПГ) и организованного преступного сообщества (ОПС), боевиками частных военных компаний (ЧВК) и «гражданских армий» (милиционных ополчений) и т.д. Вместе с тем все большее значение приобретает внедрение робототехники и различных форм дистанционной войны, а также технологий ИИ, что следует рассматривать как объективную тенденцию.

Большое разнообразие «гибридных» форм и методов вооруженной и невооружённой борьбы, а также методов и технологий противодействия гибридным войнам требует их точного учёта и классификации. В том числе, особое внимание стоит уделять её информационной составляющей (информационным

войнам/информационным операциям), представляющей собой основу современных гибридных войн. В этом ключе автором (с учетом специфики современных гибридных войн) дополнена разработанная ранее А. В. Манойло модель стандартной схемы западной информационной операции. К тому же, на основе анализа складывающейся ситуации в международной конкуренции и борьбе автор сделал прогноз относительно перспектив развития стратегии и тактики гибридных войн, отмечая, что в будущем так назвыаемая «битва за мозг» противника с большой степенью вероятности станет главной и приоритетной целью любой гибридной войны.

Триада ценности современных теорий гибридных войн заключается в том, что:

1) интегрировав различные концепции подобного рода под одним «зонтичным брендом», данный неологизм отличается неограниченной инклюзивностью и адаптивностью и стал «терминатором» различных концепций в современных международных противоборствах;

2) данный термин адекватно описывает облик современной международной системы отношений в ее конфликтном измерении и раскрывает, настолько расширился инструментарий агрессивного воздействия на противника. Ценность данной концепции выросла в глазах международных и региональных держав и организаций, которые рассматривают гибридные войны как удобное средство для анализа сегодняшних международных конкурентов и противоборств и выработки предметных планов;

3) Гибридная война стала главным инструментом современной международной борьбы, и их распространение формирует новый мировой ландшафт. Гибридные войны могут стать состоянием существования международной системы в ближайшем будущем.

Все это обусловило то, что феномен гибридных войн будет сохранять свое долгосрочное присутствие, при этом давно созрела возможность для России перейти от теоретической дискуссии на стратегическое и тактическое применение технологий гибридных войн.

Национальная безопасность Российской Федерации сталкивается с широким спектром гибридных угроз, как с традиционными вооружёнными конфликтами, так и с новыми угрозами, при этом всё большей угрозой становятся кибернетические и информационные атаки, диверсии, эрозия традиционных духовно-нравственных ценностей и цветные революции, что требует системного подхода для противодействия им. В сложившихся условиях наиболее активными методами гибридных войн США и их союзников против России является военное, экономическое и информационно-психологическое давление.

Меры по противодействию гибридным угрозам и войнам, применяемые Российской Федерацией, раскрываются автором на двух уровнях: первый, когда Россия действует самостоятельно, а второй, когда Россия действует, кооперируясь с другими странами в форме двухстороннего и многостороннего сотрудничества. Соответственно, анализируются как ключевые меры во внутренней политике России, так и основные направления внешнего сотрудничества по совместному разрешению гибридных угроз.

Во внутренней политике для организации работы по противодействию гибридным угрозам предпринимаются следующие комплексные меры: совершенствование нормативно-правовой и организационной системы, разработка целенаправленных программ и планов, реализация конкретных образовательных, культурных и других мер в сферах общества.

Отмечается, что в России сформирована эффективная система правовых норм по обеспечению национальной безопасности, в частности, принятие серии «Законов об иноагентах» стало эффективным средством сокращения иностранного влияния путём ужесточения контроля над деятельностью иностранных организаций и их «агентов» на территории России. Однако действующие концептуальные и правовые документы по обеспечению национальной безопасности касаются только отдельных аспектов гибридных угроз, по некоторым важнейшим направлениям отсутствуют необходимые специальные федеральные законы. Так, в России до сих пор нет официального профильного документа по обеспечению кибербезопасности. К тому же, в действующей правовой системе наблюдаются

разногласия в трактовке и в толковании отдельных норм. Ввиду этого, есть необходимость совершенствовать правовую основу и ввести единую внутренне согласованную систему нормативно-правовых актов по обеспечению национальной безопасности страны в сфере гибридных войн, имеющей строгую иерархию, чтобы утратить существующие разногласия и размывания в трактовке и понимании норм по одному и тому же вопросу.

В организационном аспекте, несмотря на достаточно консервативный характер структуры «силового блока», всё равно произошла существенная трансформация правоохранительной системы страны в виде переоформления и учреждения ряда специализированных органов, призванных реагировать на гибридные угрозы. Хотя в существующей системе власти образовались министерства и подразделения с полномочиями противодействия отдельным аспектам гибридных войн , тем не менее, до сих пор нет органа, который бы «централизовал» их и замкнул на себя, при этом согласованность действий всех звеньев соответствующих структур недостаточна, что снижает эффективность работы на этом направлении.

Для укрепления легитимности политического режима в условиях перекрёстного давления со стороны внутренней несистемной оппозиции и внешних оппонентов России российское руководство видит выход в опоре на патриотические идеологемы, возводя политику защиты исторической памяти в ранг государственной стратегической задачи, для реализации которой были образованы различные профильные организации и ускорена работа по ведению единого «переосмысленного» учебника истории для школьников. Реализация образовательных программ по противодействию гибридныы войнам также является важным шагом на этом направлении.

Во внешнеполитическом сотрудничестве по противодействию гибридным угрозам и войнам особое внимание уделяется двустороннему сотрудничеству с Беларусью и Китаем и многостороннему сотрудничеству в рамках ОДКБ, СНГ, ЕАЭС, ШОС и ООН. Отмечается, что на площадках постсоветского пространства приоритетным направлением взаимодействия членов этих интеграционных

объединений стало коллективное реагирование на вооружённые конфликты, вместе с тем наблюдается тенденция оживления их функций по организации совестной борьбы с новыми угрозами и вызовами. Стоит также отметить, что внешняя политика России в данной сфере основана на продвижении повестки международной информационной безопасности, в этом ключе значительные сдвиги достигнуты как на постсоветском пространстве, так и в рамках различных переговорных площадок, в частности, ШОС и ООН.

В разделе, отдельно посвящённом вопросу о противодействии Российской Федерации ИО иностранных государств, анализируются правовая основа, организационная структура и сила обеспечения информационной безопасности РФ, раскрыты схемы проведения ИО и контроопераций. Отмечается, что в системе государственного управления России в сфере информационной безопасности закрепилась ведущая роль силовых структур.

Установлено, что боевые силы российских ИО состоят из трех типов акторов: государственные акторы, зависимые от государства акторы и независимые от государства акторы, при этом большинство осуществлённых ИО слабо организовано и делегировано широкому кругу субъектов, некоторые из которых тесно связаны с командной цепочкой, другие связаны с государственными органами гораздо менее прочно.

Российские методы по противодействию ИО базируются на восприятии Россией данного феномена. В связи с этим, прежде чем раскрыть меры в ответ на ИО со стороны Российской Федерации, сначала подробно проанализированы особенности российского подхода к феномену «информационного противоборства». Проведен сравнительный анализ понятий, тесно связанных с «информационным противоборством» в российском и западном представлении, в том числе – «информационных операций», «информационной безопасности» и «информационного суверенитета». Указано, что российский подход к ИО имеет большие различия с подходом так называемого «коллективного Запада». Российское правительство понимает информационный суверенитет как нераспространение «вредоносной» иностранной информации среди российских граждан и обмен «соот-

ветствующей информацией о России» с иностранными партнёрами. Соответственно, Россия выступает за усиление государственного контроля над информацией, что подвергается острой критике на Западе, который воспринимает такой подход как угрозу политической стабильности демократических стран. Вместе с тем ИО в России стали широкоохватывающим понятием, включающим широкий диапазон деятельности, включая преднамеренные, систематические попытки формировать восприятие, манипулировать когнациями и направлять поведение для достижения реакции, которая способствует желаемым намерениям их инициатора. В российском восприятии выделяется двойственность – ИО рассматривают в России как угрозу безопасности режима и, одновременно, как эффективное оружие в борьбе с противниками России.

Параллельно с модернизацией представлений о вышесказанных явлениях, развивается и боеспособность российских сил ИО. Предполагается, что рост боеспособности ИО современной России начался после «первой чеченской войны» 1994 года, когда российские военные фактически проиграли информационную войну чеченским сепаратистам. К началу «Евромайдана» 2014 года технологии и боевые силы России по ведению информационно-психологических операций (ИПО) претерпели качественное изменение, Россия стала менять ситуацию в ИО в свою пользу.

В результате синергии теории и практики в сфере ИО, в России укрепился подход к информационной войне, в котором ИО рассматриваются как «оружие» для сохранения статуса великой державы и внутриполитической стабильности:

- во-первых, российское руководство и элиты, как политические, так и военные, проецируют важное положение России в мире с помощью российских информационных операций;

- во-вторых, повышается сплочённость российского общества с помощью подчёркивания или даже преувеличения угроз информационных операций «недружественных» государств-агрессоров (переключение внимания с внутренних конфликтов на внешние угрозы);

- в-третьих, достаточно просто узаконивать при этом новые меры по усилению контроля государством над общественным мнением и потоками информации.

Далее раскрыты стратегия и основная цель ИВ, ведущаяся США против России, и применяемые ими формы и методы ИО. Отмечается, что основная цель ИВ Запада против современной России заключается в осуществлении контроля над ней путём организации цветной революции, с помощью которой проамериканские силы получат абсолютное господство в российском правительстве. В контексте СВО структура ИО, проводимых США в отношении России, состоит из четырёх ярусов: стратегические ИО, оперативные игры, фейки и спецпропаганда. Первые три формы ведения ИВ являются типичными в практике США в их противостоянии современной России в информационной сфере, а спецпропаганда, давно известная еще со времён «холодной войны» форма информационной борьбы, начинает с началом СВО доминировать.

Всё вышесказанное представляет собой основу и предпосылки для принятия мер Российской Федерацией по противодействию ИО. На этой основе российские контрмеры в ответ на ИО рассмотрены автором с двух точек зрения.

С одной точки зрения, российские методы по противодействию ИО базируются на её восприятии «двойственности» данного феномена – ИО как угрозы национальной безопасности и как оружия защиты государственных интересов. Соответственно, ответные меры России на ИО Запада делится на два крупных вида – оборонительные и наступательные. Оборонительные контрмеры включают в себя меры по уничтожению или нейтрализации эффекта злонамеренных ИО противника в отношении своей стороны с целью защиты безопасности собственной инфраструктуры киберпространства и своего информационного суверенитета от враждебных посягательств. Наступательные контрмеры к ИО также можно назвать превентивными контрмерами, то есть, на основе существующего опыта или при получении «сигнала» о потенциальном информационном нападении противника цель таких ИО – нанести удар на упреждение. В отличие от вышеописанных контрмер защитного характера, данный тип операций носит наступа-

тельный характер и дает возможность вскрыть и пресечь враждебную деятельность на самой ранней стадии ее возникновения, заставить противника действовать в невыгодных условиях. К нему можно отнести: кибероперации, операции по коррекции восприятия и активные мероприятия спецслужб.

С другой точки зрения, анализируются российские контрмеры, направленные на три звена жизненного цикла информации: производства контента, распространения контента по каналам ОТКС и потребления контента целевой аудиторией.

К тому же, автор полагает, что в информационном противоборстве с США и их союзниками Россия придерживается следующего основного принципа: информационная безопасность неотделима от национальной безопасности, для обеспечения которой необходимо комбинировать оборонительные и наступательные подходы и осуществлять достойные контратаки асимметричными средствами.

Эффективность российских контрмер к ИО США и их союзников оценена со следующих точек зрения: 1) конкретных кейсов по ИВ; 2) оценок или мнений ученых и представителей экспертных организаций в данной области исследования; 3) применяемых конкретных средств в ИВ. Установлено, что на данный момент в России разрабатываются эффективные методики для противодействия информационным атакам, но предпринимаемых мер сейчас явно недостаточно. В этом плане, украинский конфликт 2022 г. можно считать переломным моментом, проявившим недостатки России в информационном противоборстве с противником. Существует критическая необходимость внедрения новых, эффективных и адекватных мер для повышения эффективности работы по противодействию гибридным угрозам, частью которых являются ИО.

В отношении проблемных зон и угроз, реализуемых уже на данном этапе и возможных в будущем, даны рекомендации по увеличению эффективности работы по данному направлению, как с точки зрения российского пространства, так и в аспекте международного сотрудничества.

Перечень сокращений и условных обозначений

№	Аббревиатура	Расшифровка
1	ГОУ	Главное оперативное управление
2	ГРУ	Главное разведывательное управление
3	ГУ ГШ	Главное управление Генерального штаба Вооружённых сил Российской Федерации
4	ЕАЭС	Евразийский экономический союз
5	ИИ	Искусственный интеллект
6	ИКТ	Информационно-коммуникационные технологии
7	ИО	Информационные операции
8	ИПВ	Информационно-психологическаявойна
9	МИБ	Международная информационная безопасность
10	ОБДЭ	«операции, базирующиеся на достижении эффектов» (англ. effects-based operations)
11	ОДКБ	Организации Договора о коллективной безопасности
12	ОПГ	Организованные преступные группировки
13	ОПС	Организованного Преступного Сообщества
14	ОТКС	Открытая информационно-телекоммуникационная сеть
15	РИО	Российское историческое общество
16	СНБ	Совет национальной безопасности США (англ. National Security Council, NSC)
17	ЦИП	Центр информационного противоборства
18	ЦРУ	Центральное разведывательное управление США (Central Intelligence Agency, CIA)
19	ЧВК	Частные военные компании
20	IRA	Internet Research Agency

Библиография

Официальные документы и нормативные правовые акты

1. Выступление Главы государства Касым-Жомарта Токаева на внеочередной сессии Совета коллективной безопасности ОДКБ. Текст : электронный. // Официальный сайт Президента Республики Казахстан. 2022. URL: https://akorda.kz/ru/vystuplenie-glavy-gosudarstva-kasym-zhomarta-kemelevicha-na-vneocherednoy-sessii-soveta-kollektivnoy-bezopasnosti-odkb-1002245 (дата обращения 11.10.2022).
2. Выступление Министра иностранных дел Российской Федерации С. В. Лаврова на Совещании с постоянными членами Совета Безопасности Российской Федерации. Текст : электронный. // МИД РФ. 2023. URL: https://www.mid.ru/tv/?id-1861005&lang-ru (дата обращения: 20.04.2023).
3. Выступление Президента РФ В. В. Путина на встрече с делегатами Всероссийской конференции преподавателей гуманитарных и общественных наук 21 июня 2007 г. // Преподавание истории в школе. 2007. № 6. С. 4-7. – Текст : непосредственный.
4. Выступление пресс-секретаря МИД КНР Хуа Чуньин на пресс-конференции 26 марта 2021 года. Текст : электронный. // Embassy of the People’s Republic of China in the Democratic Socialist Republic of Sri Lanka. 2021. URL: http://lk.china-embassy.org/fyrth/202103/t20210326_8909867.htm (дата обращения: 06.03.2022)(2021 年 3 月 26 日外交部发言人华春莹主持例行记者会 //中华人民共和国驻斯里兰卡民主主义社会共和国大使馆.26.03.2021. URL: http://lk.china-embassy.org/fyrth/202103/t20210326_8909867.htm).
5. Выступление Си Цзиньпина при встрече с участниками-посланниками в ежегодной рабочей конференции для посланников за рубежом 2017 года Текст :

электронный. // Центральное народное правительство КНР. 2017. URL: http://www.gov.cn/xinwen/2017-12/28/content_5251251.htm (дата обращения 28.01.2023)(习近平接见 2017 年度驻外使节工作会议与会使节并发表重要讲话 // 中华人民共和国中央人民政府. 2017 年 12 月 28 日) .

6. Декларация глав государств Шанхайской организации сотрудничества. Текст : электронный. // Центральное народное правительство КНР. 2005 URL: http://www.gov.cn/gongbao/content/2005/content_64324.htm (дата обращения 20. 08. 2022) (《上海合作组织成员国元首宣言》// 中华人民共和国中央人民政府官网. 2005 年 7 月 5 日).
7. Декларация по случаю пятой годовщины Шанхайской организации сотрудничества государств Шанхайской организации сотрудничествТекст : электронный. // Официальный сайт МИД КНР. 2006. URL: https://www.fmprc.gov.cn/chn/pds/ziliao/1179/t346575.htm (дата обращения 20.08.2022) (《上海合作组织五周年宣言》 // 中华人民共和国外交部官网. 2006 年 6 月 15 日).
8. Договор от 8 декабря 1999 года о создании союзного государстваТекст : электронный. // Посольство Республики Беларусь в Российской Федерации. 1999. URL:https://russia.mfa.gov.by/ru/bilateral_relations/sojuz/legal_acts/a8c7dec6793bf47e.html (дата обращения: 15.09.2022).
9. Доктрина информационной безопасности Российской Федерации Текст : электронный. // Контур Норматив. 2000. URL: https://normativ.kontur.ru/document? moduleId=1&documentId=40613 (дата обращения: 20.09.2022).
10. Доктрина информационной безопасности Российской Федерации Текст : электронный. // Российская газета. 2016. URL: https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 20.10.2022).
11. Екатеринбургская декларация глав государств – членов Шанхайской организации сотрудничества Текст : электронный. // Президента России. 2009. URL:

http: //archive.kremlin.ru/text/docs/2009/06/217868.shtml (дата обращения 11.10.2022).

12. Заявление по итогам встречи на высшем уровне в ВаршавеТекст : электронный. // NATO. 2016. URL: http://www.nato.int/cps/en/natohq/official_texts_133169.htm (дата обращения: 12.07.2022).
13. Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В. В. Путиным 31 марта 2023 г.) Текст : электронный. // МИД РФ . 2023. URL: https://www.mid.ru/ru/detail-material-page/1860586/ (дата обращения: 20.04.2023).
14. Об итогах организационной сессии Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025 Текст : электронный. // МИД РФ.2021. URL: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1423780/(дата обращения 13.10.2022).
15. Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря Текст : электронный. // МИД РФ. 2015. URL: https://www.mid.ru/upload/iblock/507/50773c33e891c2b04c4a1e795eed9470.pdf (дата обращения 11.10.2022).
16. Об инициативе стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности» Текст : электронный. // МИД РФ . 2015. URL: https://www.mid.ru/ru/foreign_policy/news/1582268/?lang=ru (дата обращения 11.10.2022).
17. Совместное заявление Президента Российской Федерации и Председателя Китайской Народной Республики о взаимодействии в области развития ин-

формационного пространства Текст : электронный. // Президент России. 2016. URL: http://www.kremlin.ru/supplement/5099 (дата обращения 15.09.2022).

18. Стенографический отчёт о встрече с разработчиками концепции нового учебно-методического комплекса по отечественной истории Текст : электронный. // Президент России. 2014. URL: http://www.kremlin.ru/events/president/news/20071 (дата обращения: 20.10.2022).
19. Стратегии национальной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 02.07.2021 г. № 400 Текст : электронный. // Президент России . 2021. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 20.09.2022).
20. Стратегии национальной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 31.12.2015 г. № 683 Текст: электронный. // Президент России. 2015. URL: http://www.kremlin.ru/acts/bank/40391 (дата обращения: 20.09.2022).
21. Стратегия национальной безопасности Российской Федерации до 2020 года Текст : электронный. // Президент России. 2009. URL: http://www.kremlin.ru/supplement/424 (дата обращения: 25.10.2022).
22. Строим лучший мир вместе — К 10-летию идеи Председателя КНР Си Цзиньпина о создании Сообщества человеческой судьбы Текст : электронный. // Центральное народное правительство КН . 2023. URL: http://www.gov.cn/xinwen/2023-03/23/content_5747952.htm (дата обращения 28.01.2023) (携手建设更加美好的世界—写在习近平主席提出构建人类命运共同体理念十周年之际 // 中华人民共和国中央人民政府.2023年3月23日).
23. Указ О Комиссии при Президенте Российской Федерации по противодействию попыткам фальсификации истории в Ущерб интересам России Текст : электронный. // Президент России. 2009. URL: http://www.kremlin.ru/acts/bank/29288 (дата обращения: 20.10.2022).

24. Указ о мерах по повышению эффективности деятельности государственных СМИ Текст : электронный. // Президент России. 2013. URL: http://www.kremlin.ru/events/president/news/19805 (дата обращения: 20.09.2022).
25. Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» Текст: электронный. // Президент России. 2021. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 25.10.2022).
26. Указ Президента Российской Федерации от 05.02.2010 г. №146, О Военной доктрине Российской Федерации Текст: электронный. // Президента России. 2010. URL: http://www.kremlin.ru/acts/bank/30593 (дата обращения: 01.10.2022).
27. Указ Президента Российской Федерации от 20.05.2022 № 295 «О внесении изменений в Указ Президента Российской Федерации от 11 июля 2004 г. № 865 «Вопросы Министерства иностранных дел Российской Федерации и в Положение, утвержденное этим Указом» Текст: электронный. // Официальный интернет-портал правовой информации. 2022. URL:https://news.ru/world/v-mid-rf-poyavitsya-departament-myagkoj-sily/(дата обращения: 10.11.2022).
28. Указ Президента РФ от 5 апреля 2016 № 157 «Вопросы Федеральной службы войск национальной гвардии Российской Федерации» Текст: электронный. // Президент России. 2016. URL: http://www.kremlin.ru/acts/ bank/40689 (дата обращения: 20.09.2022).
29. Федеральный закон от 14.07.2022 г. № 255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием» Текст: электронный. // Президент России. 2022 г. URL: http://kremlin.ru/acts/bank/ 48170 (дата обращения: 01.112022).
30. Федеральный закон от 2 декабря 2019 г. N 426-ФЗ «О внесении и изменений в Закон Российской Федерации “О средствах массовой информации» и Федеральный закон «Об информации, информационных технологиях и о защите

информации» Текст : электронный. // Президент России . 2019. URL: http://www.kremlin.ru/acts/bank/44875 (дата обращения: 01.10.2022).

31. Федеральный закон от 20.07. 2012 г. №121-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента» Текст : электронный. // Президент России . 2012. URL: http://kremlin.ru/acts/bank/35748 (дата обращения: 01.10.2022).
32. Федеральный закон от 23.05.2015 г. № 129-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»Текст : электронный. // Президент России . 2015. URL: http:// kremlin.ru/acts/ bank/ 39720 (дата обращения: 01.10.2022).
33. Федеральный закон от 24.11.2014 № 355-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросу финансовой отчётности политических партий, избирательных объединений, кандидатов на выборах в органы государственной власти и органы местного самоуправления» Текст : электронный. // Президент России . 2014. URL: http://www.kremlin.ru/acts/bank/39075 (дата обращения: 20.10.2022).
34. Федеральный закон от 25 ноября 2017 года№ 327-ФЗ «О внесении изменений в статьи 10.4 и 15.3 Федерального закона “Об информации, информационных технологиях и о защите информации” и статью 6 Закона Российской Федерации “О средствах массовой информации» Текст : электронный. // Президент России . 2017. URL: http://www.kremlin.ru/acts/bank/42487 (дата обращения: 01.10.2022).
35. ФСБ России совместно с КГБ Республики Беларусь пресечена противоправная деятельность граждан Республики Беларусь Зянковича Юрия Леонидовича и Федуты Александра Иосифовича， планировавших осуществление военного переворота в Белоруссии Текст : электронный. // ФСБ РФ . 2021. URL: http://www.fsb.ru/fsb/press/message/single.htm%
21id%3D10439220%40fsbMessage.html (дата обращения: 15.09.2022).

36. Assessing Russian Activities and Intentions in Recent US Elections Текст : электронный. // Office of the Director of National Intelligence . 2017. URL: https://www.dni.gov/files/documents/ICA_2017_01.pdf (Дата обращения: (10.02.2023).
37. FY 2021 Congressional Budget Justification Текст : электронный. // U.S. Agency for Global Media. 2020. URL: https://www.usagm.gov/wp-content/uploads/2020/02/FINAL-USAGM-FY-2021-Congressional-Budget-Justification_2_9_2020.pdf (дата обращения: 12.07.2022).
38. FY 23 NDAA Agreement Executive Summary Текст : электронный. // United States Senate Armed Services Committee on armed services . 2022. URL: https://www.armed-services.senate.gov/imo/media/doc/fy23_ndaa_ agree-ment_summary.pdf (дата обращения: 06.02.2023).
39. Joint Statement on Hong Kong Текст : электронный. // U.S. Department of State . 2021. URL: https://www.state.gov/joint-statement-on-hong-kong/ (дата обраще-ния: 06.12.2021).
40. Joint statement on human rights situation in Xinjiang at 47th Session of UN Hu-man Rights Council Текст : электронный. // the Government of Canada . 2021. URL: https://www.international.gc.ca/world-monde/ international_relations-relations_internationales/un-onu/statements-declarations/2021-06-22-statement-declaration.aspx?lang=eng (дата обращения: 06.12.2021).
41. President Dwight D. Eisenhower's Farewell Address Текст : электронный. // Na-tional Archives . 1961. URL: https://www.archives.gov/ -documents/president-dwight-d-eisenhowers-farewell-address (дата обращения: 25.01.2023).
42. Quadrennial Defense Review Report February 2010 Текст : электронный. // The U.S. Department of Defense . 2019. URL: https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf (дата обращения: 05.04.2022).
43. SecretaryGeneral’sAnnualReport 2015Текст : электронный. // NATO . 2016. URL: http://www. nato.int/nato_static_fl2014/assets/pdf/pdf_

2016_01/20160128_SG_AnnualReport_2015_en.pdf (дата обращения: 20.01.2021).

44. The National Defense Strategy of the United States of America. – Washington, D.C.: U.S. Department of Defense, 2005.– 24 p.
45. ARMY PLANNING. Comprehensive Risk Assessment Needed for Planned Changes to the Army's Force Structure Текст : электронный. // USGAO . 2016. URL: http://www.globalsecurity.org/military/library/report/gao/ 676516.pdf (дата обращения 28.07.2022);
46. Hybrid Warfare, GAO-10-1036R Текст : электронный. // USGAO . 2010. URL: http://www.globalsecurity.org/military/library/ report/gao/d101036r.pdf (дата обращения 28.07.2022).
47. NATO's military presence in the east of the Alliance Текст : электронный. // NATO . 2022. URL: nato.int/cps/en/natohq/topics_136388.htm (дата обращения: 25.01.2023).
48. U.S. Joint Chiefs Staff. Joint Operations. Join Publication 3-0 Текст : электронный. // U.S. Department of Defense . 2006.(Incorporating Change 1, 2008). URL: https://www.bits.de/NRANEU/others/jp-doctrine/jp3_0%2808ch1%29.pdf (дата обращения: 05.04.2022).
49. U.S., Russia, China and Pakistan Joint Statement on Peace in Afghanistan Текст : электронный. // U.S. Department of State . 2019. URL: https://ru.usembassy.gov/u-s-russia-china-and-pakistan-joint-statement-on-peace-in-afghanistan/ (дата обращения 15.08.2022).
50. Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales Текст : электронный. // NATO . 2014. URL: http://www.nato.int/cps/en/natohq/ official_texts_112964.htm (дата обращения: 20.01.2021).
51. WarsawSummitCommuniqué Текст : электронный. // NATO . 2016. URL: http://www.nato.int/cps/en/natohq/official_texts_133169.htm (дата обращения: 02.10.2021).

Монографии и отдельные издания

52. Арзуманян, Р. В. Стратегия иррегулярной войны: теория и практика применения. Теоретические и стратегические проблемы концептуализации, религиозные и военно-политические отношения в операционной среде иррегулярных военных действий / Р. В. Арзуманян; под общ. ред. А. Б. Михайловского. – М.: АНО ЦСОиП, 2015. – 334 с. – Текст : непосредственный.

53. Арский, Ф. Перикл. Жизнь замечательных людей / Ф. Арский. – М.: Молодая гвардия, 1971. – 220 с.– Текст : непосредственный.

54. Багдасарян, В. Э. Россия – Запад: цивилизационная война / В. Э. Багдасарян. – М.: Форум, 2017. – 410 с. – Текст : непосредственный.

55. Бартош, А. А. Вопросы теории гибридной войны / А. А. Бартош. – М.: Горячая линия –Телеком, 2023. – 324 с. – Текст : непосредственный.

56. Бартош, А. А. Конфликты XXI века. Гибридная война и цветная революция / А. А. Бартош. – М.: Горячая линия –Телеком, 2020. – 281 с. – Текст : непосредственный.

57. Бартош, А. А. Театры гибридной войны / А. А. Бартош. – М.: Горячая линия – Телеком, 2022. – 356 с. – Текст : непосредственный.

58. Бартош, А. А. Туман гибридной войны. Неопределённости и риски конфликтов современности / А. А. Бартош. – М.: Горячая линия – Телеком, 2019. – 324 с. – Текст : непосредственный.

59. Буренок, В. М. Национальная безопасность России в эпоху сетевых войн / В. М. Буренок, Е. В. Горгола , С. Ф. Викулов. – М.: Граница, 2015. – 190 с.– Текст : непосредственный.

60. Буренок, В. М. Развитие военных технологий XXI века: проблемы планирование, реализация / В. М. Буренок, А. А. Ивлев, В. Ю. Корчак. – М.: Тверь: Купол, 2009. – 623 с. – Текст : непосредственный.

61. Зюганов, Г. А. Россия под прицелом глобализма / Г. А. Зюганов. – М.: Эксмо, 2018. – 382 с. – Текст : непосредственный.

62. Иншаков, С. М. Гибридная война в системе военных угроз национальной безопасности / С. М. Иншаков. – М.: КноРус, 2018. – 312 с. – Текст : непосредственный.

63. Клаузевиц, К. О войне / К. Клаузевиц. – М.: Госвоениздат, 1934. – 692 с. – Текст : непосредственный.

64. Крысько, В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / В. Г. Крысько. – Минск: Харвест, 1999. – 446 с. – Текст : непосредственный.

65. Лепский В. Е. Методологический и философский анализ проблематики управления / В. Е. Лепский. – М.: Когито-Центр. 2019. – 340 с. – Текст : непосредственный.

66. Ма, Цзяньгуан. Откровение сирийской войны / Цзяньгуан Ма. –У Хань, 2017. – 272 с. (马建光. 《叙利亚战争启示录》，长江文艺出版社，2017 年,272 页) – Текст : непосредственный.

67. Манойло, А. В. Государственная информационная политика в условиях информационно-психологической войны. 4-е изд., перераб. и доп. / А. В. Манойло, А. И. Петренко, Д. Б. Фролов – М.: Горячая линия – Телеком, 2021. – 635 с. – Текст : непосредственный.

68. Манойло, А. В. Информационные войны и психологические операции. Руководство к действию / А. В. Манойло. – М.: Горячая линия – Телеком, 2020. – 495 с. – Текст : непосредственный.

69. Манойло, А. В. Технологии неклассической войны. Генезис. Эволюция. Практика / А. В. Манойло, К. С. Стригунов. –М.: Горячая линия– Телеком., 2020.– 378 с. – Текст : непосредственный.

70. Манойло, А. В. Технологии несилового разрешения современных конфликтов / А. В. Манойло. – М.: Горячая линия – Телеком, 2015. – 392 с. – Текст : непосредственный.

71. Месснер, Е. Э. Всемирная мятежевойна / Е. Э. Месснер. – М.: Жуковский: Кучково поле, 2004. – 511 с. – Текст : непосредственный.

72. Най, Дж. Гибкая сила. Как добиться успеха в мировой политике / Дж. Най. – М.: Тренд, 2006. – 397 с. – Текст : непосредственный.

73. Панарин, И. Н. Гибридная война и передел мира / И. Н. Панарин. – М.: Горячая линия –Телеком, 2022. – 274 с. – Текст : непосредственный.
74. Панарин, И. Н. Гибридная война против России (1816-2016 гг.) / И. Н. Панарин. – М.: Горячая линия Телеком, 2016. – 221 с. – Текст : непосредственный.
75. Панарин, И. Н. Гибридная война. Теория и практика / И. Н. Панарин. – М.: Горячая линия –Телеком, 2022. – 402 с. – Текст : непосредственный.
76. Панарин, И. Н. Информационная война и власть / И. Н. Панарин. – М.: мир безопасности, 2001. – 223 с. – Текст : непосредственный.
77. Панарин, И. Н. Информационная война и коммуникации / И. Н. Панарин. – М.: Горячая линия – Телеком, 2018. – 233 с. – Текст : непосредственный.
78. Панарин, И. Н. Первая мировая информационная война. Развал СССР / И. Н. Панарин. – М.: Санкт-Петербург [и др.]: Питер, 2010. – 253 с. – Текст : непосредственный.
79. Панарин, И. Н. Технология информационной войны / И. Н. Панарин. – М.: КСП+, 2003. – 320 с. – Текст : непосредственный.
80. Партийная школа ЦК КПК. Основные вопросы по идеям Си Цзиньпина о социализме с китайской спецификой в новой эпохе. – Пекин: издательство «Партийная школа ЦК КПК», Народное издательство, 2020. – 433 с.（中共中央党校：《习近平新时代中国特色社会主义思想基本问题》，北京:中共中央党校出版社；人民出版社，2020，433 页).– Текст : непосредственный.
81. Петренко, А. И. Информационно-психологическая война как инструмент политического воздействия / А. И. Петренко. – М.: МИФИ, 2003. – 228 с. – Текст : непосредственный.
82. Почепцов, Г. Г. Информационные войны. Новый инструмент политики / Г. Г. Почепцов . – М.: Алгоритм, 2015. – 256 с. – Текст : непосредственный.
83. Прокопенко, И. С. Злые мифы о России. Что о нас говорят на Западе? / И. С. Прокопенко. – М.: Эксмо, 2016. – 288 с. – Текст : непосредственный.
84. Психология масс: хрестоматия / ред.-сост. Д. Я. Райгородский. – М.: Самара: Бахрах, 2006. – 591 с. – Текст : непосредственный.

85. Пушкарев, Н. ГРУ: вымысли и реальность / Н. Пушкарев. – М: Яуза: Эксмо, 2004. – 382 с. – Текст : непосредственный.

86. Расторгуев, С. П. Формула информационной войны / С. П. Расторгуев. – М.: Вузовская книга, 1999. – 222 с. – Текст : непосредственный.

87. Рожков, И. Я. Имидж России. Ресурсы. Опыт. Приоритеты / И. Я. Рожков, В. Г. Кисмерешкин . – М.: РИПОЛ классик, 2008. – 366 с. – Текст : непосредственный.

88. Российско-китайский диалог: модель 2020: доклад / С. Г. Лузянин (рук.), Х. Чжао (рук.) [и др.] . – М.: НП РСМД. 2020. – 254 с. – Текст : непосредственный.

89. Снесарев, А.Е. Философия войны / А.Е. Снесарев. – М.: Ломоносовъ. 2013. – 283 с. – Текст : непосредственный.

90. Союзное государство Белоруси и России. От сообщества к построению единого государства / под. ред. Г. А. Рапоты，Р. А. Курбанова. – М.: Юнити-Дана，2017. – 667 с. – Текст : непосредственный.

91. Сунь, Цзы. Искусство войны / Цзы Сунь; пер. с древнекит. Н. Кондрата. – М.: АСТ，2018. – 192 с. – Текст : непосредственный.

92. Устинова, М. Новые термины на русском языке. Глоссарий конфликтологических терминов / М. Устинова. – М.: Каллиграф, 2008. – 96 с. – Текст : непосредственный.

93. Филимонов, Г. Ю. Культурно-информационные механизмы внешней политики США. Истоки и новая реальность / Г. Ю. Филимонов. – М.: РУДН, 2012. – 408 с. – Текст : непосредственный.

94. Цыганков, П. А. Гибридные войны в хаотизирующемся мире XXI века: сборник / Цыганков П. А. [и др.]; под редакцией. П. А. Цыганкова. – М: Издательство Московского университета，2015. – 384 с. – Текст : непосредственный.

95. Шагов, А.Е. «Гибридная война» и «Гибридные угрозы» в зарубежной военно-исторической науке / А.Е. Шагов. – М.: Мир науки, 2023. – 147 с. – Текст : непосредственный.

96. Шагов, А.Е. История происхождения и эволюция концепции и методов ведения гибридной войны / А.Е. Шагов. – М.: Мир науки, 2022. – 155 с. – Текст : непосредственный.

97. Шарп, Дж. От диктатуры к демократии: Стратегия и тактика освобождения / Дж. Шарп; пер. с англ. Н. Козловской.– М.: Новое издательство, 2005. – 84 с. – Текст : непосредственный.

98. Шеллинг, Т. Стратегия конфликта / Т. Шеллинг. – М.: ИРИСЭН, Социум. 2014. – 369 с. – Текст : непосредственный.

99. Arquilla, J. The emergence of noopolitik. Toward an American information strategy / J. Arquilla, D. Ronfeldt. – Santa Monica, 1999. 102 p. – Текст : непосредственный.

100. Boot, M. Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present / M. Boot. – N.Y.: W.W. Norton, 2013. – 750 p. – Текст : непосредственный.

101. Borenstein, E. Plots against Russia: Conspiracy and Fantasy After Socialism / E. Borenstein. – Cornell University Press, 2019. – 306 c. – Текст : непосредственный.

102. Brzezinski Z. Out of Control: Global Turmoil on the Eve of the 21st Century / Z. Brzezinski. – New York: Scribner Cop, 1993. – 240 c. – Текст : непосредственный.

103. Callwell, E. Small Wars: Their Theory and Practice of Irregular Warfare / E. Callwell. – CreateSpace Independent Publishing Platform, 2016. – 438 p. – Текст : непосредственный.

104. Charap, S. Everyone Loses: The Ukraine Crisis and the Ruinous Contest for Post-Soviet Eurasia / S. Charap, T. J. Colton. – New York: Routledge for the Intern. inst. for strategic studies, 2017. – 211 p. – Текст : непосредственный.

105. Davis, J.R. The hybrid mindset and operationalizing innovation: toward a thoery of hybrid: SAMS Monograph / J.R. Davis. – Fort Leavenworth (Kansas). 2014. – 81 p. – Текст : непосредственный.

106. Deptula D. A. Effects-Based Operations: Change in the Nature of Warfare / David A. Deptula. – Arlington VA: Aerospace Education Foundation. Defense and Airpower Series, 2001. – 41 p. – Текст : непосредственный.

107. Galeotti, M. Russian Political War: moving beyond the hybrid / M. Galeotti. – London: Routledge, 2019. – 136 p. – Текст : непосредственный.

108. Giles K. Handbook of Russian Information Warfare / K. Giles. – Rome, Italy: NATO Defense College, 2016. – 90 p. – Текст : непосредственный.

109. Herman, M. Intelligence Power in Peace and War / M. Herman. – Cambridge: Cambridge University Press, 1996. – 414 p. – Текст : непосредственный.

110. Hoffman, F. Conflict in the 21st Century: The rise of Hybrid War / F. Hoffman. – Potomac Institute for Policy Studies, 2007. – 72 p. – Текст : непосредственный.

111. Korybko, A. Hybrid wars: The indirect adaptive approach to regime change / A. Korybko. – Moscow Peoples' Friendship University of Russia, 2015. – 128 p. – Текст : непосредственный.

112. Liang, Q. Unrestricted warfare / Q. Liang, W. Xiangsui. – Beijing: PLA Literature and Arts Publishing House Arts, 1999. FBIS Translated Text. – 228 p. – Текст : непосредственный.

113. Libicki, M. C. What is Information Warfare? / M.C. Libicki. – Washington: National defense university, 1995. – 104 p. – Текст : непосредственный.

114. Libicki, M.C. Conquest in cyberspace. National security and information warfare / M.C. Libicki. – Cambridge, 2007. – 337 p. – Текст : непосредственный.

115. Mumford, A. Proxy Warfare / A. Mumford. – Cambridge: Polity Press, 2013. – 180 p. – Текст : непосредственный.

116. Pain, E. The Second Chechen War: The Information Component / E. Pain; translated by Robert R. Love. – Fort Leavenworth: Foreign Military Studies Office, 2000. – 300 p. – Текст : непосредственный.

117. Rickerman, L.D. Effects-Based Operations: A New Way of Thinking and Fighting / L. D. Rickerman. . – Fort Leavenworth, KS: School of Advanced Military Studies,

Army Command and General Staff College, 2003. 48 p. – Текст : непосредственный.

118. Russia Military Power: Building a Military to Support Great Power Aspirations. – Defense Intelligence Agency (Washington, D. C.), 2017. – 116 p. – Текст : непосредственный.

119. Sharp, G. Exploring Nonviolent Alternatives / G. Sharp. – Boston: Porter Sargent, 1970. – 162 p. – Текст : непосредственный.

120. Sharp, G. Social Power and Political Freedom / G. Sharp. – Boston,1980. – 440 p. – Текст : непосредственный.

121. Sharp, G. The Politics of Nonviolent Action, Vol. 2: The Methods of Nonviolent Action / G. Sharp. – Boston: Porter Sargent Publishers,1973. – 368 p. – Текст : непосредственный.

122. Smart Sanctions: Targeting Economic Statecraft / D. Cortright, G.A. Lopez, J. Stephanides [et al.]. – New York: Rowman & Littlefield, 2002. – 256 p. – Текст : непосредственный.

123. Soldatov, A. The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries / A. Soldatov, I. Borogan. – New York: Public Affairs, 2015. – 384 p. – Текст : непосредственный.

124. Szafranski, R. Neocortical warfare? The acme of skill / R. Szafranski // Athena's camp. Preparing for conflict in the information age. Ed. by J. Arquilla, D. Ronfeldt. – Santa Monica, 1997. – 405 p. – Текст : непосредственный.

125. The Military Balance 2015. – Oxfordshire: Routledge for International Institute for Strategic Studies, 2015. – 504 p. – Текст : непосредственный.

126. Whittingham, D. Warrior-Scholarship in the Age of Colonial Warfare: Charles E. Callwell and small wars / D. Whittingham // The Theory and Practice of Irregular Warfare: Warrior-Scholarship in Counter-Insurgency / A. Mumford, B. C. Reis (eds). – London: Routledge, 2013. – 176 p. – Текст : непосредственный.

127. Yablokov, I. Fortress Russia: Conspiracy Theories in Post-Soviet Russia / I. Yablokov. – Medford: MA; Polity, 2018. – 288 p. – Текст : непосредственный.

128. Zarate, J. Treasury's War. The Unleashing of a New Era of Financial Warfare. Public Affairs / J. Zarate. – New York, 2013. – 512 p. – Текст : непосредственный.

Статьи в научных периодических печатных изданиях и сборниках

129. Антонович, П. Ключевые аспекты информационной войны / П. Антонович // Армейский сборник. – 2014. – No. 1. – С. 26-30. – Текст : непосредственный.

130. Арбатов, А. Г. Украинский кризис и стратегическая стабильность / А. Г. Арбатов. // Полис. Политические исследования. – 2022. – № 4. – С. 10-31. – Текст : непосредственный.

131. Барабаш, Н. С. Оценка уровня вовлеченности пользователей в радикальные группы в социальных сетях / Н. С. Барабаш, Д. С. Жуков // Инноватика и экспертиза: научные труды. – 2019. – № 3 (28). – С. 113-122. – Текст : непосредственный.

132. Бартош, А. А. Адаптивные стратегии информационной войны (часть 1) / А. А. Бартош // Вестник Академии военных наук. – 2016. – № 2(55). – С. 85-93. – Текст : непосредственный.

133. Бартош, А. А. Гибридная война как возможный катализатор глобального конфликта / А. А. Бартош // Вопросы безопасности. – 2016. – № 4. – С. 41-53. – Текст : непосредственный.

134. Бартош, А. А. Модель гибридной войны / А. А. Бартош // Военная мысль. – 2019. – № 5. – С. 6-23. – Текст : непосредственный.

135. Бартош, А. А. Модель управляемого хаоса в культурно-мировоззренческой сфере / А. А. Бартош // Вестник Московского государственного лингвистического университета. – 2014. –Выпуск. 39. – С. 9-27. – Текст : непосредственный.

136. Бартош, А. А. Стратегия и контрстратегия гибридной войны / А. А. Бартош// Военная мысль. – 2018. – №10. – С. 5-20. – Текст : непосредственный.

137. Бартош, А. А. Трансформация современных конфликтов / А. А. Бартош // Вопросы безопасности.– 2018. – № 1. – С. 1-18. – Текст : непосредственный.

138. Бахтин, Ю. К. Патриотическое воспитание как основа формирования нравственно здоровой личности / Ю. К. Бахтин // Молодой учёный. – 2014. –№ 10 (69). – С. 349-352. – Текст : непосредственный.

139. Белозёров, В. К. Гибридная война в отечественном политическом и научном дискурсе / В. К. Белозёров, А. В. Соловьёв // Власть. – 2015. – №9.–С. 5-11. – Текст : непосредственный.

140. Бирюков, Е. Этапы и инструменты внешней политики США на Ближнем Востоке / Е. Бирюков // Международная жизнь. – 2016. – №11. – С. 85-104. – Текст : непосредственный.

141. Болотов, Н. Н. Россия и Запад: на фронтах информационной войны вокруг событий в Сирии / Н. Н. Болотов // Информационные войны. – 2017. – №3(43). – С. 36-42. – Текст : непосредственный.

142. Бурцева, С. Б. Анализ атаки на «мягкую силу» в условиях информационной операции / С. Б. Бурцева // Вестник Московского государственного областного университета. – 2020. – № 4. – Текст : непосредственный.

143. Ван, Баофу. Гибридная война: новая форма эволюции войны / Баофу Ван // Guangming Daily. – 2016. – №11.(王宝付.《混合战争：战争演进的新形态》，载《光明日报》2016 年 04 月 06 日第 11 版). – Текст : непосредственный.

144. Ван, Сяоцзюнь. Анализ восприятия и применения доктрины «гибридной войны» российской армией / Сяоцзюнь Ван // Современная война. – 2016. – № 8. (王晓军.《解析俄军对“混合战争”理论的认知与运用》，《现代军事》,2016 年第 8 期)– Текст : непосредственный.

145. Василенко, И. А. Модель управляемого хаоса / И. А. Василенко // Наш Современник. – 2003. – №7. – Текст : непосредственный.

146. Василенко, И. Формирование нового образа России «после Крыма»: парадоксы информационной войны / И. Василенко // Власть. – 2014. –№ 10. – С. 207-208. – Текст : непосредственный.

147. Гао, Кай. Гибридная война – новый подход России к стратегической игре / К. Гао, Л. Чжао // Journal of Journalism Studies. 2019.№ 117. С. 10-13.（高凯，赵

林. “混合战争”— 俄罗斯新战略博弈手段，载《新闻研究导刊》2019年第7期，第10至13页）. – Текст : непосредственный.

148. Гареев, М. А. Характер будущих войн / М. А. Гареев // Право и безопасность. – 2003. – № 1-2. – С. 23-31. – Текст : непосредственный.

149. Глебов, М. С. Элементы и механизмы новой публичной дипломатии во внешней политике государства / М. С. Глебов // Государственное управление. – 2018. – № 68. – С. 275-293. – Текст : непосредственный.

150. Го, Фэнли. Гибридная война в исследованиях ученых китайской народной республики / Ф. Го // Гражданин. Выборы. Власть .– 2022. – № 1(23). – С. 140-152. – Текст : непосредственный.

151. Го, Фэнли. Особенность противодействия информационным операциям со стороны Российской Федерации / Ф. Го // Вопросы национальных и федеративных отношений. – 2023. – Т. 13. – № 6 (99). – С. 2554-2560. – Текст : непосредственный. – Текст : непосредственный.

152. Го Фэнли. Российский подход к информационному противоборству / Ф. Го // Вопросы политологии. – 2023. – Т. 13. – № 3 (91). – С. 1253-1260. – Текст : непосредственный.

153. Го, Фэнли. Гибридная война США и их союзников против России в контексте специальной военной операции / Ф. Го // Гражданин. Выборы. Власть. – 2023. – № 2 (28). – С. 146-155. – Текст : непосредственный.

154. Го, Фэнли. Гибридная война США и их союзников против России в контексте специальной военной операции / Ф. Го // Гражданин. Выборы. Власть. – 2023. – № 2 (28). – С. 146-155. – Текст : непосредственный.

155. Го, Фэнли, Манойло, А.В. Торговая война США против Китая в период президентского правления Д. Трампа как составляющая современных гибридных войн / Ф. Го, А.В. Манойло // Вестник Московского университета. Серия 12. Политические науки. –2022. – № 5. – С. 81-92. – Текст : непосредственный.

156. Го, Ц. Международная коммуникационная стратегия российских СМИ в свете телеканала RT / Ц. Го // Современные международные отношения. 2022. №

3. С. 52-62.(郭金峰.从 RT 电视台看俄罗斯媒体国际传播战略,载《现代国际关系》 2022 年第 3 期，第 52 至 62 页）. – Текст : непосредственный.

157. Григорьев, Ю. П. Антироссийские информационные войны / Ю. П. Григорьев // Россия: тенденции и перспективы развития. – 2015. – Выпуск 10.– Часть I. – С. 255-259. – Текст : непосредственный.

158. Гузь, Е. Школьный учебник по истории в условиях трансформации государственной образовательной политики рубежа xx–xxi вв. / Е. Гузь // История. – 2019.1 (21). – С. 114-115. – Текст : непосредственный.

159. Гэ, С. Теория гибридной войны США / С. Гэ, С. Сюй // Национальные оборонные технологии. – 2011. – № 1.(葛向宇、许向东.《美军更趋务实的混合战争理论》,国防科技,2011 年第 1 期).– Текст : непосредственный.

160. Дорохов, В. Л. О совершенствовании территориальной обороны с учётом особенностей гибридных войн / В. Л. Дорохов, А. И. Петрушин, Г. А. Никоноров // Военная мысль. – 2009. – № 12. – С. 39-47. – Текст : непосредственный.

161. Дробинин, А. Ю. Основные тенденции мирового развития и внешняя политика Российской Федерации / А. Ю. Дробинин // Дипломатическая служба. – 2023. – №1. – С. 7-8. – Текст : непосредственный.

162. Дуань, Ц. Практика российской «гибридной войны» и ее последствия / Ц. Дуань // Современные международные отношения. – 2017. – № 3. – С.31-36.(段君泽. 俄式“混合战争”实践及其影响, 载现代国际关系 2017 年第 3 期第 31 至 36 页). – Текст : непосредственный.

163. Евдокимов, А. М. Об активных информационных мероприятиях на южном стратегическом направлении / А. М. Евдокимов // Защита и безопасность. – 2010. – № 4(55). – С. 25-27. – Текст : непосредственный.

164. Евстафьев, Д. Г. Генезис современных цветных революций (на примере Венесуэлы и Белоруссии) / Д. Г. Евстафьев, А. В. Манойло // Дипломатическая служба. – 2021. – № 1. – Текст : непосредственный.

165. Евстафьев, Д. Г. Гибридные войны в контексте постглобализации / Д. Г. Евстафьев, А. В. Манойло // Контуры глобальных трансформаций: политика, экономика, право. – 2021. – Том 14, №4. – С. 332-347. – Текст : непосредственный.

166. Евстафьев, Д. Г. Информационные войны и психологические операции как базис гибридных войн нового поколения / Д. Г. Евстафьев, А. В. Манойло // История. – 2021. –Т. 12. – Выпуск 6 (104). – Текст : непосредственный.

167. Егорченков, Д. А. Теоретико-идеологические подходы к исследованию феномена «гибридных войн» и «гибридных угроз»: взгляд из России / Д. А. Егорченков, Н. С. Данюк // Вестник Московского университета. Серия 12: Политические науки. – 2018. – № 1. – С. 26-48. – Текст : непосредственный.

168. Западная Европа как фронт гибридной войны / И. А. Анапских [и др.] // Юридическая наука: история и современность. – 2020. – № 12. – С. 164-188. – Текст : непосредственный.

169. Золотухин, В.М. К вопросу о природе и сущности гибридной войны в современном мире: философско-культурологический аспект / В. М. Золотухин, Г. Е. Логинова // Вестник Кемеровского государственногоуниверситетакультурыиискусств. – 2017. – № 41. – Ч. I. – С. 99-104. – Текст : непосредственный.

170. Зорькин, В. Д. Право силы и сила права / В. Д. Зорькин // Журнал конституционного правосудия. – 2015. – № 5. – С. 1-12. – Текст : непосредственный.

171. Калдор, М. Культура новых войн / М. Калдор // Логос. – 2019. – Т. 29, № 3(130). – С. 1-21. – Текст : непосредственный.

172. Капицын, В. М. Состоятельность современного государства в условиях нарастающих прокси-войн / В. М. Капицын // Социально-гуманитарные знания. – 2019. – № 4. – С. 117-120. – Текст : непосредственный.

173. Капканщиков, С. Г. Гибридная война как угроза экономической безопасности России, и санкции как ее ведущий инструмент / С. Г. Капканщиков, С. В. Капканщикова // Национальные интересы: приоритеты и безопасность. – 2018. – Т. 14, № 6. – С. 1044-1059. – Текст : непосредственный.

174. Клименко, С. Теория и практика ведения «Гибридных войн» (по взглядам НАТО) 2015» / С. Клименко // Зарубежное военное обозрение. – 2015. – № 5. – С. 109-112. – Текст : непосредственный.

175. Колесников, Д. И. К проблеме сущности и специфики гибридной войны / Д. И. Колесников, А. М. Кривенко // Военный академический журнал. – 2020. – № 1 (25). – С. 110–114. – Текст : непосредственный.

176. Колесов, П. Информационная война Грузии против Южной Осетии и Абхазии / П. Колесов // Зарубежное военное обозрение. – 2008. – No. 10. – С. 18-21. – Текст : непосредственный.

177. Котляр, В. С. К вопросу о «гибридной войне» и о том, кто же ее ведёт на Украине / В. С. Котляр // Международная жизнь. – 2015. – № 8. – С. 57–72. – Текст : непосредственный.

178. Красовская, О. В. Информационная война как коммуникативный феномен / О. В. Красовская // Политическая лингвистика. – 2016. – № 4 (58). – С. 53-59. – Текст : непосредственный.

179. Круглов, В. В. Анализ взглядов военных теоретиков ведущих зарубежных государств на содержание и ведение современных и будущих войн /В. В. Круглов , В. Г. Воскресенский, В. Я. Мурсаметов // Военная мысль. – 2021. – № 7. – С. 120–129. – Текст : непосредственный.

180. Крылова, И. А. Информационные войны и безопасность России / И. А. Крылова // Россия: тенденции и перспективы развития. – 2016. – Выпуск 11. – Часть Ⅱ. – С. 116-121. – Текст : непосредственный.

181. Лебедева, М. М. «Мягкая сила»: понятие и подходы / М. М. Лебедева // Вестник МГИМО. – 2017. – №3 (54). – С. 212-223. – Текст : непосредственный.

182. Лебедева, О. В. Роль социальных сетей в дипломатической практике России / О. В. Лебедева // Международная жизнь. – 2021. – № 3. – С. 20-27. – Текст : непосредственный.

183. Лепский, В. Е. Технологии управляемого хаоса – оружие разрушения субъектности развития / В. Е. Лепский // Информационная война. – 2010.– №4 (16). – С. 69-78. – Текст : непосредственный.

184. Ли, Шуйинь. Стремление России к гибридной войне / Шуйинь Ли // PLA Daily. – 2016. – № 7.(李抒音.《俄罗斯发力混合战争》,解放军报, 2016 年第 007 版）.– Текст : непосредственный.

185. Ли, Юаньбин. Экстремальное давление США и цветная революция в рамках гибридной войны / Юаньбин Ли, Хаочэнь Хэ // Military Digest. – 2019. – № 9. (李元斌、何昊宸. 混合战争视角下的美国极限施压与“颜色革命”,军事文摘，2019 年第 9 期). – Текст : непосредственный.

186. Лю, Сяофэн. Международная коммуникация российских СМИ и национальная безопасность: структура, стратегии, вдохновение / Сяофэн Лю, Цзяньгуан Ма, Янъюэ Лю // RussianStudies.– 2023. – №3. – С. 78–100.（刘箫锋,马建光,刘杨钺. 俄罗斯媒体国际传播与国家安全：布局、策略、启示,载《俄罗斯学刊》2022 年第 3 期，第 78 至 100 页）.– Текст : непосредственный.

187. Лю, Цзюнь. Анализ роль социальных сетей в российско-украинский конфликт / Цзюнь Лю // Народный форум. – 2022. – № 13. – С. 108-111.（刘军. 社交媒体对俄乌冲突的影响分析, 载《人民论文》2022年第13期，第108至111页）.– Текст : непосредственный.

188. Ма, Цзяньгуан. Гибридная война и её характеристики: анализ с точки зрения российских учёных / Цзяньгуан Ма, Юаньбин Ли // Исследованиях по России, Восточной Европе и Центральной Азии. – 2021. – № 5. – С. 21-36.（马建光、李元斌. 《“混合战争”及其特点：俄罗斯学者视角的解析》，载《俄罗斯东欧中亚研究》2021 年第 5 期，第 21-36 页）. – Текст : непосредственный.

189. Манойло, А. В. «Гибридная дипломатия»: о подготовке кадров в сфере противодействиясовременным информационным и гибридным войнам / А. В. Манойло // Дипломатическая служба. – 2023. – № 2. – С. 130-139.– Текст : непосредственный.

190. Манойло, А. В. Гибридизация современной мировой политики и национальная безопасность Российской Федерации / А. В. Манойло // Геополитический журнал. – 2017. – № 1 (17). – С. 3-20. – Текст : непосредственный.

191. Манойло, А. В. Гибридные войны в контексте постглобализации / А. В. Манойло, Д. Г. Евстафьев // Контуры глобальных трансформаций: политика, экономика, право. – 2021. – Т. 14, № 4. – С. 160-175. – Текст : непосредственный.

192. Манойло, А. В. Гибридные войны и цветные революции в мировой политике / А. В. Манойло // Право и политика. – 2015. – № 7. – С. 918-929. – Текст : непосредственный.

193. Манойло, А. В. Дело Скрипалей как операция информационной войны / А. В. Манойло // Вестник Московского государственного областного университета (электронный журнал). – 2019. – № 1. – С. 72-97. – Текст : непосредственный.

194. Манойло, А. В. Информационная война и новая политическая реальность (I) / А. В. Манойло // Вестник Московского государственного областного университета (электронный журнал). – 2021. – № 1. – Текст : непосредственный.

195. Манойло, А. В. Информационная война и новая политическая реальность: Ч. II / А. В. Манойло // Вестник МГОУ. Электронный журнал. Серия Политология. –2021. – № 2. – С. 110-148. – Текст : непосредственный.

196. Манойло, А. В. Информационные диверсии в конфликте на Украине / А. В. Манойло // Вестник МГОУ. – 2022. – № 4. – Текст : непосредственный.

197. Манойло, А. В. Операция «Гедеон»: успех венесуэльских или американских спецслужб? / А. В. Манойло, К. С. Стригунов // Международная жизнь. – 2020. – №11. – С. 64-79. – Текст : непосредственный.

198. Манойло, А. В. Современная практика информационных войн и психологических операций. Вирусные технологии и эпидемии каскадного типа на примере операции по разоблачению агента влияния ЦРУ, бывшего вице-президента Венесуэлы Диосдадо Кабельо 17-21/08/2019/ А. В. Манойло // Национална сигурност. 2019. № 3. С. 3-8. – Текст : непосредственный.

199. Манойло, А. В. Современные информационно-психологические операции: технологии и методы противодействия / А. В. Манойло, Е. Г. Пономарева // Обозреватель. – 2019. – № 2. – С. 5-17. – Текст : непосредственный.

200. Манойло, А. В. Цветные революции и проблемы демонтажа политических режимов в меняющемся мире / А. В. Манойло // Вестник МГОУ. – 2014. – № 2. – С. 1-14. – Текст : непосредственный.

201. Матвиенко, Ю. А. «Цветные» революции как невоенных способ достижения политических целей в «гибридной» войне: сущность, содержание, возможные меры защиты и противодействия / Ю. А. Матвиенко // Информационные войны. – 2016. – №4(40). – С. 11-19. – Текст : непосредственный.

202. Модестов, С. А. Байты вместо пуль / С. Модестов, С. Сокут // Независимое военное обозрение. –1999. – No. 13. – Текст : непосредственный.

203. Модестов, С. А. США готовы к информационной войне с Россией / С. А. Модестов // Независимое военное обозрение. –1997. – No. 25. – Текст : непосредственный.

204. Назаров, В. П. Проблемы развития общей теории национальной безопасности в контексте корректировки Стратегии национальной безопасности Российской Федерации / В. П. Назаров, Д. А. Афиногенов // Власть. – 2020. – Том 28, № 1. – С. 9-19. – Текст : непосредственный.

205. Небренчин, С. М. Современные гибридные войны: медиасмыслы, технологии, стратегии / С. М. Небренчин // Большая Евразия: развитие, безопасность, сотрудничество. – 2022. – С. 240-242. – Текст : непосредственный.

206. Несмеянов, В. Эта тихая смертельная война / В. Несмеянов // Флаг Родины. – 2017. – № 10. – Текст : непосредственный.

207. Николайчук, И. А. О сущности гибридной войны в контексте современной военно-политической ситуации / И. А. Николайчук // Проблемы национальной стратегии (РИСИ). – 2016. – № 3 (36). – С. 85-104. – Текст : непосредственный.

208. Обухова, Т. В. Некоторые вопросы противодействия осуществлению деятельности на территории Российской Федерации иностранной или международной неправительственной организации, в отношении которой принято решение о признании нежелательной на территории Российской Федерации её

деятельности / Т. В. Обухова // Вестник Санкт-Петербургского университета МВД России. – 2019. –No1(81). – С. 121-127. – Текст : непосредственный.

209. Овчинников, В. В. Информационное противоборство в современной геополитике / В. В. Овчинников, М. П. Новиков // Защита и безопасность. – 2011. – № 2. – С. 10-11. – Текст : непосредственный.

210. Першин, Ю. Ю. Записки о «гибридной войне» / Ю. Ю. Першин // Вопросы безопасности. – 2016. – №4. – С. 63-85. – Текст : непосредственный.

211. Погорельская, А. М. Противодействие нетрадиционным угрозам безопасности на постсоветском пространстве / А. М. Погорельская // Евразия. Эксперт. – 2020. – № 1-2. – С. 47-53. – Текст : непосредственный.

212. Пономарева, Е. Г. «Цветные революции» в контексте стратегии управляемого хаоса / Е. Г. Пономарева, Е. В. Рябинин // Обозреватель. – 2015. – № 12. – С. 38-51. – Текст : непосредственный.

213. Пушкина, М. А. Теория современных гибридных войн / М.А. Пушкина, П. С. Чирков // Аллея науки. – 2017. – Т. 2, № 8. – С. 629-642. – Текст : непосредственный.

214. Романова, В. А. Информационная составляющая гибридных войн современности / В. А. Романова // Государственное и муниципальное управление. Учёные записки. – 2015. – С. 293-299. – Текст : непосредственный.

215. Соловей, В. Д. «Цветные революции» и России / В. Д. Соловей // Сравнительная политика. – 2011(1). – С. 33-43. – Текст : непосредственный.

216. Столетов О. Концепт «прокси-война» в международно-политическом дискурсе «Новой Холодной войны» / О. Столетов // Социально-гуманитарные знания. – 2019. – № 4. – С. 122-124. – Текст : непосредственный.

217. Стратегии и контрстратегии гибридной войны / перевод Ш. Ли, И. У // Russian Study. – 2020. – № 2. – С. 121-136. (李抒音、吴一鸣（译）.《混合战争战略和反战略》，俄罗斯研究，2020 年第 2 期，第 121-136 页). – Текст : непосредственный.

218. Стрельцов, А. А. Основные задачи государственной политики в области информационного противоборство / А. А. Стрельцов // Военная мысль. – 2011. – No. 5. – С. 18-25. – Текст : непосредственный.

219. Тиханычев, О. В. Гибридные войны: новое слово в военном искусстве или хорошо забытое старое? / О. В. Тиханычев // Вопросы безопасности. – 2020. – № 1. – С. 30-44. – Текст : непосредственный.

220. Толоконникова, А. В. Роль телеканала RT в формировании международного имиджа России / А. В. Толоконникова, Д. О. Будакова // Вестник Московского университета. Серия 10: Журналистика. – 2019. – № 5. – С. 89-119. – Текст : непосредственный.

221. Тянь, Фэнцзюань. Формирование и коммуникация образа российского государства в киберпространстве /Фэнцзюань Тянь // SiberianStudies. – 2021. – № 4. – С.31-48.（田凤娟.俄罗斯国家形象在网络空间的塑造与传播,载《西伯利亚研究》2021 年第 4 期，第 31 至 48 页）.– Текст : непосредственный.

222. У, Фэй. Роль СМИ в информационной войне между Россией и США в контексте геополитической борьбы / Фэй У, Сюань Ли // Внешняя коммуникация. – 2022. – № 6. – С. 72-76. （吴非，李旋. 地缘政治博弈下俄美信息战中的媒体角色，载《对外传播》2022 年第 6 期，第 72 至 76 页）.– Текст : непосредственный.

223. Усмонова, Н. Р. Правовое обеспечение национальной безопасности Российской Федерации / Н. Р. Усмонова // Молодой ученый. – 2018. – № 44 (230). – С. 189-191.– Текст : непосредственный.

224. Фадеев, А. С. Военные конфликты современности, перспективы развития способов их ведения. Прямые и непрямые действия в вооружённых конфликтах XXI века / А. С. Фадеев, В. И. Ничипор // Военная мысль. – 2019. – № 9. – С. 33-41.– Текст : непосредственный.

225. Фань, Юнпэн. Характеристики и урок информационной войны в российско-украинском конфликте / Юнпэн Фань, Циньвэнь Хань // Форум по стратегии киберпространства.–2022. – № 6. – С. 76-79. （范勇鹏，韩沁雯.俄乌冲突网

络信息战的特征与启示,载《网络空间战略论坛》2022年第6期，第76至79页）. – Текст : непосредственный.

226. Федоренко, А. В. Общая характеристика органов государственной власти по вопросам обеспечения национальной безопасности в Российской Федерации / А. В. Федоренко // Молодой ученый. – 2022. – № 5 (400). – С. 237-239. – Текст : непосредственный.

227. Филимонов, Г. Ю. «Гибридная война»: интерпретация и реальность / Г. Ю. Филимонов, Н. С. Данюк // Свободная мысль. – 2017. – № 3. – С. 17-24. – Текст : непосредственный.

228. Филимонов, Г. Ю. Социальные сети как инновационный механизм «мягкого» воздействия и управления массовым сознанием / Г. Ю. Филимонов, С. А. Цатурян // Политика и общество. NotaBene. – 2012. – № 1. –С.65-75. – Текст : непосредственный.

229. Фридман, О. «Гибридная война» понятий / О. Фридман // Вестник МГИМО-Университета. – 2016. – № 5(50). – С. 79-85. – Текст : непосредственный.

230. Хан, Кеди. «Гибридная война» России в Украине / Кеди Хан // Исследование стратегических решений. – 2021. –№ 6. – С. 51-80.（韩克敌. 俄罗斯在乌克兰的“混合战争”,载《战略决策研究》2021年第6期，第51至80页）. – Текст : непосредственный.

231. Цзя, Юаньпей. Методы ведения информационных войн Запада против России и российские контрмеры / Юаньпей Цзя, Цюн Сун // JournalofJournalismStudies.–2020. – № 22. – С. 233-234.（贾渊培，宋琼.西方对俄罗斯舆论战方式及其应对策略研究,载《新闻研究导刊》2020年第22期，第233至234页）. – Текст : непосредственный.

232. Цыганков, П. А. Гибридная война: политический дискурс и международная практика / П. А. Цыганков // Вестник Московского университета. Серия 18. Социология и политология. – 2015. – № 4. – С. 253-258. – Текст : непосредственный.

233. Цыганков, П. А. Западный дискурс о «гибридной войне России против демократии»: новое вино в ветхие мехи / П. А. Цыганков, Л. Э. Слуцкий // Вопросы политологии. – 2022. – №12. – Текст : непосредственный.

234. Чекинов, С. Г. Прогнозирование характера и содержания войн будущего: проблемы и суждения / С. Г. Чекинов, С. А. Богданов // Военная мысль. – 2015. – № 15. – С. 44-45. – Текст : непосредственный.

235. Чепрасов, К. В. Создание национальной гвардии как ответ на гибридные вызовы безопасности России / К. В. Чепрасов // Вопросы безопасности. – 2016. – № 2. – С. 8-19. – Текст : непосредственный.

236. Чжан, Хуэй. Изучение опыта гибридной войны для устранения угроз безопасности /Хуэй Чжан, Цзюньбяо Лю // China Defense News. –2017. – № 22. (张翚、刘俊彪.《借鉴“混合战争”应对安全威胁》，载中国国防报 2017 年第 022 版). – Текст : непосредственный.

237. Штоль, В. В. США – истоки и пределы американского империализма / В. В. Штоль, А. Г. Задохин // Обозреватель–Observer. – 2018. – № 7. – С. 5-16. – Текст : непосредственный.

238. Шэн, Шилян. Как Россия ответила на гибридную войну от США / Шилян Шэн // Военный сборник. –2016. – № 11.– С. 20-23. (盛世良.俄罗斯如何应对美国的 «混合战争» 军事文摘 2016年第11期第20至23页). – Текст : непосредственный.

239. Шэнь, Вэнькэ. Взгляд на современную войну из конфликта в Нагорном Карабахе / Вэнькэ Шэнь // PLA Daily. –2020. – №. 7.(沈文科：《从纳卡冲突管窥现代战争》, 解放军报, 2020 年 10 月, 第 007 版). – Текст : непосредственный.

240. Ян, Нинцун. Информационная война в российско-украинском конфликте и её просветительство / Нинцун Ян // Мировые социалистические исследования.– 2022. – № 10. – С.82-88.（杨柠聪. 俄乌冲突中的信息战及其启示, 载《世界社会主义研究》2022年第10期，第82至88页.）– Текст : непосредственный.

241. Buţa, V. Persectives on the evolution and influenct of the hybrid warfare concept / V. Buţa, V. Vasile // Romanian Military Thinking. – 2015. – № 3. – P. 11-32. – Текст : непосредственный.

242. Buzan, B. New patterns of global security in the twenty-first century / B. Buzan // International affairs. – 1991. – Vol. 67, № 3. – P. 433-451. – Текст : непосредственный.

243. Cilluffo, F. J. Thinking About Strategic Hybrid Threats: In Theory and in Practice / F. J. Cilluffo , J. R. Clark // PRISM. – 2014. – Vol. 4. – Issue 1. – P. 47-63. – Текст : непосредственный.

244. Gentile, G. P. The Imperative for an American General-Purpose Army That Can Fight / G. P. Gentile // ORBIS. – 2009. – Vol. 53, № 3. – P. 457-470. – Текст : непосредственный.

245. Hoffman, F. G. Complex Irregular Warfare: The Next Revolution in Military Affairs / F. G. Hoffman // Orbis. 2006. –Vol. 50, № 3. –P. 397-399. – Текст : непосредственный.

246. Iasiello, E. J. Russia's Improved Information Operations: From Georgia to Crimea / E. J. Iasiello // Parameters.– 2017. – Vol. 47, No. 2. – P. 51-63. – Текст : непосредственный.

247. Królikowski, H. Hybrid Threats and Warfare, Are We Really Facing Something New? / H. Królikowski // Internal Security. – 2017. – Vol. 9. – Issue 2. – P. 9-21. – Текст : непосредственный.

248. Mann, S. R. The Reaction to Chaos / S. R. Mann // Complexity, Global Politics, and National Security. – 1997. – P. 62-68. – Текст : непосредственный.

249. Mann, S.R. Chaos Theory in Strategic Thought / S.R. Mann // Parametes. – 1992. – Vol. 22, № 1. -- P. 54-68. – Текст : непосредственный.

250. Markus, B. G. Russian scholarly discussions of nonmilitary warfare as securitizing acts / B. G. Markus // Comparative Strategy. – 2022. – Vol. 41, No. 6. – P. 526-542. – Текст : непосредственный.

251. Mattis, J. N. Future Warfare: The Rise of Hybrid Wars / J. N. Mattis, F. G. Hoffman // Proceedings. – 2005. – Vol. 132, №11. – Текст : непосредственный.

252. McCuen, J. J. Hybrid Wars / J. J. McCuen // Military Review. – 2008. – Vol. 88, Issue 2. – P. 107-113. – Текст : непосредственный.

253. Popescu, N. Hybrid tactics: Russia and the West / N. Popescu // European Union Institute for Security Studies, Alert. – 2015. – № 46. – Текст : непосредственный.

254. Selhorst T. Russia's Perception Warfare: The Development of Gerasimov's Doctrine in Estonia and Georgia and Its Application in Ukraine / Tony Selhorst // Militaire Spectator. – 2016. – Vol. 185, No. 4. – P. 148-164.– Текст : непосредственный.

255. Simons, G. Digital Communication Disrupting Hegemonic Power in Global Geopolitics / G. Simons // Russia in Global Affairs. – 2019. – No. 2. – P. 108-125. – Текст : непосредственный.

256. The Changing Face of War: Into the Fourth Generation / W. S. Lind, K. Nightengale, J. F. Schmitt [et al.] // Marine Corps Gazette. – 1989. – № 73. – P. 22-26. – Текст : непосредственный.

Материалы конференций

257. Бельков, О. А. Гибридная война – выдуманная реальность? / О. А. Бельков // Гибридные войны XXI века: материалы межвузовского круглого стола 29.01.2015 г. – М.: ВУ, 2015. – 310 с. – Текст : непосредственный.

258. Булгаров, М. А. К вопросу о сущности понятия «Имидж страны» / М. А. Булгаров, М. Н. Тонян, А. А. Кутовая // WordScience: ProblemsandInnovations: сб. ст. победителей IX Междунар. науч.-практ. конф. в 2 ч. Ч. 2. – Пенза: Наука и просвещение, 2017. – С. 110-113. – Текст : непосредственный.

259. Бурило, Е. А. «Цветные революции» как разновидность политического конфликта // Е. А. Бурило // Будущее науки. Сборник научных статей 7-й Международной молодежной научной конференции. – Курск: Юго-Западный государственный университет, 2019. – С. 289-292. – Текст : непосредственный.

260. Данюк, Н. С. «Цветные революции» и «Гибридные войны» как инструменты м международной научно-практической конференции, Новосибирск, 01–11 ноября 2017 года. Том 3-4 (2). – Новосибирск: Ассоциация научных сотрудни-

ков «Сибирская академическая книга», 2017. – С. 44-55. – Текст : непосредственный.

261. Логинова, Г. Е. Проблема гибридной войны в современной геополитике: теоретиче университет им. Т. Ф. Горбачева, 2017. – Текст : непосредственный.

262. Небренчин, С. М. Информационный характер современной «мягкой силы»: россий Московский государственный лингвистический университет. – М.: Московский государственный лингвистический университет, 2017. – С. 201-220. – Текст : непосредственный.

Диссертации

263. Данюк Н.С. Внешняя политика Российской Федерации (2000-2016 гг.) и феномен «цветных революций»: дисс. ... канд. истор. наук: 07.00.15. – М., 2018. – 312 с. – Текст : непосредственный.

264. Курилкин А.В. Информационные и кибернетические операции как инструмент реализации внешней политики: формы, методы, технологии дисс. ... канд. полит. наук: 23.00.04. – М., 2021. – 207 с. – Текст : непосредственный.

265. Walker R. G. Spec Fi: The United States Marine Corps and Special Operations: Master's thesis / R. G. Walker. – Naval Postgraduate School, 1998. – 108 p. – Текст : непосредственный.

Аналитические доклады и публикации

266. Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations. // Booz Allen Hamilton. 2020. URL: https://www.boozallen.com/content/dam/home/docs/cyber/bearing-witness-uncovering-the-logic-behind-russian-military-cyber-operations-2020.pdf (дата обращения: 10.02.2023). – Текст : электронный.

267. Ben, Norton. Behind NATO's 'cognitive warfare': 'Battle for your brain' waged by Western militaries / Norton Ben. // The Grayzone. 2021. URL: https://thegrayzone.com/2021/10/08/nato-cognitive-warfare-brain/ (дата обращения: 15.06.2022). Текст : электронный.

268. Bentzen, N. Foreign Influence Operations in the EU / N. Bentzen // European Parliamentary Research Service. 2018. URL:

https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf (дата обращения 28.07.2022). – Текст : электронный.

269. Bordachev, T. Trenches and Bridges of Eurasian Integration / T. Bordachev // Valdai. 2022. URL: https://valdaiclub.com/a/highlights/trenches-and-bridges-of-eurasian-integration/ (дата обращения 20. 10. 2022). – Текст : электронный.
270. Breedlove, P. West Must Fight Russia in Information War / P. Breedlove // Military Times. 2015. URL: https://www.militarytimes.com/2015/03/22/breedlove-west-must-fight-russia-in-information-war (дата обращения: 06.01.2023). – Текст : электронный.
271. Calabresi, M. Inside Russia's Social Media War on America / M. Calabresi // TIME. 2017. URL: https://cs.brown.edu/people/jsavage/VotingProject/2017_05_18_Time_InsideRussia'sSocialMediaWarOnAmerica.pdf (дата обращения: 20.01.2023). Текст : электронный.
272. Calabresi, M. Inside Russia's Social Media War on America / M. Calabresi // Time. 2017. URL: https://time.com/magazine/us/4783906/may-29th-2017-vol-189-no-20-u-s/ (дата обращения: 20.01.2023).– Текст : электронный.
273. Clark, M. Russian Hybrid Warfare / M. Clark // The Institute for the Study of War. 2020. URL: http://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf (дата обращения: 10.02.202).– Текст : электронный.
274. Cluzel, F.D. CognitiveWarfare / F.D. Cluzel // InnovationHub. 2020. URL: https://www.innovationhub-act.org/sites/default/files/2022-02/CW%20article%20Claverie%20du%20Cluzel%20final_0.pdf (дата обращения: 20.10.2022). – Текст : электронный.
275. Costello, K. Russia's Use of Media and Information Operations in Turkey. / K. Costello // RANDCorporation. 2018. URL: https://www.rand.org/pubs/perspectives/ PE278.html (дата обращения: 06.01.2023). – Текст : электронный.

276. Davis, P. Effects-Based Operations / P. Davis // RANDCorporation. 2001. URL: https://www.rand.org/content/dam/rand/pubs/monograph_reports/2006/MR1477.pdf (дата обращения: 06.06.2022). – Текст : электронный.

277. Dominioni, S. Russia's Hybrid Strategy: Myth or Reality? / S. Dominioni, A. E. Tafuro // Italian Institute for International Political Studies (ISPI). URL: https://www. ispionline.it/en/pubblicazione/russias-hybrid-strategy-myth-or-reality-26805 (дата обращения: 05.04.2022). – Текст : электронный.

278. Elder, M. Russians Fight Twitter and Facebook Battles over Putin Election / M. Elder // The Guardian.2011. URL: https://www.theguardian.com/world/2011/dec/09/ russia-putin-twitter-facebook-battles (дата обращения: 10.02. 2023). – Текст : электронный.

279. Galeotti M. Controlling Chaos: How Russia Manages its Political War in Europe / M. Galeotti // London, United Kingdom: European Council on Foreign Relations. 2017. URL: https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_ political_war_in_europe/ (дата обращения: 15.12.2022). – Текст : электронный.

280. Galeotti, M. I'm Sorry for Creating the 'Gerasimov Doctrine / M. Galeotti // Foreign Policy. 2018. URL: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ (дата обращения: 20.01.2023). – Текст : электронный.

281. Galeotti, M. Russian hybrid warfare and other dark arts / M. Galeotti // War on the rocks. 2016. URL: https://warontherocks.com/2016/03/ russian-hybrid-warfare-and-other-dark-arts/ (дата обращения: 10.12.2021). – Текст : электронный.

282. Galeotti, M. The West is too paranoid about Russia's 'infowar' / M. Galeotti // The Moscow Times. 2015. URL: http://connections-qj.org/article/west-too-paranoid-about-russias-infowar (дата обращения: 20.10.2022). – Текст : электронный.

283. Glenn, R. W. Thoughts on 'Hybrid' Conflict / R. W. Glenn // Small Wars Journal. 2009. URL: https://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict (дата обращения: 10.02.2021). – Текст : электронный.

284. Hill, F. Mr. Putin and the Art of the Offensive Defense: Approaches to Foreign Policy (Part Two) / F. Hill // Brookings Institution. 16.03.2014. URL: https://www.brookings.edu/articles/mr-putin-and-the-art-of-the-offensive-defense-approaches-to-foreign-policy-part-two(дата обращения: 05.01.2023). – Текст : электронный.

285. Kofman, M. A Closer Look at Russia's Hybrid War / M. Kofman, M. Rojansky // KennanCable. 2015. URL: https://www.wilsoncenter.org/sites/default/files/media/documents/publication/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf (дата обращения: 10.02.2022). – Текст : электронный.

286. Kofman, M. Russia’s Armed Forces under Gerasimov, the Man without a Doctrine / M. Kofman // Russian Military Analysis. 2020. URL: https://www.ridl.io/en/russia-s-armed-forces-under-gerasimov-the-man-without-a-doctrine/ (дата обращения: 10.12.2021). – Текст : электронный.

287. Manoilo, A. Skripal Readings as an Example of a Special Operation to Intercept the Information Agenda. The Latest Practice of Modern Information Warfare and Psychological Operations / A. B. Manoilo // Medium. 06.03.2020. URL: https://medium. com/@andreimanoilo/skripal-readings-as-an-example-of-a-special-operation-to-intercept-the-information-agenda-dd55b3dab908 (дата обращения: 10.10.2022). – Текст : электронный.

288. Modern Political Warfare: Current Practices and Possible Responses / L. Robinson, T. C. Helmus, R. S. Cohen [et al.] // RAND Corporation. 2018. URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1772/RAND_RR1772.pdf(дата обращения: 10.12.2022). – Текст : электронный.

289. Nye, J. Is Military Power Becoming Obsolete? / J. Nye // ProjectSyndicate. 2010. URL: https://www.project-syndicate.org/commentary/is-military-power-becoming-obsolete-2010-01 (дата обращения: 12.06.2021). – Текст : электронный.

290. Overextending and Unbalancing Russia: Assessing the Impact of Cost-Imposing Options / J. Dobbins, R.S. Cohen, N. Chandler [et al.] Santa Monica, CA: RAND Corporation Текст : электронный // RAND Corporation. 2019 URL: https://www.rand.org/pubs/research_briefs/RB10014.html (дата обращения: 10.02.2021). – Текст : электронный.

291. Pomerantsev, P. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money: A Special Report Presented by the Interpreter, a Project of the Institute of Modern Russia / P. Pomerantsev, M. Weiss // Institute of Modern Russia. 2014. URL: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_ Peter_Pomerantsev__The_Menace_of_Unreality.pdf (дата обращения: 10.02.2023). – Текст : электронный.

292. Pomerantsev, P. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money: A Special Report Presented by the Interpreter, a Project of the Institute of Modern Russia / P. Pomerantsev, M. Weiss // New York: Institute of Modern Russia. 2019. URL: https://imrussia.org/media/pdf/Research/Michael_ Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf (дата обращения: 20.01.2023). – Текст : электронный.

293. Report of Pew Research Center: Seven-in-Ten Americans Now See Russia as an Enemy / R. Wike, J. Fetterolf, M. Fagan [et al.] // Pew Research Center.2022. URL: https://www.pewresearch.org/global/2022/04/06/russia-nato-ukraine-march-2022-acknowledgments/ (дата обращения: 15.06.2022). – Текст : электронный.

294. Rühle, M. Enlarging NATO’s toolbox to counter hybrid threats / M. Rühle, C. Roberts // NATO Review magazine. 2021. URL: https://www.nato.int/docu/review/ articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html (дата обращения: 06.07.2022). – Текст : электронный.

295. Rühle, M. NATO’s Unified Response to Hybrid Threats / M. Rühle, C. Roberts // CEPA. 2021. URL: https://cepa.org/natos-unified-response-to-hybrid-threats/ (дата обращения: 06.07.2022). – Текст : электронный.

296. Scott, J. Russia’s Ultimate Weapon Might Be Cyber / J. Scott // The National Interest. 2018. URL: https://nationalinterest.org/pro file/scott-jasper (дата обращения: 06.01.2023). – Текст : электронный.

297. Sharikov, P. Understanding the Russian Approach to information Security / P. Sharikov // The European Leadership Network (ELN). 2018. URL: https://www.

europeanleadershipnetwork.org/commentary/understanding-the-russian-approach-to-information-security/ (дата обращения: 05.11.2022). – Текст : электронный.

298. Sherman J. Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior / J. Sherman // Atlantic Council. 12.07.2021. URL: https://www.atlanticcouncil.org/wp-content/uploads/2021/07/RuNet-Issue-Brief-2021.pdf (дата обращения: 20.10.2022). – Текст : электронный.

299. Snegovaya, M. Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare / M. Snegovaya. Russia Report I // Institute for the Study of War.2015. URL: https://www.understandingwar.org/sites/default/ files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-20Sov iet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf (дата обращения: 10.02.2023). – Текст : электронный.

300. Solmaz, T. 'Hybrid Warfare': One Term, Many Meanings / T. Solmaz // Small Wars Journal. 2022. URL: https://smallwarsjournal.com/jrnl/ art/hybrid-warfare-one-term-many-meanings (дата обращения: 20.02.2022). – Текст : электронный.

301. Stelzenmüller, C. The Impact of Russian Interference on Germany's 2017 Elections / C. Stelzenmüller // Brookings Institute. 2017. URL: https://www.brookings.edu/ testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/(дата обращения: 01.02.2022). – Текст : электронный.

302. Stoltenberg, J. Zero-sum? Russia, Power Politics, and the Post War Era / J. Stoltenberg // NATO. 2015. URL: http://www.nato.int/cps/en/ natohq/opinions_118347.htm (дата обращения 31.04.2022). – Текст : электронный.

303. The Evolution of Russian Hybrid Warfare / M. Boulègue, C.-D. Precious, A. Polyakova [et al.] // The Center for European Policy Analysis. 2020. URL: https://cepa. org/wp-content/uploads/2021/01/CEPA-HybridWarfare-1.28.21. pdf (дата обращения: 10.02.2022). – Текст : электронный.

304. The IRA, social media and Political Polarization in the United States, 2012–2018 / P. Howard, G. Bharath, Liotsiou D. [et al.] // University of Oxford: Computational Research Project. 2018. URL: https://comprop.oii.ox.ac.uk/wp-content/uploads/

sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf (дата обращения: 20.01.2023). – Текст : электронный.

305. Trends in World Military Expenditure 2021 / N. Tian, A, Fleurant, A. Kuimova [et al.] // Stockholm International Peace Research Institute. 2022. URL: https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf (дата обращения: 06.12.2022). – Текст : электронный.

306. Treyger, E. Russian Disinformation Efforts on social media / E. Treyger, J. Cheravitch, R. S. Cohen // RAND Corporation. 2022. URL: https://www.rand.org/pubs/research_reports/RR4373z2.html (дата обращения: 15.01.2023). – Текст : электронный.

307. Ulrik, F. Russian Politics and the Internet in 2012 / F. Ulrik, C. V. Pallin // Stockholm: Defense Research Agency. 2012. URL: https://www.foi.se/rest-api/report/FOI-R--3590--SE (дата обращения: 25.01.2023). – Текст : электронный.

308. Барабанов, О. Н. Новая концепция внешней политики РФ : структура и семантика / О. Н. Барабанов // Валдай. 2023. URL: https://ru.valdaiclub.com/a/highlights/novaya-kontseptsiya-vneshney-politiki-rf-semantika/?sphrase_id=645683 (дата обращения: 20.04.2023). – Текст : электронный.

309. Бартош, А. А. Гибридная война становится новой формой межгосударственного противоборства / А. А. Бартош // Военное обозрение. 2017. URL: https://topwar.ru/112955-gibridnaya-voyna-stanovitsya-novoy-formoy-mezhgosudarstvennogo-protivoborstva.html (дата обращения: 15.05.2021). – Текст : электронный.

310. Бартош, А. А. Вычисляем будущие конфликты / А. А. Бартош // Военно-промышленный курьер. 2021. № 2 (865). URL: https://vpk-news.ru/articles/60450(дата обращения: 05.06.2022). – Текст : электронный.

311. Бартош, А. А. Гибридная война: интерпретации и реальность / А. А. Бартош // Независимое военное обозрение. 2016. URL: https://nvo.ng.ru/concepts/2016-09-16/1_war.html (дата обращения: 20.10.2021). – Текст : электронный.

312. Бартош, А. А. Цель и механизмы модели управляемого хаоса / А. А. Бартош // Независимое военное обозрение. 2013. URL: https://nvo. ng.ru/concepts/2013-09-27/6_chaos.html (дата обращения: 25.05.2022). – Текст : электронный.

313. Белозеров, В. СМИ: Информационное противоборство / В. Белозеров, Д. Копылова // Ориентир. 2014. No. 5. URL: http://milportal.ru/smi-informatsionnoe-protivoborstvo/ (дата обращения: 05.01.2023). – Текст : электронный.

314. Ван, Сяншуй. Гибридная война – важный инструмент в нынешней международной политической игре / Сяншуй Ван // Экономический вестник. 2018. URL: https://www.jingjidaokan.com/icms/null/null/ns:LHQ 6LGY6LGM6MmM5Y2QyOTA2NzJhN2ViMjAxNjczNDE4N2ZlMjAwZDUscDosYTosbTo=/show.vsml (дата обращения: 07.08.2021)（王湘穗.混合战争是当前国际政治博弈的重要工具,《经济导刊》编辑部，2018 年 11 月 21 日). – Текст : электронный.

315. Вашингтон ставит на «управляемый хаос» // Независимая. 2018. URL: https://www.ng.ru/armies/2018-04-10/8_7208_washington.html (дата обращения: 20.05.2021). – Текст : электронный.

316. Герасимов, В. По опыту Сирии / В. Герасимов // Военно-промышленный курьер. 2016. No. 9. URL: https://vpk.name/news/150974_po _opytu_sirii.html (дата обращения: 20.01.2023). – Текст : электронный.

317. Герасимов, В. Ценность науки в предвидении / В. Герасимов // Военно-промышленный курьер. 2013. No. 8. URL: https://vpk.name/ news/85159_cennost_nauki_v_predvidenii.html(дата обращения: 20.01.2023). – Текст : электронный.

318. Гибридная война в будущих конфликтах / перевод Сюй Дэцзюнь // Strategic Frontier Technologies. 2021. URL: https://mp.weixin.qq.com/s/_vxEPz5tsmwJaQ4vcILHww (дата обращения: 10.06.2021)(许得君(编译). 《未来冲突中的混合战争》战略前沿技术 2021 年 3 月 26 日). – Текст : электронный.

319. Глобальная киберповестка: дипломатическая победа. Интервью директора Департамента международной информационной безопасности МИД России А. В. Крутских // Международная жизнь. 2021. URL:

https://interaffairs.ru/news/ show/30374 (дата обращения: 26.10.2022). – Текст : электронный.

320. Гриняев, С. Н. Информационная война: история, день сегодняшний и перспектива / С. Н. Гриняев // Центр стратегических оценок и прогнозов. 2001. URL: http://csef.ru/ru/oborona-i-bezopasnost/265/informaczionnaya-vojna-istoriya-dense godnyashnij-i-perspektiva-538 (дата обращения: 12.02.2021). – Текст : электронный.

321. Дворников, А. Штабы для новых войн / А. Дворников // Военно-промышленный курьер. 2018. No. 28. URL: https://vpk.name/news/ 222202_shtaby_dlya_novyh_voin.html (дата обращения: 20.09.2022). – Текст : электронный.

322. Действия соединений, частей и подразделений СВ при проведении специальной операции по разоружению НВФ в 1994-96 гг. на территории Чеченской республики. Доклад бывшего начальника штаба СКВО генерал-лейтенанта В. Потапова // Вестник ПВО. 04.11.2005. URL: http://pvo.guns.ru/book/chechnya _pvo.htm (дата обращения: 06.01.2023). – Текст : электронный.

323. Катасонов, В. Экономические войны и экономические санкции / В. Катасонов // Военное обозрение. 2015. URL: https://topwar.ru/68238-ekonomicheskie-voyny-i-ekonomicheskie- sankcii.html (дата обращения: 06.01.2022). – Текст : электронный.

324. Коренев, Е. «Осажденная крепость» с открытыми воротами. Новая Стратегия национальной безопасности РФ / Е. Коренев // РСМД. 2022. URL: https://russiancouncil.ru/analytics-and-comments/columns/riacdigest/-osazhdennaya-krepost-s-otkrytymi-vorotami-novaya-strategiya-natsionalnoy-bezopasnosti-rf/ (дата обращения: 01.10.2022). – Текст : электронный.

325. Кудряшов, А. Использование за рубежом сети Интернет в интересах ведения информационных войн / А. Кудряшов // Зарубежное военное обозрение. 2011. URL: https://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2011-zvo/8028-ispolzovanie-za-rubezhom-seti-internet-v-interesah (дата обращения: 05.01.2023). – Текст : электронный.

326. Кузьмин В. Роль США в осуществлении «цветных революций» в зарубежных странах / В. Кузьмин // Зарубежное военное обозрение. 2008. URL: https:// militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2008-zvo/7658-rol-ssha-v-osushestvlenii-cvetnyh-revoljucij-v (дата обращения: 05.01.2023). – Текст : электронный.

327. Ма, Цзяньгуан. Россия создает кибервойска / Цзяньгуан Ма, Пэн Ся // Военное обозрение. 2013. URL: https://topwar.ru/31668-rossiya-sozdaet-kibervoyska-stdailycom-kitay.html(дата обращения: 15.12.2022). – Текст : электронный.

328. Микрюков, В. Победа в войне должна быть достигнута еще до первого выстрела / В. Микрюков // Независимое военное обозрение. 2016. URL: https:// nvo.ng.ru/concepts/2016-01-15/10_infowar.html (дата обращения: 05.01.2023). – Текст : электронный.

329. Микрюков, В. Ю. Прокси-война / В. Ю. Микрюков // Научно-исследовательский центр «Национальная безопасность». 2015. URL: http://nic-pnb.ru/ analytics/proksi-vojna/ (дата обращения: 06.06.2022). – Текст : электронный.

330. Мухин, В. Ставка на информационный спецназ / В. Мухин // Независимое военное обозрение. 2015. URL: https://nvo.ng.ru/realty/ 2015-04-17/1_specnaz.html (дата обращения: 05.12.2022). – Текст : электронный.

331. На гибридные войны следует отвечать гибридными методами // Центр анализ террористических угроз. 2023. URL: https://catu.su/ analytics/1256-na-gibridnye-vojny-sleduet-otvechat-gibridnymi-metodami (дата обращения: 20.04.2023). – Текст : электронный.

332. Небренчин, С. М. Устоит ли Россия против «гибридной цветной революции»? / С. М. Небренчин // REGNUM. 2016. URL: https://regnum.ru/news/polit/ 2158662.html (дата обращения 25.08.2021). – Текст : электронный.

333. Несмеянов, В. Сумеем ли защитить Великую Победу? / В. Несмеянов // Флаг Родины. 2013. URL: https://sc.mil.ru/files/morf/military/archive/%5Bфлаг%20 Родины» %5D%5B2013-06-04%5D. pdf (дата обращения: 05.01.2023). – Текст : электронный.

334. Новик, А. Оружие будущего по-британски / А. Новик // Страж Балтики. 2019. URL: https://ric.mil.ru/upload/site173/3smeFty8fn.pdf (дата обращения: 20.01.2023). – Текст : электронный.

335. Отчёт о санкции Запада против России. Институт финансовых исследований Чунъян Китайского народного университета. апрель 2022 г. (中国人民大学重阳金融研究院研究报告：《大杀器？美国对俄罗斯制裁评估与启示》. 2022 年 4 月). URL: http://rdcy.ruc.edu.cn›yw/HOME/index.htm. – Текст : электронный.

336. Пономарева, Е. Г. Секреты «цветных революций» / Е. Г. Пономарева // Свободная мысль. 2012. URL: http://svom.info/entry/208-sekrety-cvetnyh-revolyucij/ (дата обращения: 15.10.2022). – Текст : электронный.

337. Пришло наше время послужить России: как война в Грузии вдохновила спецслужбы на вербовку хакеров-патриотов // Вестник К. 2018. URL: https:// vestnikk.com/society/crucial/32201-prishlo-nashe-vremya-posluzhit-rossii-kak-voyna-v-gruzii-vdohnovila-specsluzhby-na-verbovku-hakerov-patriotov.html (дата обращения: 10.01.2023). – Текст : электронный.

338. Путин, В. В. Солдат есть звание высокое и почётное. Выступление с ежегодным Посланием Федеральному Собранию / В. В. Путин // Красная звезда. 2006. URL: http://old.redstar.ru/2006/05/11_05/1_01.html (дата обращения: 06.02.2023). – Текст : электронный.

339. Рябиченко, А. Цифровая дипломатия вчера и сегодня / А. Рябиченко // РСМД. 2018. URL: http://russiancouncil.ru/analytics-and comments/columns/digitaldiplomacy/tsifrovaya-diplomatiya-vchera-i-segodnya/ (дата обращения: 17.12.2022). – Текст : электронный.

340. Сивков, К. «Мудрость» Януковича / К. Сивков // Военное обозрение. 2014. URL: https://topwar.ru/54802-mudrost-yanukovicha.html (дата обращения: 05.01.2023). – Текст : электронный.

341. Су, Цзинсян. Цветная революция в Гонконге и гибридная война США против Китая / Цзинсян Су // China·Us focus. 2019. URL: http://cn.chinausfocus.com/culture-history/20190819/41477.html (дата обращения: 10.06.2021) (宿景祥.

《香港“颜色革命”与美国对华”混合战“》,载《中美聚焦》,2019 年). – Текст : электронный.

342. Сун, Чжунпин. Китай и США находятся не в новой холодной войне, а в гибридной войне / Чжунпин Сун // Union-Tribune. 2020. URL: http://www.haozaobao.com/mon/keji/20200529/71989.html (дата обращения: 10.06.2021)(宋忠平. 《中美两国非新冷战而是混合战》,载《联合早报》，2020 年 5 月 29 日). – Текст : электронный.

343. Тавровский, Ю. В. США–Китай: идёт война гибридная / Ю. В. Тавровский // Независимая. 2018. URL: https://www.ng.ru/dipkurer/2018-09-02/9_10_7301_dipuschina.html (дата обращения: 06.03.2022). – Текст : электронный.

344. Тимофеев, В. Про информшаблону / В. Тимофеев // Красная звезда. 2005. URL: http://old.redstar.ru/2005/01/19_01/3_03.html (дата обращения: 05.01.2023). – Текст : электронный.

345. Тиханский, А. Новая военная доктрина Союзного государства Беларуси и России: «гибридные войны» и «цветные революции» / А. Тиханский // Аналитический портал «Евразия. Эксперт». 2017. URL: https://eurasia.expert/novaya-voennaya-doktrina-soyuznogo-gosudarstva-belarusi-i-rossii-gibridnye-voyny-i-tsvetnye-revolyuts/ (дата обращения: 15.09.2022). – Текст : электронный.

346. Триггеры информационной схватки // Независимое военное обозрение. 2020. URL: https://nvo.ng.ru/nvo/2020-11-12/1_1117_triggers.html (дата обращения: 10.11.2022). – Текст : электронный.

347. Цыганок, А.Д. Первые жертвы оружия нового поколения / А.Д. Цыганок // Независимое военное обозрение. 2018. № 44. URL: https://nvo.ng.ru/armament/2018-11-16/8_1022_victim.html (дата обращения: 06.01.2023). – Текст : электронный.

348. Черненко, Е. Использование Россией «мягкой силы» / Е. Черненко // Газета «Коммерсантъ». 2021. №181. URL: https://www.kommersant.ru/theme/1806 (дата обращения: 05.12.2022). – Текст : электронный.

Материалы СМИ и источники из сети Интернет

349. ‘It’s the right thing to do’: the 300,000 volunteer hackers coming together to fight Russia // The Guardian.2022. URL: https://www.theguardian.com/world/2022/mar/ 15/volunteer-hackers-fight-russia (дата обращения: 01.02.2023). – Текст : электронный.

350. «Merci, RT»: активисты «жёлтых жилетов» не доверяют французским СМИ // RT. 2019. URL: https://russian.rt.com/press_releases/article/589428-rt-france-zhyoltye-zhilety (дата обращения: 17.11.2022). – Текст : электронный.

351. «Информационная битва». Как Россия создавала фейковых американцев, чтобы повлиять на выборы // Главк. 2017. URL: https://glavk.net/news/265042-nformatsionnaja_bitva._kak_rossija_sozdavala_fejkovyh_amerikantsev_chtoby_povlijatj_na_vybory (дата обращения: 20.12.2022). – Текст : электронный.

352. «Касперский» выявил рост числа DDoS-атак на компании России в 8 раз Текст : электронный // РБК. 2022. URL: https://www.rbc.ru/technology_and_media/01/04/2022/624699a89a79473501fa15f9 (дата обращения: 01.02.2023). – Текст : электронный.

353. «Основа Всеобъемлющей концепции национальной безопасности» вышла в свет // Центральное народное правительство КНР. 2022. URL: http://www.gov.cn/xinwen/2022-04/15/content_5685392.htm (дата обращения 06.05.2022)(《总体国家安全观学习纲要》出版发行// 中华人民共和国中央人民政府. 15.04.2022. – Текст : электронный.

354. Britain managing Huawei risks, has no evidence of spying: official // Reuters. 2019. URL: https://www.reuters.com/article/us-huawei-europe-britain-idUSKCN1Q91PM) (дата обращения: 20.12.2021). – Текст : электронный.

355. Carbonnel, A. Insight: socialmedia Makes Anti-Putin Protests ‘Snowball’ / A. Carbonnel // Reuters. 2011. URL: https://www.reuters.com/article/us-russia-protests-socialmedia-idUSTRE7B60R720111207 (дата обращения: 15.01.2023). – Текст : электронный.

356. China, Russia propose lifting some U.N. sanctionson North Korea, U.S. says not the time // Reuters. 2019. URL: https://www.reuters.com/article/us-northkorea-usa-un/china-russia-propose-lifting-of-some-u-n-sanctions-on-north-korea-idUSKBN1YK20W(дата обращения 15.08.2022). – Текст : электронный.

357. Cohen, D. Behind a made-for-TV Hong Kong protest narrative, Washington is backing nativism and mob violence / D. Cohen // The Gray zone. 17.08.2019. URL: https://www.state.gov/joint-statement-on-hong-kong/ (дата обращения: 08.12.2021). – Текст : электронный.

358. Elder, M. Russian Protests: Thousands March in Support of Occupy Abay Camp / M. Elder // The Guardian. 13.05.2012. URL: https://www.theguardian.com/world/2012/may/13/russian-protests-march-occupy-abay (дата обращения: 15. 01.2023). – Текст : электронный.

359. Exporting Revolution // RT. 2012. URL: https://www.rt.com/usa/revolution-activists-world-people-297 (дата обращения: 10.01.2023). – Текст : электронный.

360. German IT watchdog says ‘no evidence’ of Huawei spying // The local. 2018. URL: https://www.thelocal.de/20181216/german-it-watchdog-says-no-evidence-of-huawei-spying/ (дата обращения: 10.11.2021). – Текст : электронный.

361. Gutterman, S, PutinSaysU.S. StokedRussianProtests / S. Gutterman, G. Bryanski // Reuters. 2011. URL: https://www.reuters.com/article/uk-russia-idUKTRE7B70H720111208 (дата обращения: 10.01.2023). – Текст : электронный.

362. Hoffman, D. Yeltsin’s Immunity Upheld by Duma Vote / D. Hoffman // WashingtonPost. 2000. URL: https://www.washingtonpost.com/wp-srv/WPcap/2000-03/30/ 090r-033000-idx.html (дата обращения: 05.02.2023). – Текст : электронный.

363. Hong Kong unmasked: The real reasons & instigators behind anti-Beijing riots // RT. 2019. URL: https://www.rt.com/news/474756-hong-kong-protests-china-us/ (дата обращения 15.07.2021). – Текст : электронный.

364. Ignatius, D. Russia’s Radical New Strategy for Information Warfare / D. Ignatius // Washington Post. 2017. URL: https://www.washingtonpost.com/blogs/post-

partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/ (дата обращения: 20.12.2022). – Текст : электронный.

365. Interview: U.S. military complex to benefit from Russia-Ukraine conflict: ex-Pentagon analyst // Xinhua. 2022. URL: https://english.news. cn/20220316/819 b5fa5927c462abae6b9a4b5d67bff/c.html (дата обращения: 06.01.2023). – Текст : электронный.

366. Kovacs, E. Russian Cyberspies Shift Focus from NATO Countries to Asia / E. Kovacs // Security Week. 2018. URL: https://www. securityweek.com/russian-cyber spies-shift-focus-nato-countries-asia/ (дата обращения: 06.01.2023). – Текст : электронный.

367. Kovalev, A. The Secrets of Russia's Propaganda War, Revealed / A. Kovalev, M. Bodner // Moscow Times. 2017. URL: https://www.themoscowtimes.com/2017/ 03/01/welcome-to-russian-psychological-warfare-operations-101-a57301 (дата обращения: 20.01.2023). – Текст : электронный.

368. Nakashima, E. Inside a Russian Disinformation Campaign in Ukraine in 2014 / E. Nakashima // Washington Post. 2017. URL: https://www.washingtonpost.com/ world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html (дата обращения: 05.02.2023). – Текст : электронный.

369. Oliker, O. Russia's New Military Doctrine: Same as the Old Doctrine, Mostly / O. Oliker // Washington Post. 2015. URL: https://www.washingtonpost.com/ news/monkey-cage/wp/2015/01/15/russias-new-military-doctrine-same-as-the-old-doctrine-mostly/(дата обращения: 06.01.2023). – Текст : электронный.

370. Outmatched in military might, Ukraine has excelled in the information war / M. Ryan, E. Nakashima, M. Birnbaum [et al.] // Washington Post. 2022. URL: https://www.washingtonpost.com/national-security/2022/03/16/ ukraine-zelensky-information-war/ (дата обращения: 20.10.2022). – Текст : электронный.

371. Pentagon Press Secretary Brig. Gen. Pat Ryder Holds an On-Camera Press Briefing // U.S. Department of Defense. 2023. URL: https://www.defense.gov/News/Trans cripts/Transcript/Article/3288141/pentagon-

press-secretary-brig-gen-pat-ryder-holds-an-on-camera-press-briefing/ (дата обращения: 05.02.2023). – Текст : электронный.

372. Rosenberg, M. Russia Sees Midterm Elections as Chance to Sow Fresh Discord Intelligence Chiefs Warn / M. Rosenberg, C. Savage, M. Wines // New York Times. 13.02.2018. URL: https://www.nytimes.com/2018/02/13/us/politics/russia-sees-mid term-elections-as-chance-to-sow-fresh-discord-intelligence-chiefs-warn.html (дата обращения: 20.12.2022). – Текст : электронный.

373. Russia’s Putin: Panama Papers Area ‘Provocation // Reuter. 2016. URL: https://www.reuters.com/article/us-russia-putin-panamapapers/russias-putin-pana ma-papers-are-a-provocation-idUSKCN0XB16D (дата обращения: 05.01.2023). – Текст : электронный.

374. RussiaBeyondTheHeadlines передали управляющей телеканалом RT компании Текст : электронный // РБК. 2017. URL: https://www.rbc.ru/technology_and_ media/09/01/2017/587399da9a7947c7cccd70f3 (дата обращения: 20.09.2022). – Текст : электронный.

375. Seddon, M. Documents Show How Russia’s Troll Army Hit America / M. Seddon // Buzzfeed News. 02.01. 2014. URL: https://www.buzzfeednews.com/article/max seddon/documents-show-how-russias-troll-army-hit-america (дата обращения: 05.01.2023). – Текст : электронный.

376. Smith, R. Columbia Chemical Hoax Tracked to ‘Troll Farm’ Dubbed the Internet Research Agency / R. Smith // News. 2015. URL: https://www.news.com.au/techno logy/online/social/columbia-chemical-hoax-tracked-to-troll-farm-dubbed-the-internet-research-agency/news-story/ 128af54a82b83888158f7430136bcdd1 (дата обращения: 05.02.2023). – Текст : электронный.

377. Soldatov, A. How Edward Snowden Inadvertently Helped Vladimir Putin’s Internet Crackdown / A. Soldatov, I. Borogan // BuzzFeedNews. 2015. URL: https://www. buzzfeednews.com/article/andreisoldatov/how-edward-snowden-inadvertenly-hel ped-vladimir-putins-inter (дата обращения: 05.01.2023). – Текст : электронный.

378. Taylor, A. Putin Saw the Panama Papers as a Personal Attack and May Have Wanted Revenge, Russian Authors Say / A. Taylor // Washington Post. 2017. URL: https:// www.washingtonpost.com/news/worldviews/wp/2017/08/28/putin-saw-the-panama-papers-as-a-personal-attack-and-may-have-wanted-revenge-russian-authors-say (дата обращения: 05.01.2023). – Текст : электронный.

379. There’s no proof to show Huawei was spying in Europe, France says // The print. 2020. URL: https://theprint.in/world/theres-no-proof-to-show-huawei-was-spying-in-europe-france-says/357011/ (дата обращения: 20.12.2021). – Текст : электронный.

380. Timberg, C. Russian Propaganda Effort Helped Spread ‘Fake News’ During Election, Experts Say / C. Timberg // Washington Post. 2016. URL: https://www.washingtonpost.com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election-experts-say/2016/11/24/793903b6-8a40-4ca9-b712-716af660 98fe_story.html (дата обращения: 20.01.2023). – Текст : электронный.

381. Troianovski, A. How Russia’s Military Intelligence Agency Became the Covert Muscle in Putin’s duels with the West / A. Troianovski, E. Nakashima // Washington Post. 2018. URL: https://www.washington post.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html (дата обращения: 10.01.2023). – Текст : электронный.

382. Trump administration hits China's Huawei with one-two punch // Reuters. 2019. URL: https://www.reuters.com/article/us-usa-china-trump-telecommunications/trump-administration-hitschinas-huawei-with-one-two-punch-idUSKCN1SL2QX (дата обращения: 06.12.2021). – Текст : электронный.

383. Trump’s blacklisting of Huawei is failing to halt its growth // Bloomberg. 2020. URL: https://www.bloomberg.com/news/articles/2020-01-06/ trump-s-blacklisting-of-huawei-is-failing-to-halt-its-growth (дата обращения: 06.12.2021). – Текст : электронный.

384. U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations // U.S. Department of Justice, Office of Public

Affairs. 2018. URL: https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and (дата обращения: 20.01.2023). – Текст : электронный.

385. Wintour, P. US urges Britain to take another 'hard look' at letting Huawei into 5G / P. Wintour // TheGuardian. 2020. URL: https://www.theguardian.com/technology/2020/feb/14/us-urges-britain-to-take-another-hard-look-at-letting-huawei-into-5g (дата обращения: 10.12.2021). – Текст : электронный.

386. Аганбегян, А. Российский академик оценил стоимость военной операции в 1 млрд долларов в день / А. Аганбегян // Капитал страны. 16.01.2023. URL: https://kapital-rus.ru/news/392921-rossiiskii_akademik_ocenil_stoimost_voennoi_ operacii_v_1_mlrd_dollar/ (дата обращения: 01.02.2023). – Текст : электронный.

387. Аналитики заявили о росте кибератак на критическую инфраструктуру на 150 % // РБК. 12.07.2021. URL: https://www.rbc.ru/technology_and_media/12/07/2021/60eb7ca69a7947b2f91f6a8d (дата обращения: 20.11.2022). – Текст : электронный.

388. Баулз, У. RussiaToday: СМИ нового образца? / У. Баулз // ИноСМИ. 05.07.2011. URL: http://www.inosmi.ru/politic/20110705/ 171615730.html (дата обращения: 16.10.2022). – Текст : электронный.

389. В Вооружённых силах создают войска информационных операций // Независимое военное обозрение. 2014. URL: https://nvo.ng.ru/concepts/2014-05-16/2_red.html (дата обращения: 15.12.2022). – Текст : электронный.

390. В МГУ открылась магистерская программа «Информационные и гибридные войны» // ТАСС. 2022. URL: http://www.kremlin.ru/ acts/bank/29288 (дата обращения: 25.07.2022). – Текст : электронный.

391. В Минобороны заявили, что США начали против России ментальную войну // РИА НОВОСТИ. 2021. URL: https://ria.ru/20210325/ ssha-1602735487.html (дата обращения: 15.06.2022). – Текст : электронный.

392. В Минобороны обвинили Запад в развязывании ментальной войны с РФ // Известия. 2021. URL: https://iz.ru/1142000/2021-03-25/v-minoborony-obvinili-zapad - v-razviazyvanii-mentalnoi-voiny-s-rf(дата обращения: 15.06.2022). – Текст : электронный.

393. В Минобороны РФ создали войска информационных операций // Интерфакс. 2017. URL: https://www.interfax.ru/russia/551054 (дата обращения: 15.12.2022).

394. В Минобрнауки поддержали введение курса по изучению гибридных войн в вузах // ТАСС. 2022. URL: https://tass.ru/obschestvo/ 15212025?utm_source google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 25.07.2022). – Текст : электронный.

395. В Минске опубликовали «перехваченный разговор Варшавы и Берлина» // РБК. 2020. URL: https://www.rbc.ru/politics/04/09/2020/ 5f527c719a7947ab31a92a85 (дата обращения: 15.09.2022). – Текст : электронный.

396. В России уже заблокированы Twitter и Facebook // Super. 2022. URL: https://super. ru/l/socialmediainrussia22 (дата обращения: 10.10.2022). – Текст : электронный.

397. Встреча с представителями общественности по вопросам патриотического воспитания молодёжи // Президент России. 2012 URL: http://www.kremlin.ru/ events/president/news/16470 (дата обращения: 20.10.2022). – Текст : электронный.

398. Замахина, Т. Принят закон о контроле за деятельностью иноагентов / Т. Замахина // Российская газета. 2022. URL: https://rg.ru/ 2022/06/29/priniat-zakon-o-kontrole-za-deiatelnostiu-inoagentov.html (дата обращения: 24.10.2022). – Текст : электронный.

399. Информационное противоборство отработали на «Кавказе-2016» // Известия. 2016. URL: https://iz.ru/news/632393 (дата обращения: 15.12.2022). – Текст : электронный.

400. Информационные и гибридные войны: как совершить прорыв в области гуманитарных технологий и противодействовать угрозам // Россия Сегодня.

2019. URL: http://pressmia.ru/pressclub/20190606/ 952378627.html (дата обращения: 25.07.2022). – Текст : электронный.

401. Исследование показало рост влияния RT во Франции // RT. 2019. URL: https://russian.rt.com/world/news/643260-rt-france-issledovanie(дата обращения: 17.11.2022). – Текст : электронный.

402. Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций // ТАСС. 2014. URL: https://tass.ru/politika/1179830 (дата обращения: 15.12.2022). – Текст : электронный.

403. Кибервойска появятся в армии до конца года // Москва. 2013. URL: https:// www.m24.ru/articles/Minoborony/05072013/20906 (дата обращения: 15.12.2022). – Текст : электронный.

404. Китайский Интернет подвергается иностранным кибератакам // Cyberspace Administration of China. 2022. URL: http://www.cac.gov. cn/2022-03/11/c_16 48615063553513.htm (дата обращения: 01.02.2023)（我国互联网遭受境外网络攻击 // 中国国家互联网信息办公室.11.03.2022). – Текст : электронный.

405. Китайский мозговой центр опубликовал первый в мире Отчёт о санкции Запада против России // CHINANEWS. 2022. URL: https://www.chinanews. com.cn/cj/2022/04-02/9718600.shtml (дата обращения: 15.04.2022) (中国智库发布首份美国对俄制裁评估报告 // 中国新闻网. 2022 年 4 月 2 日). – Текст : электронный.

406. Лавров заявил, что Россия ведёт с Западом уже не гибридную войну // РИА НОВОСТИ. 2023. URL: https://ria.ru/20230123/rossiya-1846778090.html (дата обращения: 28.01.2023). – Текст : электронный.

407. Лавров обвинил Запад в «нечистоплотности» в отношении России и КНР // NEWS. 2022. URL: https://news.ru/vlast/lavrov-obvinil-zapad-v-nechistoplotnosti-v-otnoshenii-rossii-i-knr/ (дата обращения: 01.11.2022). – Текст : электронный.

408. Лидеры ШОС приняли пакет документов по итогам саммита Текст : электронный // РИА НОВОСТЬ. 2020. URL: https://ria.ru/20201110/shos-1583945748. html (дата обращения 11.10.2022). – Текст : электронный.

409. Мероприятия. Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма // Евразийская группа. 2019. URL: https://eurasiangroup.org/ru/events/2019 (дата обращения 11.10.2022). – Текст : электронный.

410. Методики Запада к продвижению цветных революций меняются, к которому Китай должен бдителен // TheGlobalTimes.2020. URL: https://world.huanqiu.com/article/40zcpYrwMO3 (дата обращения: 20.07.2022) (西方推动“颜色革命”方式正发生变化中国应保持警惕 // 环球时报.06.12.2020). Текст : электронный.

411. МИД вручил посольству США ноту с требованием не вмешиваться в дела России // РИА НОВОСТИ. 2023. URL: https://ria.ru/20230207/ssha-1850326734.html (дата обращения: 20.01.2023). – Текст : электронный.

412. МИД РФ назвал задачи нового 42-го департамента // Интерфакс. 2019. URL: https://www.interfax.ru/russia/689780 (дата обращения: 01.11.2022). – Текст : электронный.

413. Министерство юстиции и Национальное управление по пропаганде права КНР развёртывают кампанию по пропаганде права на 2020 г. в рамках Дня образования в области национальной безопасности // Синьхуа. 2020. URL: http://www.xinhuanet.com/legal/2020-04/07/c_1125823054.htm (дата обращения: 12.06.2022) (司法部、全国普法办部署开展 2020 年全民国家安全教育日普法宣传活动 // 新华网.07.04.2020.). – Текст : электронный.

414. Минобороны России прорабатывает вариант создания гуманитарных научных рот Текст : электронный // ТАСС. 2013. URL: https://nauka.tass.ru/nauka/631973 (дата обращения: 15.12.2022). – Текст : электронный.

415. Мир находится в разгаре великих перемен, невиданных за столетие // BeijingDaily. 2019. URL: https://ie.bjd.com.cn/bjd/Html/

20190114/0/7ED2E8CD5F30C
46A_Phone.html?newsid=7ED2E8CD5F30C46A&from=groupmessage&isappinstalled=0 (дата обращения 28.01.2023) （世界处于百年未有之大变局 // 北京日报. 2019 年 1 月 14 日）. – Текст : электронный.

416. На учениях «Кавказ-2016» впервые отработали «информационное противоборство» // РИА НОВОСТИ. 2016. URL: https://ria.ru/20160914/1476902330.html (дата обращения: 15.12.2022). – Текст : электронный.

417. Нарышкин поздравил МИА «Россия сегодня» с 80-летием // РИА НОВОСТЬ. 2021. URL: https://ria.ru/20210624/yubiley-173835 6654.html (дата обращения: 10.05.2021). – Текст : электронный.

418. О дальнейшем совершенствовании Горячей линии правительственных услуг Текст : электронный // Центральное народное правительство КНР. 2021. URL: http://www.gov.cn/zhengce/2021-01/08/content_5577884.htm (дата обращения: 20.10.2021)(政务服务便民热线有了“总客服” // 中华人民共和国中央人民政府. 08.01.2021). – Текст : электронный.

419. О ситуации в Белоруссии // СВР РФ. 2020 г. URL: http://www.svr.gov.ru/smi/2020/09/o-situatsii-v-belorussii-2.htm (дата обращения: 15.09.2022). – Текст : электронный.

420. Образовано Управление по общественным проектам // Президент России. 2012 URL: http://www.kremlin.ru/events/president/news/16692 (дата обращения: 25.10.2022). – Текст : электронный.

421. Особый фронт // Аргументы времени.2018. URL: https://svgbdvr.ru/voina/osobyi-front (дата обращения: 10.01.2023). – Текст : электронный.

422. Отец Всемирной паутины поспорил с Путиным об интернете как проекте ЦРУ // РБК. 2014. URL: https://www.rbc.ru/technology_and_media/11/12/2014/5489a
91d2ae5960852e224e9 (дата обращения: 05.01.2023). – Текст : электронный.

423. Патрушев заявил, что Запад балансирует между гибридной войной и открытым конфликтом с РФ // ТАСС. 2022. URL: https://tass.ru/ politika/15511991 (дата обращения: 10.01.2023). – Текст : электронный.

424. Патрушев призвал Россию и Китай усилить готовность к взаимной поддержке // РИА НОВОСТЬ. 2022. URL: https://ria.ru/20220919/ kitay-1817822340.html (дата обращения 20.09.2022). – Текст : электронный.

425. Посол США в России назвала странным и средневековым понятие «англосаксы» Текст : электронный // РБК. 2023. URL: https://www.rbc.ru/rbcfreenews/644 ac8469a7947383e0ff8b0 (дата обращения: 20.04.2023). – Текст : электронный.

426. Представители оборонных ведомств государств – членов ОДКБ обсудили вопросы профилактики и борьбы с коронавирусной инфекцией COVID-19 // ОДКБ. 2020. URL: https://odkb-csto.org/news/news_odkb/predstaviteli-oboronnykh-vedomstv-gosudarstv-chlenov-odkb-obsudili-voprosy-profilaktiki-i-borby-s-ko/#loaded (дата обращения 11.10.2022). – Текст : электронный.

427. Президент подписал Указ об органах, участвующих в обмене информацией в сфере противодействия легализации доходов, полученных преступным путем // Федеральная служба по финансовому мониторингу. 2022. URL: https://www.fedsfm.ru/special/releases/5945(дата обращения 20. 08. 2022). – Текст : электронный.

428. Путин подписал закон об иноагентах // РИА НОВОСТЬ. 2022. URL: https://ria.ru/20220714/zakon-1802397942.html (дата обращения: 01.11.2022). – Текст : электронный.

429. Путин рассказал о состоянии безопасности в России // РИА НОВОСТЬ. 2022. URL: https://ria.ru/20221025/putin-1826724536.html (дата обращения: 25.10.2022). – Текст : электронный.

430. Путин, В. В. Патриотизм – прочный фундамент будущего России» / В. Путин // Кубанское Казачье Войско. 2012. URL: http://www.slavakubani.ru/p-service/military-service/patriotic-education/vladimir-putin-patriotizm-prochnyy-

fundament-budushchego-rossii/ (дата обращения: 25.10.2022). – Текст : электронный.

431. Путин, В. В. Программа патриотического воспитания должна основываться на базовых ценностях / В. В. Путин // ТАСС. 2019. URL: https://tass.ru/obschestvo/7325009 (дата обращения: 20.10.2022). – Текст : электронный.

432. Роскомнадзор объяснил блокировку сайтов ЦРУ и ФБР дискредитацией армии // РБК. 2023. URL: https://www.rbc.ru/politics/27/01/2023/63d3b5e69a79479d2da 90fd2 (дата обращения: 20.01.2023). – Текст : электронный.

433. Роскомнадзор уведомил «Яндекс.Музыку» о необходимости удалить подкасты BBC // RT. 2022. URL: https://russian.rt.com/russia/news/989886-roskomnadzor-podkasty-bi-bi-si(дата обращения: 10.10.2022). – Текст : электронный.

434. Россия выигрывает информационную борьбу у Запада, заявил Киселев // РИА НОВОСТЬ. 2018. URL: https://ria.ru/20180912/ 1528348402.html (дата обращения: 10.05.2021). – Текст : электронный.

435. Руководитель администрации президента России – в спецпроекте ТАСС «Первые лица» // ТАСС. 2015. URL: https://tass.ru/top-officials/ 2356242 (дата обращения: 20.10.2022). – Текст : электронный.

436. Рустамова, С. В МИД РФ появится департамент «мягкой силы» / С. Рустамова // NEWS. 2022. URL:https://news.ru/world/v-mid-rf-poyavitsya-departament-mya gkoj-sily/(дата обращения: 01.11.2022). – Текст : электронный.

437. РФ создаёт комиссию по противодействию попыткам фальсификации истории // РИА НОВОСТЬ. 2009. URL: https://ria.ru/20090519/ 171517015.html (дата обращения: 20.10.2022). – Текст : электронный.

438. Скосырев, В. КНР предлагает России вместе бороться с цветными революциями / В. Скосырев // Независимая газета. 2021. URL: https://www.ng.ru/world/ 2021-03-09/1_8097_china.html (дата обращения: 12.06.2022). – Текст : электронный.

439. Снегирев, В. Н. Каким оружием в борьбе с вызовами глобального характера располагает МИД РФ / В. Н. Снегирев // Российская газета. 2021. URL:

https:// rg.ru/2021/11/18/kakim-oruzhiem-v-borbe-s-vyzovami-globalnogo-haraktera-raspolagaet-mid-rf.html(дата обращения: 20.10.2022). – Текст : электронный.

440. Советник министра обороны России рассказал о новом типе войны // РИА НОВОСТИ. 2021. URL: https://ria.ru/20210822/mentalnye-1746750876.html (дата обращения: 15.06.2022). – Текст : электронный.

441. Советник Министра обороны России рассказал, как победить США в «ментальной войне» // RT. 2021. URL: https://russian.rt.com/russia/news/847721-mino borony-mentalnaya-voina-pobeda (дата обращения: 15.06.2022). – Текст : электронный.

442. Советник Шойгу рассказал о «ментальной войне» против России Текст : электронный // Радио Свобода. 2021. URL: https://www.svoboda.org/a/31168918.html (дата обращения: 15.06.2022). – Текст : электронный.

443. Субботина, С. Дума предлагает создать список нежелательных иностранных организаций. С. Субботина // Известия. 2014. URL: http://izvestia.ru/news/579968 (дата обращения: 24.10.2022). – Текст : электронный.

444. США довели группировку своих войск в Европе до 100 тысяч человек // Интерфакс. 2022 URL: https://www.interfax.ru/world/829578 (дата обращения: 25.01.2023). – Текст : электронный.

445. Таможня и КГБ Белоруссии помогли остановить ввоз оружия в Россию с Украины // РИА НОВОСТЬ. 2019 г. URL: https://ria.ru/20190917/1558754175.html (дата обращения: 15.09.2022). – Текст : электронный.

446. Туровский, Д. Пришло наше время послужить России / Д. Туровский // Meduza. 2018. URL: https://meduza.io/feature/2018/08/07/prishlo-nashe-vremya-posluzhit-rossii (дата обращения: 10.01.2022). – Текст : электронный.

447. Туровский, Д. Пришло наше время послужить России / Д. Туровский // Meduza. 2018. URL: https://meduza.io/feature/2018/08/07/prishlo-nashe-vremya-posluzhit-rossii (дата обращения: 10.01.2023). – Текст : электронный.

448. Фетисов В. В. Правовая основа патриотического воспитания граждан Российской Федерации / В. В. Фетисов // Росвоенцентр. 2014. URL:

http://www.ros voencentr-rf.ru/press-tsentr/pravovaya-baza/osnova-patrioticheskogo-vospitani ya.php (дата обращения: 25.10.2022). – Текст : электронный.

449. ФСБ не видит нарушения закона в действиях томских хакеров против сайта «Кавказцентр» // Newsroom. 2002. URL: https://www.newsru.com/russia/04feb2002/tomsk.html (дата обращения: 10.01.2023). – Текст : электронный.

450. Цзинь, Канронг. Интерпретация «беспрецедентные изменения за столетие» / Канронг Цзинь // Наблюдатель. 2020. URL: https://www. guancha.cn/JinCanRong/2020_10_16_568238.shtml (дата обращения 28.01.2023) (金灿荣：解读“百年未有之大变局” // 观察者网.2020 年 10 月 16 日). – Текст : электронный.

451. Эскалация кризиса в Белоруссии: Особенности протеста и трагедия Лукашенко // EurAsiaDaily. 17 .08 2020 г. URL: https://eadaily.com/ru/news/2020/08/17/ eskalaciya-krizisa-v-belorussii-osobennosti-protesta-i-tragediya-lukashenko (дата обращения: 15.09.2022). – Текст : электронный.