

УДК 34

Информационная безопасность на современном этапе гибридных войн

Габараев Алан Шотаевич

Кандидат политических наук,
ведущий научный сотрудник научно-исследовательского центра,
Академия управления Министерства внутренних дел Российской Федерации,
125993, Российская Федерация, Москва, ул. Зои и Александра Космодемьянских, 8;
e-mail: gabiron@mail.ru

Новиков Алексей Валерьевич

Доктор педагогических наук, кандидат юридических наук, профессор;
главный научный сотрудник,
Научно-исследовательский институт Федеральной службы исполнения наказаний России,
125130, Российская Федерация, Москва, ул. Нарвская, 15-а;
профессор кафедры уголовного права,
Астраханский государственный университет,
414056, Российская Федерация, Астрахань, ул. Татищева, 20-а;
профессор кафедры частного права,
Пермский институт Федеральной службы исполнения наказаний России,
614012, Российская Федерация, Пермь, ул. Карпинского, 125;
e-mail: novikov.pra vo@mail.ru

Слабкая Диана Николаевна

Старший научный сотрудник,
Научно-исследовательский институт Федеральной службы исполнения наказаний России,
125130, Российская Федерация, Москва, ул. Нарвская, 15-а;
e-mail: sdn10.70@mail.ru

Аннотация

Информационная безопасность становится все более значимой в условиях современных гибридных войн. В эпоху, когда технологии присутствуют повсеместно, защита информации приобретает стратегическое значение. Гибридные войны, объединяющие классические военные действия с кибератаками, дезинформацией и экономическим, санкционным давлением, требуют нового подхода к информационной безопасности, в том числе для таких структур, как уголовно-исполнительная система России. Информационная безопасность в УИС России в условиях современных гибридных войн является критически важным аспектом, который требует постоянного внимания и развития. В условиях, когда информационные атаки становятся все более изощренными и труднопредсказуемыми, устоявшиеся методы защиты данных нуждаются в постоянной адаптации и модернизации. Статья посвящена разрешению актуальной проблемы

национальной безопасности России – информационному противоборству в условиях гибридных войн. Рассмотрен один из элементов гибридных войн – информационный терроризм. Объектом исследования выступает «информационная составляющая гибридных войн» и их влияние на национальную безопасность Российской Федерации. Дана целевая характеристика информационных угроз в условиях гибридной войны. Показаны ненасильственные (стратегии «мягкой силы») стратегии современной международной политики и их использование для изменения сложившегося статуса-кво. Определены способы и технологии гибридной деятельности современных акторов международной политики: военной и гибридной, традиционной и иррегулярной, явной и скрытой, государственной и негосударственной. Исследовано влияние информационных угроз и гибридных войн на принятие политических решений и национальную безопасность России.

Для цитирования в научных исследованиях

Габараев А.Ш., Новиков А.В., Слабкая Д.Н. Информационная безопасность на современном этапе гибридных войн // Вопросы российского и международного права. 2024. Том 14. № 10А. С. 50-58.

Ключевые слова

Безопасность общества, уголовно-исполнительная система, кибербезопасность, информационная безопасность, гибридная война, прокси войны, национальная безопасность России.

Введение

Информационная безопасность выступает ключевым элементом защиты государственной инфраструктуры и данных. В рамках УИС России это включает в себя защиту данных, передаваемых и хранящихся в учреждениях системы, а также информацию, связанную с управлением и контролем деятельности в учреждениях ФСИН России. Учитывая специфичность задач, осуществляемых правоохранительными органами, информационная безопасность должна рассматриваться как комплексная проблема, требующая интеграции новейших технологий и стратегий.

Основное содержание

Современные гибридные конфликты предполагают использование кибератак для подрыва национальной безопасности. Важным аспектом является предотвращение утечки конфиденциальных данных, которые могут быть использованы для шантажа или создания напряженности в обществе. УИС России нуждаются в укреплении своих «кибер-рубежей», что включает обучение персонала, повышение их осведомленности о киберугрозах, а также внедрение современных технологий защиты информации.

В УИС обеспечение информационной безопасности регулируется федеральным законодательством, в том числе федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который закрепляет правовые основы борьбы с преступлениями против безопасности важнейших для российского общества и государства информационных и автоматизированных систем, информационно-телекоммуникационных сетей, с преступлениями, совершаемыми с

использованием компьютерной техники, сети Интернет, включая ответственность за незаконные действия в сфере информационных технологий, защиту от кибератак и др. [Попова, 2024, с. 52].

Значимая роль отводится разработке и использованию программного обеспечения, которое может противостоять современным киберугрозам. Обеспечение информационной безопасности требует постоянного мониторинга сетей, применения криптографических методов защиты и разработки адаптивных мер реагирования на внештатные ситуации. В условия гибридной войны это приобретает особое значение, так как быстрота и эффективность ответной реакции могут стать решающими для предотвращения катастрофических последствий.

Также стоит уделить внимание потребности в обмене опытом и сотрудничестве с международными партнерами – дружественными странами. Гибридные войны зачастую пересекают государственные границы, и создание межведомственных и международных альянсов может усилить защитные меры каждой из участвующих стран [Родачин, 2019]. Это также предоставляет возможность совместной разработки технологий и стратегий, соответствующих текущим вызовам.

Отметим, что современные гибридные войны характеризуются комбинированием традиционных военных действий и кибервойн, что значительно усложняет задачи, стоящие перед управлением информационной безопасностью в рамках УИС России. В такие периоды противник может применять разнообразные стратегии, включающие в себя атаки на информационную инфраструктуру, манипуляцию общественным мнением, распространение дезинформации и кибершпионаж. Это диктует необходимость многоуровневой защиты, включающей технические, организационные и правовые меры.

На фоне постоянно изменяющейся локации угроз, УИС России предстоит комплексная трансформация своих подходов к информационной безопасности. Это включает в себя интеграцию новейших технологий, подготовку квалифицированных кадров и разработку новых стратегий реагирования на гибридные угрозы. Основной задачей остается обеспечение защиты данных и устойчивости систем управления, что является фундаментом национальной безопасности в современных условиях.

На техническом уровне это подразумевает внедрение новейших решений в области криптографии, многофакторной аутентификации и продвинутых систем обнаружения угроз. Кроме того, важно обеспечить постоянное обновление программного обеспечения и защитных систем, а также обучение персонала по противодействию возможным атакам.

Организационные методы включают в себя строгий контроль доступа к конфиденциальной информации, формирование культуры информационной безопасности среди сотрудников и разработку четких стратегий реагирования на инциденты. Необходимо внедрять системы раннего предупреждения и мониторинга, которые позволяют своевременно выявлять угрозы и минимизировать потенциальный ущерб.

Современный мировой порядок основанный на тотальной (гибридной) войне из-за перезагрузки международных отношений после распада СССР, характеризуется глобализацией и формированием мегаобщества, ослаблением суверенитета национального государства, подменой политики экономикой в контексте реализацией стратегии внешней политики США и НАТО по формированию однополярного мира на основе политики доминирования и идеологии «избранности» и «дивного сада».

Поэтому попытки коллективного Запада дискредитировать Россию, признать ее террористическим государством – спонсором терроризма необходимо понимать как средство агрессивной пропаганды, связанной с лидерством России в международном сопротивлении по

установлению тоталитарной власти глобального «сверхобщества», при котором НАТО во главе с США будут выполнять роль мирового жандарма.

Миропорядок представляет собой сложную систему, состоящую из комплекса взаимодополняющих процессов – идеологических, военных, политических, религиозных и националистических, криминальных [Макаров, 2005], где информационный терроризм является одним из элементов гибридной войны – новой технологии борьбы за переустройство мира на современном этапе.

Несмотря на глобальные геополитические перемены в международных отношениях, Россия сохраняет свой великодержавный статус в мировом сообществе. В тоже время необходимо понимать, что в условиях процесса глобализации международных отношений, геостратегическое положение России на международной арене будет определяться возможностью обеспечения и защиты национальных интересов. Одним из них является проблема обеспечения суверенитета и территориальной целостности Российской Федерации, которая особенно актуализировалась в эпоху в том числе информационного противоборства [Бровко, 2021].

Указанные обстоятельства, позволяют выдвинуть гибридную войну в ряд наиболее актуальных угроз для национальной безопасности Российского государства. Теория гибридной войны порождена также новыми информационными и технологическими возможностями в современном мире применительно к социально-психологической, политической и военной деятельности [Колесников, 2020].

На сегодня совершенно очевидно, что кризис на Юго-Востоке Украины по сути является непрямым противостоянием России и НАТО во главе с англосаксами и носит характер гибридной войны еще со времен холодной войны, где США вели борьбу против СССР методами гибридной войны. Важно осознать, что гибридная война коллективного Запада против России после окончания холодной войны превратилась в новую форму межгосударственного противоборства. Современный мир вступил в эпоху хаотизации международных отношений. Причем, как военными аналитиками и ученым сообществом, так и политиками все больше говорят о возможности возникновения Третьей мировой войны.

По мнению политолога Сергея Кургияна, современной краеугольной доктриной США является «средняя война в средней зоне». Применительно к реальной политике, американская стратегия, нацеленная на пересмотр фундаментальных констант устройства мира, экспериментально проверяет, например, переплетением конфликтов вокруг Украины «кто чего стоит и кто что может» - в «серой зоне», конвенционально, «на территории, на какой можно»: чтобы поняв это, начать «какую-то следующую фазу». На украинском театре гибридной войны задействована концепция «серой зоны», включающая в себя прокси-войну, и кибервойну [www, Вертлиб].

Согласимся с мнением В.Ю. Лукьянова: «...будем надеемся такой сценарий маловероятен и противостояние между государствами все больше будет уходить именно в сферу «несиловой» войны просветительского и пропагандистского воздействия... [Лукьянов, 2021].

Украинский кризис предельно обострил противоречие между американоцентричным проектом мирового лидерства и полицентричным проектом международного сотрудничества, которой привержены Россия, Китай, Индия и многие другие страны. Агрессивная риторика западных политиков дошла до того, что поднялась политическая дискуссия о признании России террористическим государством или страной – спонсором терроризма или страной, использующей террористические методы [www]. Запад определял действия России в таких нарративах как «российская оккупационная армия» и «преступная политика Москвы», которая квалифицировалась в качестве террористических действий. Таким образом происходит «разложение терроризма на другие смыслы», которые позволяют использовать терроризм, как

клише, повод и предлог для решения геополитических задач военной стратегии США и его союзников.

Жупел (прим. авт. в церковнославянском языке – горящая сера, в переносном смысле – нечто пугающее, внушающее ужас) «международного терроризма» активно используется как технология гибридной войны с целью создания политической нестабильности в различных странах и регионах мира. В частности, американская «мягкая сила», в качестве устойчивого политического клише, успешно используется при организации «цветных революций» [Алферов, 2020], которые являются внешнеполитическим инструментом США для обеспечения глобального доминирования в контексте формирования нового миропорядка. В этой связи необходимо объективно оценивать наших настоящих стратегических противников.

Подобное воздействие оказывается и на Россию. По словам заместителя председателя Совета безопасности России Дмитрия Медведева «США открыто ведут гибридную войну против России, поставляя оружие Украине, отправляя своих военных специалистов и используя работу разведки» [<https://lenta.ru>].

Очевидно, что основной целью развязанной гибридной войны коллективного Запада против нашей страны является ликвидации российской государственности, разделение страны на «удельные княжества» с последующим переводом под внешний контроль. В реализации указанной геополитической стратегии, будут использоваться существующие проблемы внутренней безопасности Российской Федерации в сфере межэтнических, религиозных и социально-экономических и других отношений.

Отметим, что юг России – самая уязвимая территория в отечественном геополитическом пространстве. Здесь в полной мере проявляется вся сложность и неоднозначность проблемы терроризма, так как этот регион России содержит критический уровень противоречий в сфере национально-государственного устройства, межэтнических отношений, которые осложняются конфессиональным фактором, в большей мере внесенным искусственно извне международными экстремистскими и террористическими организациями [Вольхина, 2014, с.176]. В целом, обеспечение устойчивости в этом регионе представляет собой приоритетное направление защиты государственной безопасности и государственных интересов нашей страны.

Следующей проблемой, требующей своего разрешения является увеличение масштабов международной миграции. Так, по официальным данным, в 2023 году на 42,4 % увеличилось количество иностранных граждан, прибывающих в Российскую Федерацию в визовом порядке с целью осуществления трудовой деятельности. При этом большинство рабочих виз было оформлено гражданам Китая, Вьетнама, Индии, Турции [МВД РФ].

По сведениям члена Совета при президенте Российской Федерации по межнациональным отношениям, члена Общественного совета при МВД России, доктора политических наук Владимира Александровича Волоха, в настоящее время в Российской Федерации находится около 6,5 млн. иностранных граждан [<https://nsn.fm>]. Безусловно миграция имеет свои положительные и отрицательные стороны для экономики страны. Положительные связаны с трудовой миграцией: пополнением убыли населения, восполнением недостатка в определенных областях промышленности. В тоже время, массовая миграция превращается в серьезный источник обострения социально-экономической обстановки в любой стране мира.

Заключение

Особое место в системе угроз национальной безопасности принадлежит информационной безопасности. По словам министра иностранных дел Российской Федерации «Запад ведет

информационную войну против России, она включает элементы информационного терроризма».

Действительно, на сегодня качество и уровень глобального информационного и социокультурного воздействия на сознание и психику нашего населения можно смело охарактеризовать как информационный терроризм. Эта война направлена на поражение массового сознания российского общества, слом культурного кода страны и цивилизационную перевербовку, которая разрушает национальный менталитет и самобытность российского общества способствует расшатыванию и ослаблению конституционного строя России.

Информационная и культурная глобализация создает все возможности для манипулирования общественным сознанием, сознательной дезинформации, особенно молодежи. Следует отметить, что западные культуртрегеры формально декларируют, как правило, чисто просветительские и образовательные цели, но по факту преследуют переформатирование сознание населения России в целях нанести ущерб ее национальным интересам.

В условиях гибридных войн информационная безопасность становится не только средством защиты данных, но и важным инструментом национальной безопасности и суверенитета. УИС России, действуя в современных реалиях, должна быть готова к быстрому реагированию на любые потенциальные угрозы, обеспечивая информационную защиту государственных интересов и безопасности граждан. Информационная безопасность в современном мире требует постоянного развития и совершенствования, чтобы оставаться на шаг впереди потенциальных угроз.

Библиография

1. Федеральный закон «О противодействии терроризму» от 06.03.2006 № 35-ФЗ // СПС КонсультантПлюс (дата обращения: 25.07.2024).
2. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ: https://www.consultant.ru/document/cons_doc_LAW_220885/
3. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»// СПС КонсультантПлюс (дата обращения: 25.06.2024).
4. «Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»// СПС Консультант Плюс (дата обращения: 25.06.2024).
5. Алферов, С. Ю. Фактор «мягкой силы» в процессе подготовки и осуществления «цветных революций» / С. Ю. Алферов // Вестник Поволжского института управления. – 2020. – Т. 20, № 1. – С. 43-49. – DOI 10.22394/1682-2358-2020-1-43-49. – EDN HSLYVO.
6. Бровко, В. Ю. Особенности реализации информационного суверенитета государства в условиях нарастания гибридного противоборства / В. Ю. Бровко, Л. Н. Гарас // Вестник Московского университета. Серия 12: Политические науки. – 2021. – № 1. – С. 14-32. – EDN LHVGGK.
7. Бушкова, А. Ю. Технологии информационного воздействия на государственность российской Федерации: пути противодействия / А. Ю. Бушкова // Манускрипт. – 2018. – № 9(95). – С. 63-67. – DOI 10.30853/manuscript.2018-9.13. – EDN XYQAUP.
8. Вольхина А.В. Винник Ю.О. Терроризм как глобальная проблема человечества// Политические институты и процессы. – 2014. – № 2. С. 175-179
9. Евгений Вертлиб Рецензия на монографию Л.В. Савина «Гибридная война и серая зона». М.: Евразийское движение, 2022. - 180 с., с ил. С 13 ISBN 978-5-521-18587-0, <https://www.geopolitika.ru/article/slozhnye-konflikt-y-gibridnaya-voyna-i-seraya-zona>
10. Гринин, Л. Е. Новый мировой порядок и эпоха глобализации. Ст. 1. Американская гегемония: апогей и ослабление. Что дальше? / Л. Е. Гринин // Век глобализации. – 2015. – № 2(16). – С. 3-17. – EDN UNSMQF.
11. Давитадзе, М. Д. Основы сосуществования однополярного и многополярного мира / М. Д. Давитадзе // Вестник Московского университета МВД России. – 2023. – № 4. – С. 75-77. – DOI 10.24412/2073-0454-2023-4-75-77. – EDN VFETWA.
12. Интернет-источник, "Мир знает, кто вы": европейцев взбесила резолюция Европарламента о России: <https://ria.ru/20221123/rezolyutsiya-1833730973.html>

13. 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. – EDN DHTJCG.
14. Лукьянов, В. Ю. Гибридные войны как угроза безопасности в XXI веке / В. Ю. Лукьянов // Вестник Северного (Арктического) федерального университета. Серия: Гуманитарные и социальные науки. – 2021. – Т. 21, № 3. – С. 5-14. – DOI 10.37482/2687-1505-V098. – EDN HARZMD.
15. Макаров, Н. Е. Экстремизм как фактор глобальной опасности / Н. Е. Макаров // Известия Алтайского государственного университета. – 2005. – № 4(37). – С. 048-053. – EDN RDPJPZ.
16. Министерство внутренних дел Российской Федерации: [официальный сайт]//Результаты деятельности подразделений по вопросам миграции территориальных органов МВД России за январь – декабрь 2023 года. URL: <https://мвд.рф/dejatelnost/statistics/migracionnaya/item/47183542/>
17. Национальная Служба Новостей: [Электронный ресурс]. URL: <https://nsn.fm/society/v-rossii-na-2024-god-nahodyatsya-65-mln-inostrannyh-grazhdan>
18. Попова А. Д. Обеспечение информационной безопасности учреждений и органов уголовно-исполнительной системы Российской Федерации // Вестник Прикамского социального института. 2024. № 2 (98). С. 51–55. EDN: MAIMUI.
19. Родачин, В. М. Гибридные войны и обеспечение национальной безопасности России / В. М. Родачин // Гуманитарные науки. Вестник Финансового университета. – 2019. – Т. 9, № 4(40). – С. 93-99. – DOI 10.26794/2226-7867-2019-9-4-93-99. – EDN DLKCCK.
20. Российское новостное интернет-издание «Лента.ру» [сайт]. URL: <https://lenta.ru/news/2024/03/19/medvedev-otsenil-vozmozhnost-peregovorov-s-ssha-posle-prizyva-vashingtona/>
21. Соломатин, Е. В. Социально-психологические основы информационно-психологического противоборства в гибридной войне / Е. В. Соломатин // Гуманитарные проблемы военного дела. – 2021. – № 1(26). – С. 137-141. – EDN NUBSL.

Information security at the present stage hybrid wars

Alan Sh. Gabaraev

PhD in Political Science,
Leading Researcher,
Scientific Research Center,
Academy of Management of the Ministry of Internal Affairs of the Russian Federation,
125993, 8, Zoya and Alexander Kosmodemyansky str., Moscow, Russian Federation;
e-mail: gabiron@mail.ru

Aleksei V. Novikov

Doctor of Pedagogy, PhD in Law, Professor;
Chief Researcher,
Scientific-Research Institute of the Federal Penitentiary Service of the Russian Federation,
125130, 15-a, Narvskaya str., Moscow, Russian Federation;
Professor of the Department of Criminal Law,
Astrakhan State University,
414056, 20-a, Tatishcheva str., Astrakhan, Russian Federation;
Professor of the Department of Private Law,
Perm Institute of the Federal Penitentiary Service of the Russian Federation,
614012, 125, Karpinskogo str., Perm, Russian Federation;
e-mail: novikov.pravo@mail.ru

Diana N. Slabkaya

Senior Researcher,
Scientific-Research Institute of the Federal Penitentiary Service of the Russian Federation,
125130, 15-a, Narvskaya str., Moscow, Russian Federation;
e-mail: sdn10.70@mail.ru

Abstract

Information security is becoming more and more significant in the conditions of modern hybrid wars. In the era, when technologies are present everywhere, information protection is acquired by strategic importance. Hybrid wars, uniting classical military operations with cyber ends, disinformation and economic, sanctioning pressure, require a new approach to information security, including for structures such as the Russian criminal-executive system. Information security in the Russian penal system in the conditions of modern hybrid wars is a critical aspect that requires constant attention and development. In conditions when information attacks become more and more sophisticated and difficult to predict, established data protection methods need constant adaptation and modernization. The article is devoted to the resolution of the urgent problem of the national security of Russia - information confrontation in the conditions of hybrid wars. One of the elements of hybrid wars is considered - information terrorism. The object of the study is the “information component of hybrid wars” and their influence on the national security of the Russian Federation. The target characteristic of information threats in the conditions of a hybrid war is given. Non-violent (“soft power” strategies) strategy of modern international policy and their use are shown to change the current status-quo. The methods and technologies of hybrid activity of modern actors of international politics are determined: military and hybrid, traditional and irregular, obvious and hidden, state and non-state. The influence of information threats and hybrid wars on the adoption of political decisions and the national security of Russia has been investigated.

For citation

Gabaraev A.Sh., Novikov A.V., Slabkaya D.N. (2024) *Informatsionnaya bezopasnost' na sovremennom etape gibridnykh vojn* [Information security at the present stage hybrid wars]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 14 (10A), pp. 50-58.

Keywords

Society Security, Criminal-Executive System, Cybersecurity, Information Security, Hybrid War, Proksi of War, National Security of Russia, International Policy.

References

1. Federal'nyj zakon «O protivodejstvii terrorizmu» ot 06.03.2006 № 35-FZ // SPS Konsul'tantPlyus (data obrashcheniya: 25.02.2024).
2. Federal'nyj zakon «O bezopasnosti kriticheskoy informacionnoj infrastruktury Rossijskoj Federacii» ot 26.07.2017 № 187-FZ: https://www.consultant.ru/document/cons_doc_LAW_220885/
3. Ukaz Prezidenta RF ot 02.07.2021 № 400 «O Strategii nacional'noj bezopasnosti Rossijskoj Federacii»// SPS Konsul'tantPlyus (data obrashcheniya: 25.06.2024).
4. «Ukaz Prezidenta RF ot 5 dekabrya 2016 g. № 646 «Ob utverzhenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii»// SPS Konsul'tant Plyus (data obrashcheniya: 25.06.2024).
5. Alferov, S. Yu. Faktor «myagkoj sily» v processe podgotovki i osushchestvleniya «cvetnyh revolyucij» / S. Yu. Alferov

-
- // Vestnik Povolzhskogo instituta upravleniya. – 2020. – T. 20, № 1. – S. 43-49. – DOI 10.22394/1682-2358-2020-1-43-49. – EDN HSLYVO.
6. Brovko, V. Yu. Osobennosti realizacii informacionnogo suvereniteta gosudarstva v usloviyah narastaniya gibridnogo protivoborstva / V. Yu. Brovko, L. N. Garas // Vestnik Moskovskogo universiteta. Seriya 12: Politicheskie nauki. – 2021. – № 1. – S. 14-32. – EDN LHVQK.
 7. Bushkova, A. Yu. Tekhnologii informacionnogo vozdejstviya na gosudarstvennost' rossijskoj Federacii: puti protivodejstviya / A. Yu. Bushkova // Manuskript. – 2018. – № 9(95). – S. 63-67. – DOI 10.30853/manuscript.2018-9.13. – EDN XYQAYP.
 8. Vol'hina A.V. Vinnik Yu.O. Terrorizm kak global'naya problema chelovechestva// Politicheskie instituty i processy. – 2014. – № 2. S. 175-179
 9. Evgenij Vertlib Recenziya na monografiyu L.V. Savina «Gibridnaya vojna i seraya zona». M.: Evrazijskoe dvizhenie, 2022. - 180 c., s il. S 13 ISBN 978-5-521-18587-0, <https://www.geopolitika.ru/article/slozhnye-konflikty-gibridnaya-voyna-i-seraya-zona>
 10. Grinin, L. E. Novyj mirovoj poryadok i epoha globalizacii. St. 1. Amerikanskaya gegemoniya: apogeji oslablenie. Chto dal'she? / L. E. Grinin // Vek globalizacii. – 2015. – № 2(16). – S. 3-17. – EDN UNSMQF.
 11. Davitadze, M. D. Osnovy sosushchestvovaniya odnopolyarnogo i mnogopolyarnogo mira / M. D. Davitadze // Vestnik Moskovskogo universiteta MVD Rossii. – 2023. – № 4. – S. 75-77. – DOI 10.24412/2073-0454-2023-4-75-77. – EDN VFETWA.
 12. Internet-istochnik, "\"Mir znaet, kto vy\": evropejcev vzbescila rezolyuciya Evroparlamenta o Rossii: <https://ria.ru/20221123/rezolyuciya-1833730973.html>
 13. Kolesnikov, D. I. K probleme sushchnosti i specifiki gibridnoj vojny / D. I. Kolesnikov, A. M. Krivenko // Voennyj akademicheskij zhurnal. – 2020. – № 1(25). – S. 110-114. – EDN DHTJCG.
 14. Luk'yanov, V. Yu. Gibridnye vojny kak ugroza bezopasnosti v XXI veke / V. Yu. Luk'yanov // Vestnik Severnogo (Arkticheskogo) federal'nogo universiteta. Seriya: Gumanitarnye i social'nye nauki. – 2021. – T. 21, № 3. – S. 5-14. – DOI 10.37482/2687-1505-V098. – EDN HARZMD.
 15. Makarov, N. E. Ekstremizm kak faktor global'noj opasnosti / N. E. Makarov // Izvestiya Altajskogo gosudarstvennogo universiteta. – 2005. – № 4(37). – S. 048-053. – EDN RDPIPJZ.
 16. Ministerstvo vnutrennih del Rossijskoj Federacii: [oficial'nyj sajt]//Rezultaty deyatel'nosti podrazdelenij po voprosam migracii territorial'nyh organov MVD Rossii za yanvar' – dekabr' 2023 goda. URL: <https://mvd.rf/deyatelnost/statistics/migracionnaya/item/47183542/>
 17. Nacional'naya Sluzhba Novostej: [Elektronnyj resurs]. URL: <https://nsn.fm/society/v-rossii-na-2024-god-nahodyatsya-65-mln-inostrannyh-grazhdan>
 18. Popova A. D. Obespechenie informacionnoj bezopasnosti uchrezhdenij i organov ugolovno-ispolnitel'noj sistemy Rossijskoj Federacii // Vestnik Prikamskogo social'nogo instituta. 2024. № 2 (98). S. 51–55. EDN: MAIMUI.
 19. Rodachin, V. M. Gibridnye vojny i obespechenie nacional'noj bezopasnosti Rossii / V. M. Rodachin // Gumanitarnye nauki. Vestnik Finansovogo universiteta. – 2019. – T. 9, № 4(40). – S. 93-99. – DOI 10.26794/2226-7867-2019-9-4-93-99. – EDN DLKCKK.
 20. Rossijskoe novostnoe internet-izdanie «Lenta.ru» [sajt]. URL. <https://lenta.ru/news/2024/03/19/medvedev-otsenil-vozmozhnost-peregovorov-s-ssha-posle-prizyva-vashingtona/>
 21. Solomatin, E. V. Social'no-psihologicheskie osnovy informacionno-psihologicheskogo protivoborstva v gibridnoj vojne / E. V. Solomatin // Gumanitarnye problemy voennogo dela. – 2021. – № 1(26). – S. 137-141. – EDN NUBSLS.
-