DOI 10.35775/PSI.2025.66.1.002
УДК 32

А.С. ГАДЖИЕВА
магистрант кафедры
политологии и этнополитики РАНХ и ГС
при Президенте РФ, Россия, г. Москва

С.В. АПАРИН
преподаватель кафедры
информационного обеспечения ОВД
Ростовского юридического института МВД России,
Россия, г. Ростов-на-Дону

Д.К. ГРИГОРЯН
кандидат политических наук,
профессор кафедры политологии и этнополитики РАНХ и ГС
при Президенте РФ, Россия, г. Москва

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЙ АСПЕКТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ СЕТЕВОГО ОБЩЕСТВА

В статье рассматривается возрастание значения информационного аспекта в обеспечении национальной безопасности. В современном сложном информационном мире все большее значение приобретает поиск инновационных путей взаимодействия между отраслями промышленности. Это стремление может способствовать повышению общего качества жизни и снижению потенциальных рисков, связанных с информацией. Поскольку будущие препятствия требуют выявления этих угроз и борьбы с ними, особенно в свете внешних ограничений, в этой статье исследуется значение и роль информационной безопасности в рамках национальной безопасности страны.

Ключевые слова: *национальная безопасность, информационная безопасность, информационная война, информационная интервенция, информационно-психологические операции.*

С появлением информационных технологий социальные связи стали разрастаться на столько, что человек может спокойно общаться с людьми, которые находятся не только в другом городе, но и на другом континенте. Информация и скорость ее распространения приобрели еще большую ценность и огромное влияние на экономику, политику, социальные сферы всех стран нашей планеты без исключений [7. С. 140-145].

Национальная безопасность – состояние защищенности личности, общества и государства от внутренних и внешних угроз. Она включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией и законодательством

Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности.

Важность информации для поддержания национальной безопасности значительно возросла, поскольку эволюция методов коммуникации изменила способы взаимодействия различных субъектов в контексте международных отношений. В современном взаимосвязанном мире обмен жизненно важными данными стал иметь решающее значение для обеспечения безопасности стран и адаптации к глобальной политике. Такое повышенное внимание к информации стимулировало разработку передовых технологий и стратегий для защиты и распространения конфиденциальных данных, тем самым влияя на то, как страны сотрудничают и конкурируют в постоянно меняющейся цифровой среде.

В связи с появлением новых компьютерных и телекоммуникационных технологий, а также развитие сети Интернет, что позволило ускорить появление, передачи и получения данных, на которые сложно быстро реагировать, большую роль начала играть информационно-психологические операции и войны.

Следует подчеркнуть, что в работах российских и зарубежных авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 2; 3; 5; 8; 9; 10; 11; 12; 16; 17; 18; 19; 20; 21; 22; 24].

Однако проблему анализа информационного аспекта в обеспечении национальной безопасности нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Многие исследователи продвигают тезис о том, что войну можно вести более «цивилизованно». Считается, что можно уничтожить суверенитет государства, если изнутри ослабить систему информационного правления.

Внедрение социальных технологий может привести к возникновению различных угроз, в первую очередь направленных на культурную идентичность обществ. Эти угрозы обуславливаются деградацией культурного звена в жизни этих обществ, изменением мировоззренческой структуры в групповом сознании, а также неопределенностью ценностных установок. Более того, историческая память подвергается риску, и, в конечном счете, государственная система претерпевает значительные изменения. Таким образом, социальные технологии могут представлять угрозу культурной целостности, сплоченности мировоззрения, систем ценностей, исторической памяти и стабильности государственной системы.

К примеру, современная политика Запада уделяет большое внимание Украине, которая является после распада СССР развитой республикой с мощным промышленным, аграрным и научным преимуществами. Задача для США и ЕС было вынуждение работать экономику на западный капитал, которой добивались с помощью того, что уничтожали хозяйственный комплекс страны, разрывали экономические, торговые и культурные связи с Россией. Тем самым, Украину сделали источником дешевого продовольствия и сырья для западных

компаний. Запад, используя социальные технологии, создал у населения на Украине ненавистное отношение к России, а также условия для вытравливания памяти о совместном прошлом и взращивания неонацистких настроений [13].

Понятие «информационное противоборство» обозначает соперничество, где используются всевозможные информационные технологии. Оно направлено на то, чтобы достигнуть информационного превосходства над противником [6. С. 139-148].

Самым распространенным методом, который используют противники-государства, является национальные и транснациональные средства массовой информации. Кроме того, применяют информационные сети, способствующие тому, что влиять на мировоззрение, политические взгляды, правосознание, менталитет, духовные идеалы и ценностные установки отдельного человека, так и на общество в целом.

Информационная политика и методы информационного противоборства имеют огромное значение в Соединенных штатах Америки, поэтому исследователи из данной страны больше занимаются изучением понятия «информационное противоборство». Необходимо сказать, что информационная борьба эволюционировала с течением времени благодаря различным факторам, которые сформировали данную операцию в стратегический инструмент управления политическими процессами. Изначально, информационную борьбу рассматривали как средство для решения боевых задача. А теперь является важнейшим элементом глобального политического управления [6].

Если государства находятся в информационной борьбе, то они стремятся к тому, чтобы превосходить над противоборствующей стороной, используя такие различные методы, как дезинформирование, скрытие фактов, иллюзия информационного обилия и многообразия, искажение смысловой нагрузки используемой терминологии [6].

На сегодняшний день даже если страны находятся намного дальше от зоны конфликта, то это не значит, что они не могут пострадать от современных средств уничтожения. Так происходит по той причине, что развивается сетевая информационная и телекоммуникационная инфраструктура, которая позволяет распространять свое влияние на большое расстояние.

Благодаря постоянному развитию и совершенствованию данной системы происходит важное влияние на динамический характер геополитического ландшафта, который всегда расширяется из-за трансформации традиционных ценностей индустриального общества в такую систему ценностей, подходящая информационному обществу. Следовательно, изменения привели к тому, что приоритеты и принципы геополитической конкуренции поменялись, а информационно-психологическое противостояние иметь все больше значение в формировании геополитического баланса сил между конкурирующими объектами.

Геополитический баланс сил включает в себя различные аспекты, такие как информационная война и психологические тактики, которые влияют на восхождение и падение выдающихся геополитических образований. Этот изменчивый процесс может привести к ослаблению традиционных сил и появлению новых, а также к формированию геополитических альянсов.

Наиболее ярко выраженным информационное противоборство явилось в 2003 году в период военных действий на территории Ирака. США в ходе деятельности неправительственных организаций и НКО была создана такая структура, которая привела к краху государственного устройства в Ираке. И характер такой информационной борьбы приобретает на сегодняшний день новые обороты. Так, например, американские информационные войска на протяжении семи лет подготавливают кибервоинов [4. С. 186-195].

Одной из основных задач Министерства обороны США является обеспечение готовности населения противостоять информационной войне. Информационное воздействие охватывает все большие сферы и развивается крпномасштабно. Информационное оружие способно просачиваться, в повседневную жизнь как обычных граждан (через компьютерные игры, скачивание файлов, переходы по сомнительным ссылкам), так и органов гос.управления (взлом серверов, кража информации и т.д.).

Также хотим упомянуть о феномене «Пробирка Пауэлла», который стал поводом для введения американских войск в Ирак. Государственный секретарь США Колин Пауэлл 5 февраля 2003 году в своем выступлении предъявил Совету безопасности ООН пробирку с белым порошком как образец иракского оружия массового уничтожения [14]. Сама речь госсекретаря длилась долго, а пробирку вынул из кармана всего лишь на несколько секунд, но именно этот момент запомнился людям больше всего. Он сказал: «Потребовалось меньше, чем одна чайная ложка спор сибирской язвы в сухой форме в конверте, для того чтобы заставить закрыться Сенат Соединенных Штатов осенью 2001 года. Это заставило сотни людей подвергнуться чрезвычайному медицинскому лечению и привело к гибели двух почтовых работников – и все из-за содержимого того конверта спор, того количества, о котором я сказал». И вот на словах «чайная ложка» Колин Пауэлл достал колбу [14].

Данный прием визуализации был довольно эффектным, но вызвал огромное количество вопросов. Многие были связаны с тем, как секретарь смог пронести отраву в здание ООН, которое охраняется. Позже Пауэлл объяснял, что он хотел напомнить объем чайной ложки, а внутри пузырька была безобидная субстанция. Однако до сих пор в массовом сознании у населения осталось, что госсекретарь США показал на выступлении ООН яд, которым можно истребить тысяча людей [14].

Феномен «Пробирка Пауэлла» является политическим шоу, которое заставила с помощью манипуляции аудиторию поверить в то, что лидер Ирака Саддам Хусейн прячет от мира оружие массового уничтожения. В связи с тем,

что доказательств скрытия ОМУ не хватало, использовали колбу для убедительности речи [14].

Началась американская военная интервенция в Ирак, приведшая к значительному числу жертв. Удивительно, но, несмотря на заявления об оружии массового уничтожения, такие запасы так и не были обнаружены. Впоследствии стало известно, что ЦРУ предоставило Пауэллу неточные данные, касающиеся оружия массового уничтожения, что способствовало оправданию кампании.

Сергей Алексеевич Рябков, заместитель главы Министерства иностранных дел, заявил, что имидж госсекретаря США воспринимается как вредное имя нарицательное, связанное с неискренностью и представлением о том, что правящая элита Соединенных Штатов считает, что у них есть власть приказывать другим странам поддерживать свое господство. Несмотря на то, что ЦРУ предоставило Колину Пауэллу ошибочные данные, его сочли виноватым в этой сложной ситуации. Следовательно, этот метод также стал формой информационной войны [14].

Когда политическая система отличается от норм глобального общества, это может привести к вмешательству в сферу деятельности государства, особенно в отношении данных и информации. Снижение уровня самоуправления стран становится все более актуальной проблемой, поскольку эрозия коммуникаций подрывает суверенитет, способствуя «информационной интервенции». Вышеупомянутая концепция, введенная американским исследователем Э. Прайс-Монро, подчеркивает значительное влияние коммуникаций на независимость нации. По мере ухудшения связи государства становятся более восприимчивыми к манипулированию внешней информацией, что может поставить под угрозу их способность к независимому принятию решений и сохранению их суверенитета. Этот сценарий подчеркивает необходимость надежных коммуникационных сетей для обеспечения автономии и самоопределения наций в нашу эпоху взаимосвязи.

В контексте гражданской войны в Сирии и Соединенные Штаты, и Россия использовали методы информационного вмешательства, используя средства массовой информации для пропаганды противоположных точек зрения. Эта стратегия использовалась для достижения информационного господства, что, в свою очередь, способствовало достижению их соответствующих политических, военных и стратегических целей.

Исследователь подчеркивает ключевую важность управления СМИ и информацией в современных войнах и миротворческих инициативах. Как информационные, так и психологические элементы могут значительно усилить или даже стать основным оружием в конфликтах. Формирование общественного мнения и восприятия с помощью различных медиа-платформ показывает, что информационные интервенции играют решающую роль в формировании геополитического ландшафта.

В современных конфликтах важность информации очевидна, поскольку манипулирование СМИ и формирование общественного мнения стали

важнейшими аспектами современной войны. Гражданская война в Сирии является примером того, как страны используют информационное вмешательство для достижения своих целей и влияния на реальные результаты.

Понимание того, как информационное вмешательство влияет на глобальную политику, имеет решающее значение, поскольку оно оказывает огромное влияние на геополитическую обстановку. Поскольку информация становится важнейшим элементом современной войны, государства должны сохранять бдительность и способность адаптироваться к постоянно меняющемуся ландшафту международных отношений, особенно в том, что касается информационных вмешательств. Участие международных сил в военных операциях подчеркивает центральную роль информационных и психологических элементов в достижении целей вовлеченных сторон. Чтобы заручиться общественной поддержкой своих усилий, эти силы должны сохранять контроль над информационной сферой. Один из примеров применяют в тактике информационной войны. Используя манипулятивные технологии, применяемые в ходе информационных кампаний, лишают человека возможности сознательно и рационально воспринимать информацию. Как правило, моральный и этический аспекты, в ходе реализации информационной кампании, не учитываются. Таким образом, способность формировать общественное мнение и управлять информационной средой имеет решающее значение для успеха военных операций и соблюдения интересов вовлеченных сторон.

Одним из способов информационной войны являются дипфейки. Данное понятие определяется как методика соединения изображений или голосов с помощью искусственного интеллекта, который может «оживлять» фотографии, осуществлять синтез голос человека, заменять лица на видео. Благодаря таким алгоритмам создается контент, который сложно отличить от оригинала (только определенными системами мониторинга можно понять) [15]. Люди могут пользоваться дипфейками как в легальных целях (в кинематографе), так и в целях дезинформации. Такие технологии часто направлены на то, чтобы манипулировать общественным мнением. Например, Украинский Центр информационно-психологических операций (ЦИПсО) в августе 2024 года создал дипфейк с врио губернатора Курской области Алексеем Смирновым. На кадрах ролика «поддельный» Смирнов обращается к курянам. Он заявляет, что принял решение отменить на территории региона новый учебный год и призывает всех срочно покинуть территорию Соловьиного края. Более того, ненастоящий глава региона нагло вступает с утверждением, что якобы «на свой страх и риск договорился с украинской стороной о безопасности при эвакуации». Само собой разумеется, что настоящий врио губернатора Курской области не записывал подобных видео. При создании дипфейка использовались кадры обращения Смирнова к жителям региона по случаю вступления в должность [23].

Также существуют информационные операции, которые могут организовываться специальными службами. Они сопровождаются пропагандой и контрпропагандой в информационном пространстве и дезинформацией противника.

Информационные операции состоят из последовательных вбросов информации, которые провоцируют объект информационного воздействия дать какую-то реакцию на внешний стимул.

В пример можно привести ситуацию со статей из газеты The New York Times, которая была опубликована 24 мая 2019 года. Статья повествует о том, что у Президента РФ есть агент, который работает в ЦРУ. По данным из газеты, сообщается, что этот агент предоставил информацию о «вмешательстве» России в президентские выборы 2016 г. и о «личном интересе Российского Президента» к данному делу. Благодаря такому вбросу Д. Трамп мог бы получить обвинение в том, что совершил государственную измену, так как он пытался найти первоисточник сведений о российском вмешательстве в выборы. Следовательно, из-за его поисков мог быть раскрыт агент. В связи с этими событиями, было очень трудно сказать, что Д. Трамп хотел искренне помочь докопаться до истины. Легче было отметить, что он не оставил без внимания национальную безопасность США из-за личной мести.

Цели данного вброса для Российской Федерации:

1. Полностью «ближайшее окружение» президента должно было оказаться под подозрением того, что кто-то может сотрудничать с США.

2. Отвлечение внимания от действительно работающей в окружении какого-нибудь другого чиновника особо ценной действующей агентуры ЦРУ.

Однако самое главное в данном информационном методе – это хорошо сформированная легенда прикрытия, которая состоит из того, как Д. Трамп приказал У. Барру найти агента по делу о вмешательстве РФ в выборы в США и как он поставил всех других агентов под опасность.

Одним из национальных интересов, которые указаны в Указе Президента от 2 июля 2021 года, является развитие информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия. Следовательно, система защита от угроз в информационной сфере и информационное обеспечение внешнеполитической деятельности государства нуждается в совершенствовании и развитии. Поэтому в Российской Федерации стремятся проводить некоторые меры, чтобы обеспечить информационную безопасность. Например, Минцифры обсуждает введение сбора с российских компаний, продолжающих использовать зарубежное ПО, так как это может «уравнять» иностранный софт с российским. Такая необходимость связана с вопросами безопасности – использование решений недружественных государств автоматически дает им доступ и к данным и к управлению, в том числе критической информационной инфраструктуры. Но и в «некритических» информационных системах назрел переход на собственное ПО.

Таким образом, глобализационные процессы создали практически идеальные условия для эффективного информационного воздействия. Важным моментом является то, что в настоящее время нарушение суверенитета в информационной сфере может быть позиционировано не только как правомерное, но и как необходимое действие. В связи с этим одними из важнейших условий

обеспечения национальной безопасности становятся, во-первых, сохранение контроля над информационной сферой государства, и во-вторых, укрепление позиций государства как актора коммуникационных процессов на международной арене.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Айрапетян Д.А.** Институциональные перспективы перехода к посткапитализму: трансформация государства как субъекта власти в эпоху цифро-сетевых технологий // Вопросы политологии. 2024. № 7.
2. **Алаудинов А.А., Манойло А.В.** Когнитивная и ментальная составляющие современной гибридной войны // Вопросы политологии. 2024. № 2.
3. **Алаудинов А.А., Стригунов К.С., Гончаренко А.Р.** Структура и характеристика субъектов военного конфликта на Украине и его основные отличия от гибридных войн в Сирии и Ливии // Вопросы национальных и федеративных отношений. 2024. № 6.
4. **Бедрань В.В.** Механизмы информационной войны США против Ирака в начале XXI в. // Вестник РГГУ. Серия: Политология. История. Международные отношения. Зарубежное регионоведение. Востоковедение. 2012. № 7 (87).
5. **Бельков О.А.** Национальные интересы в координатах национальной безопасности // Вопросы политологии. 2023. № 11-2.
6. **Выходец Р.С., Панцерев К.А.** Сравнительный анализ современных концепций информационного противоборства // Евразийская интеграция: экономика, право, политика. 2022. № 16 (4).
7. **Григорян Д.К.** Национализация интернета как инструмент власти по контролю за цифровым пространством / Д.К. Григорян, Н.С. Делов, М.В. Ганжа // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2022. № 2 (141). EDN WIKSGV.
8. **Жбанов А.М.** Современные тенденции политики кибербезопасности крупных держав // Вопросы политологии. 2024. № 7.
9. **Жбанов А.М.** Современное состояние киберпространства в системе обеспечения международной безопасности // Вопросы политологии. 2024. № 4.
10. **Жбанов А.М.** Практика государственно-частного партнерства в системе обеспечения политики кибербезопасности США// Вопросы национальных и федеративных отношений. 2024. № 6.
11. **Ло Дунмэй, Ян Бо.** Российско-китайское сотрудничество в области кибербезопасности в XXI веке: возможности и вызовы // Вопросы политологии. 2023. № 11-2.
12. **Новосельский С.О., Антропова Т.Г., Гагарина И.Ю., Булавина М.А.** Особенности формирования интеллектуального капитала в России как фактора обеспечения национальной безопасности в условиях санкций // Вопросы политологии. 2023. № 9-1.

13. О роли Запада в конфликте на Украине // https://kbrria.ru/mneniya/OroliZapadavkonfliktenaUkraine.
14. «Пробирка Пауэлла». Как США сфабриковали повод для вторжения в Ирак // https://ria.ru/20230205/irak-1849161911.html.
15. Современные информационные технологии и информационная безопасность: сборник научных статей 3-й Всероссийской научно-технической конференции, Курск, 02 февраля 2024 года. Курск: ЗАО «Университетская книга», 2024.
16. **Степовая Д.А.** Безопасность национального киберпространства в условиях информационно-психологического противоборства // Вопросы политологии. 2023. № 5.
17. **Сунь Сяомэн, Медведев Н.П.** Нетрадиционные угрозы безопасности и пути им противодействия в контексте международного сотрудничества // Вопросы политологии. 2024. № 5.
18. **Сурма И.В.** Вызовы и угрозы технологий искусственного интеллекта как универсального инструмента социально-политической и экономической трансформации современного общества // Вопросы политологии. 2024. № 6.
19. **Сурма И.В.** Международно-правовые особенности обеспечения кибербезопасности в условиях развития высокотехнологичной преступности // Вопросы национальных и федеративных отношений. 2024. № 7.
20. **Сурма И.В.** Кенселлинг как форма государственного кибер-остракизма// Вопросы национальных и федеративных отношений. 2024. № 6.
21. **Филатов О.В.** Подходы НАТО к обеспечению информационной безопасности: от общих киберугроз до злонамеренного использования искусственного интеллекта // Вопросы политологии. 2023. № 2.
22. **Форостянный Н.С., Тёмкина А.М.** Политический потенциал БРИКС в трансформации системы международной безопасности // Евразийский Союз: вопросы международных отношений. 2024. № 7.
23. ЦИПсО разгоняет очередной дипфейк с врио губернатора Курской области // https://bloknot-kursk.ru/news/tsipso-razgonyaet-ocherednoy-dipfeyk-s-vrio-gubern-1768115.
24. **Чжао Лэй.** Сотрудничество в области кибербезопасности и борьбы с кибертерроризмом в рамках ШОС // Евразийский Союз: вопросы международных отношений. 2024. № 5.

A.S. GADZHIEVA
Undergraduate of the Department
of Political Science and Ethnopolitics
of the Russian Academy of Sciences and GS
under the President of the Russian Federation,
Moscow, Russia

S.V. APARIN
Lecturer, Department of Information Support
for Internal Affairs, Rostov Law Institute of the Ministry
of Internal Affairs of Russia, Rostov-on-Don, Russia

D.K. GRIGORYAN
Candidate of Political Sciences,
Professor of the Department
of Political Science and Ethnopolitics
of the Russian Academy of Sciences and the State Duma
under the President of the Russian Federation,
Moscow, Russia

THE INFORMATIONAL AND PSYCHOLOGICAL ASPECT OF NATIONAL SECURITY IN THE CONTEXT OF NATIONAL SECURITY IN THE CONTEXT OF AN INFORMATION AND NETWORK SOCIETY

The article examines how the importance of the information aspect in ensuring national security has increased. In today's complex information world, the search for innovative ways of interaction between industries is becoming increasingly important. This commitment can help improve the overall quality of life and reduce the potential risks associated with information.

Since future obstacles require identifying and combating these threats, especially in light of external constraints, this article explores the importance and role of information security within the national security framework of a country.

Key words: *national security, information security, information warfare, information intervention, information and psychological operations.*