DOI 10.35775/PSI.2024.109.9.016
УДК 32

А.А. МИТРОФАНОВ
аспирант кафедры глобалистики факультета глобальных процессов МГУ им. М.В. Ломоносова,
Россия, г. Москва

ЭВОЛЮЦИЯ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ В КОНТЕКСТЕ СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ ВОЙНЫ

Информационные операции используются государствами и другими акторами в борьбе за контроль над информационным пространством. Подобные операции появились тысячелетия назад и с течением времени усовершенствуются лишь инструменты их реализации.

В данной статье автор прослеживает эволюцию информационных операций с периода Древнего мира по настоящее время, показывает связь между информационным противоборством, гибридной войной, «острой силой» (sharp power), «мягкой силой» (soft power) и цветными революциями.

Целью данной статьи является показать, что информационное противоборство существовало с момента как человек научился письменно фиксировать и передавать данные, а информационная война стала возможной по мере развития инструментов.

Ключевые слова: *информационная операция, информационная война, психологическая операция, кибернетическая операция, острая сила, мягкая сила, цветная революция.*

Наиболее четкие определения понятиям информационная война и информационная операция в отечественной науке дал А. Манойло. Информационная война это – «вооруженный конфликт, в котором столкновение сторон происходит в форме информационных операций с применением информационного оружия» [25. С. 75], а информационная операция это – «проводимая в мирное и военное время плановая пропагандистская и психологическая деятельность, рассчитанная на иностранные дружественные, враждебные или нейтральные аудитории с тем, чтобы повлиять на их отношение и поведение в благоприятном направлении для достижения как политических, так и военных целей» [25. С. 76].

Следует подчеркнуть, что в работах российских и зарубежных авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 2; 5; 8; 9; 12; 23; 31; 36].

Однако проблему информационных операций в контексте информационных войн нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Первая в истории информационная операция была проведена в конце XIV – начале XIII вв. до н.э. после битвы между египетским и хеттским войсками при Кадеше, когда каждая из сторон зафиксировала, что она одержала победу.

Восемью веками позднее, китайский философ Сунь Цзы в «Трактате о военном искусство» [35] рассмотрел инструменты, которые применяются в информационной войне по сей день: разведка, разумное использования информации о противнике, обман и прочие. Американская корпорация RAND сегодня признает, что (признана нежелательной организацией на территории РФ) продолжает опираться на работы Сунь Цзы [55].

Платон затронул тему информационной безопасности в работе «Государство», где он выделил контроль образования стражей и воинов, с помощью цензурирования «ложных» и «вредных» представлений о мире [4]. Аристотель ввел понятие силлогизма, который используется в информационных операциях [37].

Проблемы пропаганды, контроля информации, общественного дискурса, а также влияния на массы косвенно рассматривали Цицерон, Сенека и Тацит [22; 33; 39]. Их современник из империи Маурьев, Каутилья выделил такие методы борьбы как разведка, дезинформация, например через анонимные письма или шпионаж, и прочие методы [14].

В работе «Государь» Никколо Макиавелли описал Италию в XVI веке, сделав акцент на политической борьбе, которая вбирает в себя элементы военного противоборства: обман, разведка, использование информации о противнике и прочие [24]. Следующей крупной работой о военном противостоянии и о ее информационном аспекте является труд К. фон Клаузервица «О войне» (1823), где автор сделал вывод, что «война есть продолжение политики, только иными средствами» [15. С. 25].

Основные принципы информационного противоборства были выведены к XIX веку, а позднее менялись методы и инструменты. В этот период ключевую роль в информационном противоборства играют короткие психологические операции. Автор определяет их как операции, проводимые с целью достижение стратегического преимущества над противником, путем оказания влияния на его психическое состояние.

В XIX веке расширились возможности по распространению информации и оказанию влияния на мнение масс. В 1814 году газета The Times приобрела печатный станок способный производить 1100 оттисков в час [51]. В 1835 году в Париже была основана первое в мире информационное агентство «Гавас», позднее стал активно использоваться электрический телеграф. Последовавшие изобретения телефона, телевизора и радио сделали возможным передачу информации не только в текстовом формате.

В 1908 году в США создается Федеральное бюро расследований (ФБР). После Первой Мировой Войны началось переосмысление методов противоборства: появились первые пропагандистские подразделения, начали массово распространяться первые фейки, сообщения, деморализующие противника. В 1918

году в Великобритании было создано Министерство информации ответственное за внутреннюю, внешнюю и военную пропаганду.

У. Липмана и Э. Бернейса одними из первых комплексно рассмотрели феномен пропаганды в работах «Общественное мнение» (1922) [21] и «Пропаганда» (1928) [40] соответственно. Отдельные аспекты информационного контроля и влияния на людей были открыты философом А. Грамши в работе «Тюремные тетради» [13], а также в работе К. Маннгейма «Идеология и утопия» (1929) [49].

После окончания Второй Мировой Войны г. Ласуэлл, П. Лайнбарджер, Ж. Эллюл [19; 43; 48], начали исследовать СМИ и другие коммуникационные каналы, которые могут быть использованы для убеждения и мобилизации общественного мнения. В 1947 году в США создается Центральное разведывательное управление (ЦРУ). В 1949 году, в армейском уставе ВС США «FM-33-5 Psychological warfare in combat operations» впервые вводится термин «психологическая война» [45]. На тот момент ключевую роль в информационном противоборстве продолжали играть психологические операции. В 1961 году основывается Агентство США по международному развитию (USAID), отвечающее за продвижение интересов США за рубежом. И наконец, первое официальное упоминание информационной войны было в докладе Т. Роны «Системы вооружения и война» (1976) [57. С. 27].

В 1988 году термин «психологическая операция» был внесен в полевой устав США (FM 33.1-1) [44]. Далее термины «информационная война» и «информационная операция», впервые были официально использованы в директиве Министерства обороны США TS-3600.1 в 1992 году [42]. Причиной введения понятий стала необходимость анализа результатов операции США в Ираке – «Буря в пустыне» (1990-1991), где впервые активно использовались электронные средства, спутниковая связь, а СМИ круглосуточно освещали события. США контролировали информационное пространство в контексте действий в Ираке, что было рассмотрено в работах Ж. Бодрияра [3], Х.Тоффлера [58] и других. Они сделали вывод, что грядет эпоха новых более технологических войн с использованием компьютеров и борьбой за информационное пространство.

С начала XIX века по конец XX века количество информационных операций и объем передаваемой информации возросли кратно, важнее стал не психологический – качественных эффект от проводимых операций, а количественный – информационный. Наиболее ярко это заметно на примере противостояния США и СССР в период Холодной войны. На этом этапе можно говорить о распространении информационных операций, которые приходят на смену психологическим операциям. Под информационной операцией автор понимает заранее подготовленные действия в период мирного или военного времени направленные против государства, структуры или человека с целью оказания влияния на восприятие фактов для достижения политических целей и задач.

В начале 1990-тых произошли события подготовившие перемены в информационной войне: распад СССР, что привело к преобладанию либеральной политической повестки в мире, а также появление сети Интернет, новые возможности

которого повлияли на вектор развития технологий и стратегию войны, на будущие методы противоборства.

Во-первых, снизился спрос на обычные вооруженные силы, которые были нужны на случай столкновения между коммунистическим блоком и странами запада. Число военнослужащих было сокращено и многие пошли в частные военные компании (ЧВК), которые стали активно появляться в 1980-ые –1990-ые годы [6; 7; 38].

Во-вторых, в период 1990-ых – по настоящее время появляются террористические группы и нерегулярные формирования как Аль-Каида (1988) [32], Исламское государство (ИГИЛ, 2013) – террористические организации запрещенные в Российской Федерации, Талибан (1994) [16] (находится под санкциями ООН за террористическую деятельность), Хезболла (1984) и ХАМАС (1987) [34]. Их возможности значительно выросли с появлением интернета и ряд из них начали строить инфраструктуру и вербовку через сеть [25. С. 323].

Война в глобальном смысле сменяется чередой малых региональных конфликтов, где сталкивается множество интересов, отстаивать которые удобнее руками «независимых» групп [29; 30].

В-третьих, меняется противостояние государств на идеологическом уровне, где больше не работает противопоставление коммунисты-капиталисты. Вместо традиционной «жесткой силы» Дж. Най вводит понятие мягкой силы, которое предполагает достижение результатов не с помощью силы или экономических санкций, а за счет привлекательности образа жизни государства [53]. Альтернативный инструмент предлагает в 1993 году Дж. Шарп в работе «От диктатуры к демократии» [57]. Автор фактически предложил пошаговую инструкцию к смене неугодных США «недемократических» режимов, то есть по проведению цветных революций с использованием различных каналов коммуникации.

С распространением компьютеров и интернета появляются кибернетическая война и кибернетические операции, которые предполагают наступательные и оборонительные действия с целью защиты собственной или нанесения урона вражеской инфраструктуре, а также похищение информации и использование новых технологий с целью оказания влияния на человека.

Термин кибероперации или операции в киберпространстве впервые фиксируется в «Доктрине операций в киберпространстве» США, JP 3-12(R) – действия, направленные на проникновение в компьютеры или сети для нанесения ущерба или разрушения, и действия, направленные на защиту собственных компьютеров и сетей [47].

В 2009 году в Пентагоне создается Кибернетическое командование США (USCYBERCOM), ответственное за принятие решений по кибервойне и кибероборне, работе в киберпросранстве. Оно дополняет деятельность сетей некоммерческих организаций по всему миру, а также ЦРУ, ФБР, Агентства по национальной безопасности (АНБ) и прочих структур, ответственных на продвижение интересов США.

О деятельности АНБ известно из данных полученных от Э. Сноудена. В рамках программы PRISM (Program for Robotics, Intelligents Sensing and Mechatronics) АНБ отслеживало звонки и собирало метаданные пользователей. ЦРУ известно созданием вируса Stuxnet. Вирус внедрялся в операционные системы обеспечения ядерных объектов Ирана, а также занималось слежкой за политиками. О разработках ЦРУ известно из файла «Vault-7», который размещен на сайте WikiLeaks. Согласно документу, одним из направлений в работе ЦРУ является поиск уязвимостей электронных устройств и операционных систем и последующая разработка программ проникновения [59].

Проблематика войн в информационном пространстве, продолжаются в статьях военных экспертов: США Р. Гейтса «Сбалансированная стратегия» (2009) [11], Уэсли Кларка и П. Левина – «Обеспечение безопасности информационной магистрали» (2009) [17], а также в работе Ричарда Кларка и Р. Нейка «Кибервойна» (2010) [18]. В 2010-ые выходят работы М. Либицки «Киберпространство во время войны и мира» (2016) [50] и Б. Бьюкенена «Дилемма кибербезопасности: хакерство, доверие и страх между странами» (2016) [41]. Авторы анализируют данные о кибервойне и концентрируются на проблеме атрибуции проведенных атак.

Итак, можно выделить ряд понятий, которые относят к теме информационной войны: информационная операция, которая является ключевым инструментом в информационной войне и предполагает использования информационных средств; кибероперация и кибервойна, которая предполагает нанесение критического урона инфраструктуре противника, при этом защищая свою; психологическая операция и психологическая война, которая предполагает борьбу за контроль над сознанием оппонента с целью его подчинения и управления вплоть до полного уничтожения. Можно сделать вывод, что информационная война – это борьба за контроль над информационным пространством для достижения стратегического преимущества над противником, нанесение ему психологического урона, подавление или уничтожение его информационных и кибернетических возможностей.

На закате XX века появляются первые работы по теме гибридных войн, которые можно определить как ведение противоборства во всех сферах, используя как новейшие компьютерные и ИКТ технологии, так и инструменты непрямого воздействия. Одна из первых работ по теме гибридных войн была представлена двумя полковниками армии Китая Ван Сянсуем им Цяо Лян под названием «Неограниченная война» (1999) [54]. Авторы утверждают, что по мере «слияния технологий, сферы политики, экономики, военного дела, культуры, дипломатии и религии накладываться друг на друга», что «делает все более устаревшей идею ограничения войны боевыми действиями» [54. С. 189].

В 2007 году эксперт в проблематике гибридных войн Ф. Хоффман писал, что такие конфликты «могут вести как государства, так и различные негосударственные субъекты» [47. С. 14]. В 2015 году эксперт уточнил, что гибридная война может сочетать обычные и специальные операции, наступательные кибер- и космические действия, а также психологические операции, с использованием

социальных сетей и СМИ для оказания влияния на восприятие населения и международное мнение [52].

Новым витком развития в информационных войнах стало использование открытых платформ по типу Facebook, YouTube (принадлежат компании META признана экстремистской организацией на территории РФ) для распространения контента провокационного характера для координации протестных движений внутри государств. Например, в период Арабской весны 2010-2012 годов и попытки цветной революции в России в 2011-2013 годах.

В 2013 году Начальник Генерального штаба Вооруженных сил Российской Федерации и первый заместитель министра обороны В. Герасимов написал статью «Ценность науки в предвидении» [10]. Автор четко указывает, что «в XXI веке прослеживается тенденция стирания различий между состоянием войны и мира», то есть «войны уже не объявляются, а начавшись, идут не по привычному нам шаблону» в связи с чем растет «роль невоенных способов в достижении политических и стратегических целей, которые в ряде случаев по своей эффективности значительно превзошли силу оружия», а также «акцент используемых методов противоборства смещается в сторону широкого применения политических, экономических, информационных, гуманитарных и других невоенных мер, реализуемых с задействованием протестного потенциала населения».

После 2014 года появляются новые методы информационного противоборства – многошаговые информационные операции, которые курируются спецслужбами, а также активнее применяются санкции, задача которых оказать психологическое давление на цель. Например, допинговый скандал в 2015 году, «панамское досье» в 2016, обвинение России во вмешательстве в выборы в США в 2016 году (Russiagate), Отравление Скрипалей в 2018 и многие другие операции, проведенные коллективным Западом против России [26].

В 2017 был задан новый импульс развитию парадигмы теории мягкой силы Дж. Ная. В работе «Значение Sharp Power. Как авторитарные государства проецируют свое влияние» [60] К. Уокер и Дж. Людвиг ввели понятие острой силы, которая является своеобразием антагонизма мягкой силы и предполагает использование непрямых методов для проецирования своего информационного и культурного влияния – по сути борьба за информационное пространства, обернутая в «красивую обертку». Авторы характеризуют деятельность России, Ирана и Китая в этом ключе, но в отличие от западных стран, которые по мнению авторов используют мягкую силу, три страны распространяют свое влияние при помощи скрытых и непрямых методов воздействия.

Среди отечественных исследователей, О. Леонова отметила, что введение термина – это реакция западных стран на растущее влияние восходящих центров силы, которые используют те же методы, что и страны запада и даже более эффективно, что вызывает подобную «защитную реакцию».

«Пренебрежение западных скептиков к способностям стран (Китай, Россия, Иран) ... распространять свое влияние привело к опасному самоуспокоению. Это позволило названным государствам методом проб и ошибок за короткий срок

усовершенствовать свои технологии и развить мощный арсенал собственных средств воздействия» [20].

К 2018 году западные и отечественные исследования рассматривают информационную войну с противоположных сторон. В то время как объекты исследований по темам информационная война, информационные операции, кибернетические и психологические операции, гибридные войны, цветные революции и прочие переплетаются и практически сливаются воедино к моменту начала специальной военной операции России на Украине 24 февраля 2022 года.

В этот период методы информационного противоборства упрощаются – к такому выводу приходит А.В. Манойло, а на передний план выходят фейковые новости (fake news) [27]. Фейковые новости – это информационные вбросы, содержащие в себе специально подготовленные сведения провокационного и резонансного характера [28]. Оценивая ситуацию с фейками после начала СВО А. Манойло делает вывод, что информационные операции упростились [27], а связывает подобный регресс автор с тем, что время на планирование в условиях крупного столкновения всегда не хватает. Автор выделяет четыре уровня противоборства в информационном пространстве с момента начала СВО: стратегические информационные операции, спецпропаганда, фейки и оперативные игры.

Отдельно следует выделить цензуру в социальных сетях и СМИ к которой первыми обратились государства коллективного Запада против России, а последняя была вынуждена реагировать.

В результате проведенного анализа можно заключить, что информационное противоборство строится на основе принципов, сформированных за период более двух тысяч лет. С течением времени изменялись инструменты противоборства и цели проводимых операций.

На первых этапах целью было достижение психологического эффекта над врагом и поэтому первыми появились термины психологическая операция и психологическая война. Далее, в 19 веке появились инструменты для увеличения скорости и объемов передаваемой информации, что сделало возможными проведение информационных операций – информационный эффект начал преобладать над психологическим. Последним этапом стало появление интернета, компьютеров и смартфонов, используемых для проведения кибернетических операций и ведения кибернетической войны. Таким образом, современная информационная война ведется с помощью психологических, информационных и кибернетических операций.

Понятие информационная война также пересекается с понятиями острая и мягкая сила, где острую силу можно определить как распространение влияния скрытыми методами, а мягкую силу – открытыми. Информационная война или отдельные информационные операции используются для проведения цветных революций. В свою очередь, информационная война, цветные революции, мягкая, острая, а также жесткая силы являются составными элементами

гибридной войны, которая предполагает противостояние во всех сферах, при использовании всех доступных методов и инструментов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Алаудинов А.А.** Цели и задачи России в специальной военной операции на Украине и в гибридной войне с коллективным Западом // Вопросы политологии. 2024. № 5.
2. **Алаудинов А.А., Манойло А.В.** Когнитивная и ментальная составляющие современной гибридной войны // Вопросы политологии. 2024. № 2.
3. **Бодрияр Ж.** Дух терроризма. Войны в заливе не было. М.: Рипол Классик, 2016.
4. **Бугай Д.В.** Единство платоновского «Государства» / Философский факультет МГУ имени М.В. Ломоносова. М.: Издатель Воробьев А.В., 2016.
5. **Буданцев Э.В.** Информационная безопасность как фактор стратегического суверенитета на пространстве Большой Евразии // Евразийский Союз: вопросы международных отношений. 2024. № 6.
6. **Валецкий В.В.** Частные военные компании, их создание и развитие – опыт работы в Ираке, Афганистане, Африке и в других регионах мира // Интернет-журнал «Art of War.»
7. **Веселов Ю.А.** История и роль ЧВК в современной мировой политике // Мировая политика. 2021. № 3.
8. **Власов М.С.** Особенности информационного противостояния России и США в гибридной войне // // Вопросы национальных и федеративных отношений. 2024. № 3.
9. **Волох О.В., Костюков В.А.** Влияние средств массовой информации США на формирование общественного мнения в России // Вопросы политологии. 2023. № 11-1.
10. **Герасимов В.В.** Ценность науки в предвидении // Военно-промышленный курьер. 2013.
11. **Гейтс Р.** Сбалансированная стратегия // Россия в глобальной политике. 2009. № 2.
12. **Горбунов Н.С.** Элементы внешнеполитической стратегической коммуникации в доктринальных документах России // Вопросы национальных и федеративных отношений. 2024. № 6.
13. **Грамши А.** Тюремные тетради // https://www.civisbook.ru/files/File/Gramshi,tetradi.pdf.
14. **Кальянов В.И.** Артхашастра или Наука политики (Перевод с санскрита). М.: Академия наук СССР, 1959.
15. **Карл фон Клаузервиц.** О войне. М.: Эксмо, 2007 // https://hrguru.ucoz.ru/_ld/0/9_2Aw.pdf.
16. **Карпачева О.В.** История движения «Талибан» в системе международных отношений // Вестник РУДН. Серия: Международные отношения. 2003. № 1.

17. **Кларк У., Левин П.** Обеспечение безопасности информационной магистрали // Россия в глобальной политике. 2010. № 2.
18. **Кларк Р., Нейк Р.** Третья мировая война: какой она будет? СПб.: Питер, 2011.
19. **Лайнбарджер П.** Психологическая война. Теория и практика обработки массового сознания / Пер. с англ. Е.В. Ламановой. М.: ЗАО Центрполиграф, 2013.
20. **Леонова О.** Sharp power – новая технология влияния в глобальном мире // Мировая экономика и международные отношения. 2019. № 2.
21. **Липпман У.** Общественное мнение // https://mcocos.ru/static/books/Walter_Lippman.pdf.
22. **Луций Анней Сенека.** Нравственные письма к Луцию. М.: Наука, 1977.
23. **Мажников В.И.** Феномен информационных волн и фейк-ньюз в современной медиасфере // Вопросы политологии. 2024. № 6.
24. **Маккиавели Никколо.** Государь. М.: Художественная литература, 1982.
25. **Манойло А.В.** Информационные войны и психологические операции. Руководство к действию. М.: Горячая линия – Телеком Москва, 2021.
26. **Манойло А.В.** Информационная война и новая политическая реальность (I) // Вестник Московского государственного областного университета. 2021. № 1.
27. **Манойло А.В.** Информационные диверсии в конфликте на Украине // Вестник Московского государственного областного университета (электронный журнал). 2022. № 4.
28. **Манойло А.В., Стригунов К.С., Фэнли Го.** Фейковые новости и технология превентивной делегетимизации выборов // Гражданин. Выборы. Власть. 2022. № 2.
29. **Манойло А.В., Зайцев А.Я.** Международно-правовой статус частных военных компаний // Вестник Российской академии наук. 2020. № 1.
30. **Манойло А.В., Зайцев А.Я.** Роль частных военных компаний в использовании технологий «облачного противника» // Вестник Российской академии наук. 2021. № 2.
31. **Милоевич Л.** Самостоятельность ЕС и специальная военная операция Российской Федерации на Украине // Вопросы политологии. 2024. № 5.
32. **Нечитайло Д.** «Аль-Каида» в Ираке // Россия и мусульманский мир. 2010. № 4.
33. **Публий Корнелий Тацит.** Анналы // https://www.100bestbooks.ru/item_info.php?id=9159&search=1.
34. РСМД, Политические экстремистские движения на Ближнем Востоке и в Северной Африке // https://russiancouncil.ru/extremism-mena#hezbollah.
35. **Сунь Цзы.** Трактат о военном искусство. М.: Военное издательство Министерства обороны Союза ССР, 1955.
36. **Уртаева Э.Б.** Геополитические аспекты информационных войн и их влияние на политические процессы // Вопросы политологии. 2024. № 3.
37. **Чернышев А.Н.** Аристотель. М.: «Мысль», 1987.

38. **Шишмонин С.В.** Эволюция частных военных компаний в мире // Актуальные проблемы государства и права. 2019. № 9.
39. **Цицерон М.Т.** Речи против Каталины. Екатеринослав: В.Е. Алексеев, 1888.
40. **Эдвард Бернейс.** Пропаганда. Пер. с англ. И. Ющенко. М.: Hippo Publishing, 2010.
41. **Buchanan B.** The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations. By Ben Buchanan. Oxford University Press, 2017.
42. DODD S 3600.1 Information Operations (IO) // https://archive.org/details/DODD_S3600.1/mode/2up.
43. **Ellul J.** Propaganda: The Formation of Men's Attitudes. Trans. Konrad Kellen & Jean Lerner. New York: Knopf, 1965.
44. Field Manual 33-1, Psychological Operations // http://fas.org/irp/doddir/army/3-05-30.pdf.
45. Field Manual-33-5, Psychological warfare in combat operations.
46. **Hoffman F.** Conflict in the 21st. century: the rise of hybrid wars. Arlington: Potomac Institute for Policy Studies, 2007.
47. Joint Publication 3-12 (R), Cyberspace Operations Defense // US Air Force // https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf.
48. **Lasswell H.D.** The Theory of Political Propaganda // The American Political Science Review. 1927. Vol. 21. No. 3.
49. **Mannheim K.** Ideology and Utopia. NY.: Harcourt, Brace, Routlage & Kegan Paul, 1954.
50. **Martin C.** Libicki, Cyberspace in Peace and War. Naval Institute Press, 2016.
51. **Meggs, Philip B.** A History of Graphic Design. John Wiley & Sons, Inc., 1998.
52. Military Balance 2015, International Institute for Strategic Studies.
53. **Nye J.S.** Bound To Lead: The Changing Nature Of American Power. New York, Basic Books, 1991.
54. **Qiao Liang and Wang Xiangsui.** Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House, 1999.
55. RAND, Space Competition and the Dynamics of Conflict, July 5, 2022.
56. **Rona T.P.** Weapon systems and information War. Washington: Boeing Aerospace Company, 1976.
57. **Sharp G.** From Dictatorship to Democracy. London: Serpent's Tail, 2012.
58. **Toffler A., Toffler H.** War and Anti-War: Making Sense of Today's Global Chaos. NY.: Grand Central Publishing, 1995.
59. Vault 7: CIA Hacking Tools Revealed // https://wikileaks.org/ciav7p1/index.html#ANALYSIS.
60. **Walker Ch., Ludwig J.** The Meaning of Sharp Power. How Authoritarian States Project Influence // Foreign Affairs. 2017 // https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power.

A.A. MITROFANOV
Postgraduate student of the Department
of Global Studies, Faculty of Global Processes, Lomonosov
Moscow State University,
Moscow, Russia

EVOLUTION OF INFORMATION OPERATIONS IN THE CONTEXT OF MODERN INFORMATION WARFARE

Information operations are used by states and other actors in the struggle for control over the information space. Such operations have existed for thousands of years and as time passed, only the instruments of their execution evolved.

In this article, the author traces the evolution of information operations from the ancient world to the present day and shows the relationship between information warfare, hybrid warfare, sharp power, soft power and color revolutions.

The purpose of this paper is to show that information warfare has existed since man learned to record and transmit data in writing and that information warfare became possible as tools evolved.

Key words: *information operation, information warfare, psychological operation, cyber operation, sharp power, soft power, color revolution.*