Теорема Томаса, методология информационных операций и приложения искусственного интеллекта

Павел А. Карасев, Владимир В. Соколов, Ринат А. Шаряпов

***Аннотация* — Информационно-коммуникационные технологии и глобальная информационная среда во всё большей степени начинают использоваться различными акторами международных отношений – в том числе негосударственными – для распространения специально подготовленного контента в злонамеренных политических и экономических целях. Настоящая статья посвящена изучению методологии информационно-политического воздействия на общественное мнение и общественное сознание. Опираясь на анализ доктринальных документов, документов стратегического планирования США и конкретных примеров информационных операций, авторы реконструируют этапы информационных операций и выделяют теорему Томаса в качестве теоретической основы механизмов влияния на общественное сознание. Авторы также дают оценку влияния новейших ИКТ, в том числе опирающихся на достижения в сфере искусственного интеллекта, на возможность проведения информационных операций и противодействия им.**

***Ключевые слова*—информационно-политическое воздействие, информационная безопасность, теорема Томаса, приложения искусственного интеллекта.**

I. Введение

O Tempora! O Mores!
Марк Туллий Цицерон, I в. до н.э.

За последние годы значительно выросло количество случаев использования информационно-коммуникационных технологий (ИКТ) и глобальной информационной среды для распространения специально подготовленного контента в злонамеренных политических и экономических целях. По мнению доцента МГИМО Андрея Безрукова (Президент Ассоциации экспорта технологического суверенитета, эксперт дискуссионного клуба «Валдай», член Совета по внешней и оборонной политике): «Наличие безграничного информационного пространства, расширение общения через социальные сети позволили выработать эффективные методы взаимодействия с группами населения внутри других стран, способствующие тому, чтобы виртуально направлять идеологическую, этническую или религиозную оппозицию. За 20 лет военные, разведывательные и информационные органы отладили технологию “опосредованного” вмешательства, часто используя приграничные страны в качестве базы».[3] Выступая в эфире радиостанции «ВестиFM», он охарактеризовал подобные действия как «информационно-политические операции»[6]. Похожие тезисы можно найти и в статье Чеза Фримена (Старший научный советник Института мировой и публичной политики имени Уотсона в Университете Брауна (США)), который утверждает следующее: «Поскольку знания об обществе и окружающем мире в значительной степени сосредоточены в киберпространстве, возможности государства и негосударственных акторов формировать общественное мнение в других странах беспрецедентно возросли… Технологии позволяют осуществить мягкое завоевание посредством скрытых действий в киберпространстве. Применение научных достижений ведет к эрозии суверенитета, облегчая использование мер воздействия, выходящих за рамки дипломатии, но не доводя дело до войны…».[13]

Статья получена 17 сентября 2021.
Карасев П.А., старший научный сотрудник Центра ИПИБ, к.полит.н. (e-mail: karpaul@mail.ru).
Соколов В.В., заместитель руководителя Центра ИПИБ, к.экон.н. (e-mail: sokolov46@yandex.ru).
Шаряпов Р.А., ведущий научный сотрудник Центра ИПИБ, к.полит.н. (e-mail: mabit@yandex.ru)

II. Методология анализа

Анализ эпизодов информационно-политического воздействия свидетельствует о высокой эффективности и широте применения ИКТ-инструментов и указывает на острую необходимость выработки средств противодействия им. Высокая эффективность обусловлена следующими факторами: во-первых, существованием особой среды – глобального информационного пространства с миллиардами пользователей во всех странах, – которая обеспечивает охват значительной аудитории. По данным Международного союза электросвязи, на конец 2019 г. более 50% населения мира имеет доступ в сеть Интернет [23] – не только посредством персональных компьютеров, но и через мобильные устройства. Во-вторых – инструментами (социальные сети и цифровые платформы), которые позволяют распространять специально подготовленную информацию, ориентированную на определенную целевую аудиторию. При этом, в отличие от печати, радио и телевидения, такие инструменты могут обеспечить интерактивность – постоянное взаимодействие автора контента с аудиторией через систему комментариев и/или форумов. Это может быть использовано, в том

числе, для корректировки воздействия в соответствии с поставленной задачей и изменяющейся обстановкой.

Вместе с тем, в дополнение к этому появляются ещё более эффективные инструменты информационного воздействия, в основе которых лежат технологии искусственного интеллекта.

Первым этапом анализа этой новой угрозы должно стать изучение стратегических и доктринальных документов различных государств, в которых раскрывается политика и организационные аспекты информационно-политического воздействия, а также выявление закономерностей путем анализа конкретных примеров.

Второй этап предполагает систематизацию полученных данных и выявление на их основе методологии и структуры типовой информационной операции.

Третий этап предполагает выработку предложений по противодействию информационным операциям.

III. Информационно-политическое воздействие как часть государственной политики

Использование некоторыми развитыми государствами новейших ИКТ для реализации задач внешней и внутренней политики является подтвержденным фактом. Анализ открытых источников (документов стратегического планирования, доктрин и наставлений) наглядно демонстрирует, что наиболее проработано это направление в США, где практической реализацией этих решений занимается как Министерство обороны, так и Государственный департамент США.

В 1992 г. директивой министра обороны США TS 3600.1 было введено понятие «Information Warfare»[24, p.14], которое можно перевести на русский язык как «информационная борьба», или «информационное противоборство». Указанная директива была документом повышенной секретности и поэтому не получила широкого распространения. В 1996 г. была издана директива Министерства обороны США S 3600.1, которая ввела в употребление понятие «информационные операции» [19].

Окончательно информационные операции закрепились в военном лексиконе и практике США в 1998 г. с появлением Объединённой доктрины информационных операций (Joint Doctrine for Information Operations) – документа, который предназначался для самого широкого распространения. Согласно этой доктрине, информационные операции включают в себя электронное противоборство (Electronic Warfare), операции в компьютерных сетях (Computer Network Operations), психологические операции (Psychological Operations), мероприятия по дезинформации (Military Deception), меры обеспечения безопасности проведения операций (Operations Security). К началу 2000-х гг. в США пришли к осознанию того, что информационные операции в перспективе станут отдельным видом вооруженной борьбы и приобретут такое же значение, как операции в других средах – на воде, суше, в воздухе и космосе.[28]

В 2002 г. было принято Наставление по психологическим операциям FM 3-05/30, в котором сформулированы цели и задачи психологических операций, а также дано определение: «запланированные операции по передаче отобранной информации и индикаторов зарубежной аудитории для оказания влияния на её эмоции, мотивы, объективные рассуждения и, в конечном счете, на поведение иностранных правительств, организаций, групп и отдельных лиц».[21, p. Glossary-16]

В последней (доступной для ознакомления) редакции Доктрины информационных операций, которая вышла в 2014 г.,[27] гораздо большее внимание уделяется именно информационно-психологическому воздействию. Вся первая глава этого документа посвящена обзору, что собой представляют информационные операции – там же, в сущности, приведена методология информационных операций. Под информационными операциями понимается «комплексное использование в ходе военных операций информационных сил и средств для оказания влияния, нарушения, искажения или перехвата процесса принятия решений противника или потенциального противника…».[26, p.110] Их планирование происходит в три шага. Сначала определяется целевая аудитория, в том числе проводится анализ правил, норм и убеждений, которые для неё характерны. После этого проводится оценка имеющихся средств для достижения желаемых целей. Когда определены средства или комбинации средств, следующим шагом является определение конкретных способов создания желаемого эффекта – и эти способы направлены на изменение трёх основ: правил, норм и убеждений целевой аудитории.

Из анализа вышеприведенных документов можно сделать следующий обобщающий вывод: в США на доктринальном уровне закреплена возможность проводить информационные операции, направленные на потенциального противника, в том числе в мирное время, и разработана соответствующая методология.

В отличие от Министерства обороны, Государственный департамент США начал активно развивать идеи использования ИКТ для оказания информационного воздействия несколько позже – в 2010 г., когда вышел очередной «Четырехлетний обзор внешней политики и развития»[32]. В основе этого документа лежит идеология «Государственного управления XXI в.» (21st Century Statecraft),[15] суть которой в том, что доступность и мощь информационных технологий изменяют систему международных отношений и условия для государственного управления. Практическим шагом по реализации этой идеологии стала программа стратегического развития информационных технологий Государственного департамента США «Цифровая дипломатия»[20], действовавшая в 2011–2013 гг. Среди прочего, она содержала установку на использование интернета и социальных медиа для получения доступа к новой аудитории. В «Четырехлетнем обзоре внешней политики и развития» 2010 г. фактически раскрыты некоторые элементы информационно-политического воздействия. В частности, одним из элементов стратегических основ общественной дипломатии является: «Создание нарративов. Необходимо разработать активные стратегии охвата, чтобы информировать, вдохновлять и убеждать аудиторию, и нужно быть готовыми к тому, чтобы сойти с трибуны представителя Госдепартамента и из других

традиционных платформ в места, где продвигаются и обсуждаются идеи». [32, p.60]

Там же предлагается наладить работу дипломатов не только с местными властями, но и с представителями религиозных групп, гражданами и организациями. Некоторыми ключевыми аспектами этой работы являются: использование новых ИКТ и «вооружение» индивидов новыми технологиями для применения в своих сообществах. Усилия должны быть направлены на взаимодействие с активистами, организациями, журналистами, «которые мирным путем стараются изменить свои государства к лучшему»[32, p.21], в основном на тех, кто способен формировать общественное мнение или оказывать влияние.

В сентябре 2018 г. свет увидели два новых важных документа, которые определят политику США в киберпространстве на годы, а возможно – и десятилетия вперед. Сначала администрация Дональда Трампа анонсировала новую стратегию кибербезопасности – «Национальную киберстратегию США».[29] Вторым документом стала киберстратегия Министерства обороны США, и она представляет интерес в рамках данного анализа.[18] В ней расширен спектр злонамеренной деятельности в киберпространстве – помимо кибератак, сюда были включены злонамеренные кампании пропаганды и дезинформации. Примечательно, что для предотвращения, реагирования и сдерживания злонамеренной киберактивности могут быть использованы все доступные инструменты, в том числе дипломатические, информационные, военные (как кинетические, так и кибернетические), и т.д. Кроме этого, важным фактом является и то, что в этом и других документах США выделили основных противников, которыми стали Россия, Китай, Иран и Северная Корея.

Одним из наиболее очевидных практических проявлений информационно-политического воздействия является применение так называемой «публичной атрибуции», когда в отсутствие юридически значимых фактов и должного разбирательства виновный «назначается» из политических соображений – и к нему применяются «приемлемые» меры – от экономических санкций до ракетно-бомбовых ударов. Примеров использования этого метода информационно-политического воздействия множество, и самым ярким за последнее время является обвинение Китая со стороны США в сокрытии некоторых фактов об эпидемии COVID-19 – несмотря на опровержения авторитетных экспертов и организаций. Результат – подготовлен информационный фундамент для угроз санкциями и выхода США из Всемирной организации здравоохранения, где они были важным донором. Подобные информационные манипуляции для решения своих задач внутренней и внешней политики США проводят и в отношении таких чувствительных тем, как стратегическая стабильность – под теми или иными предлогами один за другим уничтожаются важнейшие соглашения – Договор о ликвидации ракет средней и меньшей дальности, Договор по открытому небу, Совместный всеобъемлющий план действий. При этом можно констатировать, что в последние годы традиционные союзники США далеко не всегда слепо поддаются на призывы к публичной атрибуции и всё чаще задумываются о последствиях и своих интересах на перспективу.

IV. Теоретические основы и методология управления социальным поведением людей

В настоящее время одной из основных теорем социальных наук является так называемая теорема Томаса: «Если люди определяют ситуации как реальные, они реальны по своим последствиям». Уильям Айзек Томас, классик американской социологии, сформулировал это утверждение в 1923 г. и не придавал ему особого значения. Вместе с тем в политической практике многих государств следствия этого утверждения постоянно использовались и продолжают использоваться для манипулирования социальным поведением масс.

Многие специалисты предсказывали, что по мере развития новых технологий распространения информации теорема Томаса будет приобретать все более важное значение. Так, А.В.Луков в своей статье «Следствия "теоремы Томаса" в условиях становления информационной цивилизации» отмечает: «То, что было частным случаем в начале века, стало глобальной ситуацией в конце века благодаря развитию информационных технологий».[7]

Наиболее важными для практических приложений являются следствия теоремы Томаса, позволяющие управлять социальным поведением людей. Раньше считалось, что на поступки человека оказывают влияние только две «реальности» – субъективная и объективная. Теперь сформировалась «третья реальность» – глобальная медиасфера, через которую, в соответствии с теоремой Томаса, можно оказывать влияние на принятие решений и поступки людей. При этом в умах «рядовых людей» (обывателей) объективная реальность, выходящая за пределы их повседневных проблем, забот и интересов, замещается представлением об этой реальности, которое формируется «третьей реальностью» (точнее, теми фрагментами «третьей реальности», которым данный человек доверяет). Здесь под словами «рядовой человек» (обыватель) понимается человек, который не занимается профессионально экономической, социальной и политической проблематикой и не имеет ни знаний, ни возможностей, ни желания выискивать в потоках информации крупинки объективной реальности.

Использование указанных следствий теоремы Томаса в организации масштабных информационных операций последних десятилетий («пробирка Колина Пауэлла», майдан в Киеве, использование химического оружия в Сирии, отравление Скрипалей, и др.) укладывается в одну и ту же схему. Вначале проводится широкомасштабная, хорошо срежиссированная кампания с использованием всех возможных каналов глобальной медиасферы по замещению в умах людей объективной информации о ситуации на то представление об этой ситуации, которое соответствует целям разработчиков кампании. Этот этап условно можно назвать «Замещение реальности медиасобытием».

После того, как эта цель достигнута, начинается вторая фаза операции, смысл которой, в соответствии с теоремой Томаса, в том, что все последствия

сформированного представления о ситуации люди теперь будут считать правильными (можно нападать на Ирак, можно смещать Януковича, можно бомбить Сирию, и др.). Этот этап условно можно назвать «Информационное обеспечение реализации следствий из медиасобытия». Одновременно на этом этапе периодически осуществляют управление, корректировку и «обновление» медиасобытия, в соответствии с изменяющимися условиями. Здесь следует сослаться на ряд материалов авторитетного российского эксперта Андрея Масаловича [См. напр. 4, 5], в которых, в частности, исследовались графики активности обсуждения в социальных сетях конкретной тематики и показывалась необходимость периодической поддержки этой активности путём «подбрасывания» новых фактов.

V. Новые технологии информационно-политического воздействия

Технологии целенаправленной подготовки и рассылки контента постоянно совершенствуются: таргетирование информации, использование Интернет-профилей пользователей, «фэйк-новости» и использование лидеров общественного мнения для тиражирования этих новостей. В статье Андерса Фога Расмуссена и Майкла Чертоффа (Anders Fogh Rasmussen, бывший генеральный секретарь НАТО и бывший премьер-министр Дании; Michael Chertoff, бывший министр внутренней безопасности США.) предложено обобщенное понятие для характеристики таких технологий – гипертенденциозный контент (hyper-partisan content).[2] Сегодня также большое значение придаётся возможностям использования технологий искусственного интеллекта (ИИ) в этой области – при этом, как для защиты, так и для нападения. Представляется, что технологии ИИ могут быть использованы на каждом из этапов информационной операции, но наиболее существенными являются возможности по анализу больших данных, создания и анализа текстов. Сегодня видимые усилия научного сообщества сосредоточены на проблемах использования ИИ для выявления фейковых новостей. Однако эти же технологии могут быть использованы и для обратной цели – например, создания генераторов правдоподобных текстов с заданным содержанием.[См. 17, 34] Что касается больших данных, здесь можно отметить значительные успехи в создании программных комплексов, позволяющих проводить глубокий анализ пользовательских данных в социальных сетях – и, исходя из этого, выявлять лидеров общественного мнения и связанные с ними группы людей. Такие системы уже активно и с большим успехом применяются для превентивного предотвращения противоправных информационных вбросов и информационных действий и атак экстремистской и террористической направленности. В основе подобных мероприятий лежат постоянный мониторинг Интернета и анализ социальный сетей. В качестве примеров можно назвать американскую систему Palantir [31], а также российскую разработку – поисково-аналитическую систему Avalanche – созданную около 20 лет назад и применяемую в госструктурах, спецслужбах и силовых структурах, крупных банках и компаниях.[12]

Важно ещё раз отметить, что упомянутые технологии могут использоваться не только во благо, но и в качестве инструмента информационных операций, например, для манипулирования массовым сознанием, воздействия на массовую аудиторию в социальных сетях, в том числе для того, чтобы заставить эту массовую аудиторию принимать те или иные решения. Как отмечает в своём материале журнал Bloomberg Businessweek, говоря о системе Palantir, «Разведывательная платформа, предназначенная для глобальной войны с террором, была использована против обычных американцев». В своём выступлении на XI Международном Форуме в Гармиш-Партенкирхене (Германия) в апреле 2017 г., Андрей Масалович дал описание технологий компании Cambridge Analytica, которые были использованы в ходе выборов президента США в 2016 г. По мнению эксперта, эти технологии основаны на последовательном выполнении трех шагов. Шаг первый – использование так называемой психометрики – направления прикладной психологии, которое исследует поведение человека в социальных сетях и на этой основе строит его психологический портрет. Часто используется метод оценки характера личности по пяти параметрам (OCEAN): открытость, добросовестность, экстраверсия, доброжелательность и нейротизм. На основе измерений этих параметров можно прогнозировать поведенческие реакции людей. Второй шаг – это использование «таргетирования» для точного выбора целевой аудитории. Это возможно благодаря технологии анализа больших данных о пользователях: фактологической информации (пол, расовая и религиозная принадлежность, и т.д.); поведенческих привычек; личностных характеристик. По некоторым сведениям, база данных о пользователях социальных сетей Cambridge Analytica составляет 50 млн. пользователей.[33] Третий шаг – это выявление точек наиболее эффективного воздействия, то есть точек вокруг лидеров мнений, где собирается целевая аудитория, и использование того контента, который она готова воспринимать.[10, С.138-139] По мнению А.И.Масаловича, эффективность этих технологий определяется глубоким точечным анализом.

Даже краткий обзор новых технологий показывает, что в настоящее время в ИКТ-среде идёт невидимое противоборство математических алгоритмов создания, обработки, распространения и фильтрации контента. Интересно, что об угрозе использования ИИ в таком ключе на достаточно высоком уровне говорят в США. Так, в промежуточном докладе 2019 г. «Комиссии национальной безопасности по искусственному интеллекту» [16], которая была учреждена в августе 2018 г., во исполнение пункта 1051 Закона о национальной обороне им. Джона Маккейна (PL 115-232 [22]), среди прочего, сказано, что технологии ИИ могут быть использованы для дезинформации и подрыва демократической системы; эрозии конфиденциальности частной жизни и гражданских свобод.

VI. Заключение

По мнению экспертов Deutsche Bank, эпоха глобализации, длившаяся последние 40 лет, подходит к концу – возможно, что на смену ей в 2020 г. приходит

новая эпоха в истории человечества, которую будет определять понятие «беспорядка». Одним из ее главных аспектов будет состояние, близкое к холодной войне между США и Китаем, – при этом, как говорят авторы доклада, «на горизонте можно увидеть столкновение культур и интересов, особенно по мере того, как Китай приближается к крупнейшей экономике мира».[25] Вынося за скобки возможность возникновения локальных горячих точек, где США и Китай могли бы вступить в опосредованное военное противостояние, в качестве других рычагов воздействия будут использоваться уже апробированные экономические (в виде санкций, торговых барьеров и т.п.), а также информационно-политические инструменты.

Очевидно, что, по мере отработки и совершенствования методик и технологий реализации, будет возрастать количество широкомасштабных информационно-политических операций и повышаться их эффективность. Приведенный выше анализ показывает, что информационные операции основываются на принципах теоремы Томаса, а эффективность операций показывает, что эти принципы работают. Операции проходят по разработанным сценариям и в темпе, необходимом для скорейшего внедрения заданных нарративов в сознание атакуемых лидеров общественного мнения, не давая возможности обороняющейся стороне проявить оперативную реакцию на информационную атаку. Так, анализ примеров информационных операций, направленных в последние годы против России, показывает, что Российская Федерация не раз опаздывала с выявлением признаков и своевременным реагированием на масштабные резонансные информационно-политические атаки западных стран – ответ на информационные атаки начинает прорабатываться и реализовываться в тот момент, когда соответствующая негативная информация уже «внедрена» в умы западных лидеров. По оценке главного редактора телеканала RT Маргариты Симоньян, «[сегодня – прим. авт.] Информационное пространство проиграно» [14].

Опасность для России, как одного из формирующихся центров многополярного мира, заключается в перспективе столкнуться не с эпизодическими, а с ежедневными проявлениями информационно-политических операций. По оценке Секретаря Совета Безопасности Российской Федерации Н.П.Патрушева, «усиливающееся в последнее время и направленное на российскую аудиторию внешнее информационное и идеологическое воздействие преследует не только цели пропаганды терроризма, но и направлено на раскол российского общества по национальному, культурному и религиозным признакам».[9] Повышение частоты масштабных резонансных (в смысле возможных последствий) информационных операций подтверждается и хронологией событий 2020 г., которые обладают соответствующими признаками. Так, эпизод с «группой Вагнера» перед выборами в Белоруссии (29 июля) и «отравление Навального» (20 августа) разделяет меньше месяца.

Учитывая то, что путь изоляции от глобальных систем распространения информации исключается руководством России как возможная альтернатива а, напротив, государственная политика направлена на недопущение такого сценария [8], возникает потребность в эффективных средствах противодействия информационным операциям. Исходя из этого, одной из первоочередных задач должно стать создание системы мониторинга и своевременного выявления признаков готовящихся информационных операций. Принимая во внимание тот факт, что когнитивных возможностей человека по анализу и осмыслению огромного массива информации в глобальной медиасфере явно недостаточно, при разработке указанной системы необходимо использовать технологии искусственного интеллекта.

Другой важнейшей задачей должно стать своевременное реагирование на признаки готовящихся информационных операций, в том числе опровержение планируемых к распространению фейковых новостей. С одной стороны, здесь важна и уже проводится работа в правовой сфере. Так, в марте 2019 г., в России были приняты поправки в Закон «Об информации, информационных технологиях и о защите информации», которые, в частности, дают определение фейковым новостям – это информация, распространяемая «под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи». Одновременно соответствующими поправками в Кодекс об административных правонарушениях была установлена ответственность за распространение подобной информации в информационно-телекоммуникационных сетях, в том числе в интернете.

С другой стороны, важно осознавать, что проблему противодействия информационным операциям нельзя в полной мере решить только техническими или правовыми средствами. Нужны альтернативные нарративы, а для их создания требуется конвергенция дисциплин различных отраслей науки – гуманитарных, общественных, технических и естественных. Для построения точных моделей, которые могут лечь в основу обучения искусственного интеллекта, необходимо перевести на язык математики и компьютерных программ актуальные достижения психологии, социологии, политологии и других гуманитарных наук. Эффективность этого процесса может быть обеспечена путем формирования в крупных научных центрах соответствующих коллективов и их работой на постоянной основе.

В заключение, будет уместно привести в некотором смысле пророческий фрагмент из Нобелевской лекции академика Сахарова, которая была прочитана более 30 лет назад: «То же относится к исследованиям в области создания систем имитации интеллекта, к исследованиям в области управления массовым поведением людей, к созданию единых общемировых систем связи, систем сбора и хранения информации и т.п. Совершенно очевидно, что в руках безответственных бюрократических, действующих под покровом

секретности учреждений — все эти исследования могут оказаться необыкновенно опасными, но в то же время они могут стать крайне важными и необходимыми для человечества, если их осуществлять под контролем гласности, обсуждения, научного социального анализа».[11, С.53] Сегодня мы уже является очевидцами того, как технологии искусственного интеллекта начинают применяться для управления массовым поведением людей с использованием единых общемировых систем связи – прежде всего, сети интернет. На государственном уровне идёт не только реализация наступательных информационных операций, но и активный поиск научно обоснованных решений для проведения защитных и оборонительных мероприятий; проблемам информационно-психологического противоборства уделяется повышенное внимание в научной среде – прежде всего в центрах, аффилированных с соответствующими ведомствами.

Возможно, что сегодня мир и в самом деле живёт в эпоху «постправды», однако это не означает, что он стал похож на антиутопию Оруэлла. Согласно словарному определению, термином «постправда» характеризуются такие обстоятельства, при которых объективные факты оказывают меньше влияния на формирование общественного мнения, чем апелляция к эмоциям и личным убеждениям [29, ‘post-truth’] (более подробно об этом феномене см. [1]). Информационное воздействие в том или ином виде сопровождало человеческую цивилизацию на многих ключевых этапах его развития – и человечество адаптировалось к новым условиям. Нет сомнений, что со временем произойдёт адаптация и к реалиям сегодняшнего дня.

Библиография

[1] А. Манойло, А. Попадюк, «Постправда» как социальное явление и политическая технология // Журнал Международная жизнь [Официальный сайт]. Доступно по URL: https://interaffairs.ru/jauthor/material/2388

[2] Андерс Фог Расмуссен (Anders Fogh Rasmussen), Майкл Чертофф (Michael Chertoff). Запад по-прежнему не готов остановить российское вмешательство в наши выборы // Сетевое издание — Интернет-проект ИноСМИ.RU [Электронный ресурс]. Доступно по URL: https://inosmi.ru/politic/20180606/242408398.html

[3] Андрей Безруков. Многомерная война и новая оборонная стратегия // Россия в глобальной политике [Онлайн-ресурс]. Доступно по URL: https://globalaffairs.ru/articles/mnogomernaya-vojna-i-novaya-oboronnaya-strategiya/

[4] Выживший. Информационные войны // Андрей Масалович [Персональный сайт]. URL: http://www.iam.ru/guru/201605phdaysVI.pptx

[5] Гасим экстремизм в Сети. Avalanche для правопорядка // Андрей Масалович [Персональный сайт]. Доступно по URL: http://www.iam.ru/guru/201604garmish.pptx

[6] Запад раскручивает операцию «изгой», эфир программы «Формула смысла» 09.04.2008 г. // Радио «ВестиFM» [Онлайн-ресурс]. Доступно по URL: http://radiovesti.ru/brand/61007/episode/1748064/

[7] Луков А.В. Следствия "теоремы Томаса" в условиях становления информационной цивилизации» // Знание. Понимание. Умение. 2006. N4. [Онлайн-ресурс]. Доступно по URL: http://www.zpu-journal.ru/zpu/2006_4/Lukov_AV/37.pdf

[8] Медведев: Россия должна защитить себя от возможного отключения от интернета // РИА Новости [Новостной ресурс]. Доступно по URL: https://ria.ru/20190329/1552230124.html

[9] Патрушев призвал создать новую медиаполитику по воспитанию молодежи, 10.04.2020 // РИА Новости [Новостной ресурс]. Доступно по URL: https://ria.ru/20200410/1569854040.html

[10] Приложение к журналу «Международная жизнь» XI Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности. Гармиш-Партенкирхен, Германия, 24-27 апреля 2017 года. М. 2017.

[11] Сахаров А. Мир, прогресс, права человека: Статьи и выступления.— Л.: Сов. писатель, 1990.

[12] Состав технологии и семейства продуктов интернет-мониторинга Avalanche («Лавина») // Андрей Масалович [Персональный сайт]. Доступно по URL: http://www.iam.ru/guru/Avalanche%202020.docx

[13] Чез Фриман, Технологии, государственное управление и неограниченная война // Россия в глобальной политике [Онлайн-ресурс]. Доступно по URL: http://www.globalaffairs.ru/number/Tekhnologii-gosudarstvennoe-upravlenie-i-neogranichennaya-voina-19349

[14] Эфир программы «Право знать!» от 12.09.2020, 13:14, телеканал «ТВ Центр» // Телеканал ТВЦ [Официальный сайт]. Доступно по URL: https://www.tvc.ru/channel/brand/id/1756/show/episodes/episode_id/67575

[15] 21st Century Statecraft // 2009-2017 Department of State archive [Official website]. Available: https://2009-2017.state.gov/statecraft/index.htm

[16] About [NSCAI] // National Security Commission on Artificial Intelligence [Official website]. Available: https://www.nscai.gov/about/about

[17] A. Hern New AI fake text generator may be too dangerous to release, say creators // The Guardian [News website]. Available: https://www.theguardian.com/technology/2019/feb/14/elon-musk-backed-ai-writes-convincing-news-fiction

[18] Department of Defense Cyber Strategy // Department of Defense [Official website]. Available: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[19] Department of Defense Directive O-3600.01 // Federation of American Scientists [Official website]. Available: http://fas.org/irp/doddir/dod/info_ops.pdf

[20] Fiscal Years 2011–2013: IT Strategic Plan. Digital Diplomacy // 2009-2017 Department of State archive [Official website]. Available: https://2009-2017.state.gov/documents/organization/147678.pdf

[21] FM 3-05.30 MCRP 3-40.6 Psychological Operations // Federation of American Scientists [Official website]. Available: https://fas.org/irp/doddir/army/fm3-05-30.pdf

[22] H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019 // Congress.gov [Official website]. Available: https://www.congress.gov/bill/115-congress/house-bill/5515

[23] Individuals using the Internet, 2005-2019 // ITU [Official website]. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[24] Information Operations: The Hard Reality of Soft Power // IWS - The Information Warfare Site [Official website]. Available: http://iwar.org.uk/iwar/resources/jiopc/io-textbook.pdf

[25] J. Reid, L. Templeman, H. Allen, N. Burns and K. Nagalingam The Age of Disorder – the new era for economics, politics and our way of life // Deutsche Bank [Official website]. Available: https://www.dbresearch.com/servlet/reweb2.ReWEB?rwnode=RPS_EN-PROD$JIM_REID&rwsite=RPS_EN-PROD&rwobj=ReDisplay.Start.class&document=PROD0000000000511857

[26] Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms, November 8, 2010 (As Amended Through 15 February 2016) // Federation of American Scientists. [Official website]. Available: https://irp.fas.org/doddir/dod/jp1_02.pdf

[27] Joint Publication 3-13: Information Operations 27 November 2012 Incorporating Change 1 20 November 2014 // Federation of American Scientists [Official website]. Available: https://irp.fas.org/doddir/dod/jp3_13.pdf

[28] Joint Vision 2020 // PENTAGONUS [Official website]. Available: http://pentagonus.ru/doc/JV2020.pdf

[29] LEXICO // [Online] Available: https://www.lexico.com

[30] National Cyber Strategy of the United States of America // The White House [Official website]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[31] P. Waldman, L. Chapman, and J. Robertson Palantir Knows Everything About You // Bloomberg Businessweek [News website]. Available: https://www.bloomberg.com/features/2018-palantir-peter-thiel/

[32] Quadrennial Diplomacy and Development Review // 2009-2017 Department of State archive [Official website]. Available: https://2009-2017.state.gov/documents/organization/241429.pdf

[33] Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach // The Guardian [News website]. Available: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[34] Q. Zhang, B. Guo, H. Wang, Y. Liang, S.Hao, and Z. Yu, AI-Powered Text Generation For Harmonious Human-Machine Interaction: Current State And Future Directions // ArXiv.org [Online]. Available: https://arxiv.org/abs/1905.01984

Thomas Theorem, methodology of Information Operations and applications of Artificial Intelligence

Pavel A. Karasev, Vladimir V. Sokolov, Rinat A. Sharyapov

***Abstract* — Information and communication technologies and the global information environment are increasingly being used by various actors of international relations – including non-state actors – to distribute specially prepared content for malicious political and economic purposes. This article is devoted to the study of the methodology of information and political influence on public opinion and public consciousness. Based on the analysis of doctrinal documents, strategic planning documents of the US and specific examples of information operations, the authors reconstruct the stages of information operations and highlight the Thomas theorem as a theoretical basis for the mechanisms of influence on public consciousness. The authors also assess the impact of the latest ICTs, including those based on advances in artificial intelligence, on the ability to conduct information operations and counter them.**

***Key words*— information and political influence, information security, Thomas theorem, applications of artificial intelligence.**

REFERENCES

[1] A. Manojlo, A. Popadjuk, «Postpravda» kak social'noe javlenie i politicheskaja tehnologija // Zhurnal Mezhdunarodnaja zhizn' [Oficial'nyj sajt]. Dostupno po URL: https://interaffairs.ru/jauthor/material/2388

[2] Anders Fog Rasmussen (Anders Fogh Rasmussen), Majkl Chertoff (Michael Chertoff). Zapad po-prezhnemu ne gotov ostanovit' rossijskoe vmeshatel'stvo v nashi vybory // Setevoe izdanie — Internet-proekt InoSMI.RU [Jelektronnyj resurs]. Dostupno po URL: https://inosmi.ru/politic/20180606/242408398.html

[3] Andrej Bezrukov. Mnogomernaja vojna i novaja oboronnaja strategija // Rossija v global'noj politike [Onlajn-resurs]. Dostupno po URL: https://globalaffairs.ru/articles/mnogomernaya-vojna-i-novaya-oboronnaya-strategiya/

[4] Vyzhivshij. Informacionnye vojny // Andrej Masalovich [Personal'nyj sajt]. URL: http://www.iam.ru/guru/201605phdaysVI.pptx

[5] Gasim jekstremizm v Seti. Avalanche dlja pravoporjadka // Andrej Masalovich [Personal'nyj sajt]. Dostupno po URL: http://www.iam.ru/guru/201604garmish.pptx

[6] Zapad raskruchivaet operaciju «izgoj», jefir programmy «Formula smysla» 09.04.2008 g. // Radio «VestiFM» [Onlajn-resurs]. Dostupno po URL: http://radiovesti.ru/brand/61007/episode/1748064/

[7] Lukov A.V. Sledstvija "teoremy Tomasa" v uslovijah stanovlenija informacionnoj civilizacii» // Znanie. Ponimanie. Umenie. 2006. N4. [Onlajn-resurs]. Dostupno po URL: http://www.zpu-journal.ru/zpu/2006_4/Lukov_AV/37.pdf

[8] Medvedev: Rossija dolzhna zashhitit' sebja ot vozmozhnogo otkljuchenija ot interneta // RIA Novosti [Novostnoj resurs]. Dostupno po URL: https://ria.ru/20190329/1552230124.html

[9] Patrushev prizval sozdat' novuju mediapolitiku po vospitaniju molodezhi, 10.04.2020 // RIA Novosti [Novostnoj resurs]. Dostupno po URL: https://ria.ru/20200410/1569854040.html

[10] Prilozhenie k zhurnalu «Mezhdunarodnaja zhizn'» XI Mezhdunarodnyj forum «Partnerstvo gosudarstva, biznesa i grazhdanskogo obshhestva pri obespechenii mezhdunarodnoj informacionnoj bezopasnosti. Garmish-Partenkirhen, Germanija, 24-27 aprelja 2017 goda. M. 2017.

[11] Saharov A. Mir, progress, prava cheloveka: Stat'i i vystuplenija.— L.: Sov. pisatel', 1990.

[12] Sostav tehnologii i semejstva produktov internet-monitoringa Avalanche («Lavina») // Andrej Masalovich [Personal'nyj sajt]. Dostupno po URL: http://www.iam.ru/guru/Avalanche%202020.docx

[13] Chez Friman, Tehnologii, gosudarstvennoe upravlenie i neogranichennaja vojna // Rossija v global'noj politike [Onlajn-resurs]. Dostupno po URL: http://www.globalaffairs.ru/number/Tekhnologii-gosudarstvennoe-upravlenie-i-neogranichennaya-voina-19349

[14] Jefir programmy «Pravo znat'!» ot 12.09.2020, 13:14, telekanal «TV Centr» // Telekanal TVC [Oficial'nyj sajt]. Dostupno po URL: https://www.tvc.ru/channel/brand/id/1756/show/episodes/episode_id/67575

[15] 21st Century Statecraft // 2009-2017 Department of State archive [Official website]. Available: https://2009-2017.state.gov/statecraft/index.htm

[16] About [NSCAI] // National Security Commission on Artificial Intelligence [Official website]. Available: https://www.nscai.gov/about/about

[17] A. Hern New AI fake text generator may be too dangerous to release, say creators // The Guardian [News website]. Available: https://www.theguardian.com/technology/2019/feb/14/elon-musk-backed-ai-writes-convincing-news-fiction

[18] Department of Defense Cyber Strategy // Department of Defense [Official website]. Available: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[19] Department of Defense Directive O-3600.01 // Federation of American Scientists [Official website]. Available: http://fas.org/irp/doddir/dod/info_ops.pdf

[20] Fiscal Years 2011–2013: IT Strategic Plan. Digital Diplomacy // 2009-2017 Department of State archive [Official website]. Available: https://2009-2017.state.gov/documents/organization/147678.pdf

[21] FM 3-05.30 MCRP 3-40.6 Psychological Operations // Federation of American Scientists [Official website]. Available: https://fas.org/irp/doddir/army/fm3-05-30.pdf

[22] H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019 // Congress.gov [Official website]. Available: https://www.congress.gov/bill/115-congress/house-bill/5515

[23] Individuals using the Internet, 2005-2019 // ITU [Official website]. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[24] Information Operations: The Hard Reality of Soft Power // IWS - The Information Warfare Site [Official website]. Available: http://iwar.org.uk/iwar/resources/jiopc/io-textbook.pdf

[25] J. Reid, L. Templeman, H. Allen, N. Burns and K. Nagalingam The Age of Disorder – the new era for economics, politics and our way of life // Deutsche Bank [Official website]. Available: https://www.dbresearch.com/servlet/reweb2.ReWEB?rwnode=RPS_EN-PROD$JIM_REID&rwsite=RPS_EN-PROD&rwobj=ReDisplay.Start.class&document=PROD0000000000511857

[26] Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms, November 8, 2010 (As Amended Through 15 February 2016) // Federation of American Scientists. [Official website]. Available: https://irp.fas.org/doddir/dod/jp1_02.pdf

[27] Joint Publication 3-13: Information Operations 27 November 2012 Incorporating Change 1 20 November 2014 // Federation of American Scientists [Official website]. Available: https://irp.fas.org/doddir/dod/jp3_13.pdf

[28] Joint Vision 2020 // PENTAGONUS [Official website]. Available: http://pentagonus.ru/doc/JV2020.pdf

[29] LEXICO // [Online] Available: https://www.lexico.com

[30] National Cyber Strategy of the United States of America // The White House [Official website]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[31] P. Waldman, L. Chapman, and J. Robertson Palantir Knows Everything About You // Bloomberg Businessweek [News website]. Available: https://www.bloomberg.com/features/2018-palantir-peter-thiel/

[32] Quadrennial Diplomacy and Development Review // 2009-2017 Department of State archive [Official website]. Available: https://2009-2017.state.gov/documents/organization/241429.pdf

[33] Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach // The Guardian [News website]. Available: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
[34] Q. Zhang, B. Guo, H. Wang, Y. Liang, S.Hao, and Z. Yu, AI-Powered Text Generation For Harmonious Human-Machine Interaction: Current State And Future Directions // ArXiv.org [Online]. Available: https://arxiv.org/abs/1905.01984