Научная статья
https://doi.org/10.24412/2220-2404-2024-6-49
УДК 316

ОТЕЧЕСТВЕННЫЕ ПРАКТИКИ ПРОТИВОДЕЙСТВИЯ ТЕХНОЛОГИЯМ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ

Карепова С.Г., Некрасов С.В.
Институт социологии ФНИСЦ РАН

Аннотация. *В статье рассматривается актуальная и востребованная в условиях современной социальной реальности научно-практическая проблематика, посвященная отечественным практикам противодействия технологиям информационного воздействия. Данное направление актуализировано как в научной сфере, так и в нормативных государственных документах, отвечающих за национальную безопасность страны, а также в практике общественного запроса. Отмечается значимая роль социокультурного аспекта в рамках воздействия на общественное сознание отвечающего за конструирующий потенциал социума. По результатам изучения нормативных документов, разрозненных профильных исследований выявлены отечественные практики противодействия технологиям информационного воздействия и объединены в авторскую типологию, дающую о них наглядное представление. Констатируется важность изучения данной проблематики. Статья имеет выраженный теоретико-методологический и практико-ориентированный характер.*

Ключевые слова*: технологии, информационное воздействие, безопасность, сознание, социокультурный аспект, социум, противодействие, угрозы, методы.*

DOMESTIC PRACTICES TO COUNTERACT INFORMATION INFLUENCE TECHNOLOGIES

Svetlana G. Karepova, Sergey V. Nekrasov
Institute of Sociology of FCTAS RAS

Abstract. *The article deals with a scientific and practical range of problems, devoted to domestic practices to counteract information influence technologies, is relevant and demanded in modern social reality. This direction has taken on increasing importance both in science and in the country's regulatory state documents on national security, in the practice of a public request as well. The article notes the significant role of a sociocultural aspect in the influence of public consciousness that replies for the constructive potential of a society. Based on the results of studying the regulatory documents, field-oriented separate research, the authors identified domestic practices to counteract information influence technologies and integrated them into an authorial typology that provides its clear picture. Studying this range of problems is of importance. The article has a great theoretical methodological and practice-oriented nature.*

Keywords*: technologies, information influence, security, consciousness, sociocultural aspect, society, counteraction, threats, methods.*

Введение.

Социетальные трансформации современной социальной реальности России 2020-х гг., являясь частью процессов развития, поставили также на повестку дня вопросы, связанные с ее сохранением, стабилизацией и управлением.

Обсуждение.

Ключевой характеристикой новой социальной реальности стало состояние ее нестабильности и перманентной изменяемости, влекущее за собой «подвижность» во внутренних процессах и структурах современного социума. Данные бифуркационные тенденции нашли отражение в череде таких событий, как:

- прорывные, но негативно воздействующие на природу и общество достижения (информационно-коммуникационные и социальные технологии);
- попирание духовно-нравственных ценностей, нарушение норм международного права;
- спровоцированная Западом и вынужденно проводимая Россией в Украине специальная военная операция (СВО) и т.д.

Синергетический эффект от данных трансформаций, как было отмечено выше, спровоцировал развитие трудно управляемой, лабильной и «не предсказуемой» социальной реальности.

Исходя из качеств самой природы новой реальности, разумно вести речь и о значительном усилении ее рисковой составляющей, что порождает развитие таких *рисков и угроз для безопасности страны, с которыми современное общество еще не сталкивалось*. Эти угрозы обладают скрытым отложенным эффектом воздействия на социум и скажутся только в будущем. *Они информационно воздействуют на глубинные слои сознания и подсознания социума, вовлекая его в формат развязанной из вне информационной войны*.

Современные информационные войны, будучи неотъемлемой частью гибридных войн, нацелены на весь социетальный уровень общества и на глубинное поражение социокультурной сферы социума, в частности, а эта опасность обуславливается воздействием на системообразующие общественные институты. К ним относятся: наука, образование, вера, семья, мораль и др., отвечающие за духовно-нравственную целостность общества, его крепость, культурно-историческую преемственность и сформированные через систему данных институтов легитимные ценности и положительный исторический опыт.

В данном контексте, информационные войны ориентированы на дестабилизацию общества и, в конечном счете, его разрушение через глубокое информационное воздействие на коллективное сознание и психику. Вся транслируемая СМИ, в рамках подобных войн, информация активно поглощается массовым сознанием, а далее, на основе усвоенного информационного контента, социумом принимаются ключевые решения, определяющие его будущую парадигму развития. «…Речь идет о информационной основе для объективизации субъективной деятельности человечества, как главного актора цивилизационного строительства» [1, с. 205]

По существу, социальная реальность вокруг человека есть ни что иное как результат его деятельности, осуществленной на основе представлений (нравственных, научных, политических, экономических и т.д.) об окружающем мире.

За счет информационного воздействия на сознание и функционально-психическую деятельность осуществляется изменение мышления социума, а, следовательно, и управление им. Вот почему так важно качество и контроль над распространяемой СМИ и «потребляемой» обществом информацией. Во избежание провоцирования общества на создание ложных смыслов и разрушительного поведения в сторонних интересах, *актуализируется аспект изучения и сохранения информационной безопасности и, как следствие, практик противодействия технологиям информационного воздействия на правовом и научном уровнях.*

Правовый уровень проблематики нормативно концептуализирован на федеральном уровне:

- в Стратегии национальной безопасности РФ от 02.07.2021 г. N 400, в четвертом (информационная безопасность) приоритете; при этом сам феномен информационной безопасности взаимоувязан с остальными стратегическими приоритетами;

- в Законе РФ «О государственной тайне» от 21.09.1993 г. N 5485-1; Стратегии развития информационного общества в РФ на 2017-2030 гг. от 09.05.2017 г. N 203 и т.д.

Информационная безопасность представлена как феномен, детерминирующий всю социетальную сферу общества, обусловливая ее функционирование.

Теоретико-методологическая разработанность данного научного направления достаточная, что нашло свое отражение в ряде исследований отечественных ученых [2, с. 151]. Но, на фоне общей теоретической разработанности таких аспектов, как:

- концептуализация важности защиты психики социума от негативного информационного влияния;

- проблематика воздействия сети Интернет и виртуального пространства на психику человека;

- психолого-политологические аспекты информационных войн;

- вопросы правового обеспечения защиты сведений и др.,

выраженную значимость приобретает именно практико- ориентированное направление сохранения информационной безопасности – практики (меры) противодействия технологиям информационного воздействия.

С учетом уже имеющихся научных разработок, законодательного регулирования по проблематики и эффективно используемых в ежедневной работе (СМИ, органы государственной власти и др.) практик противодействия технологиям информационного воздействия целесообразно, в рамках данной

работы авторам данного исследования удалось актуализировать их и системно объединить в авторскую типологию. Данная типология включает в себя и новые направления противодействия, которые с нашей точки зрения, обладают большим потенциалом, уже применяются на практике и будут использоваться в будущем.

Результаты. Из всего разнообразия, выделяемых в нормативных документах, научной литературе и зарекомендовавших себя новых отечественных защитных практик (мер) противодействия технологиям информационного воздействия, на наш взгляд, целесообразно сформировать четыре основные группы, которые можно содержательно классифицировать в соответствии:

- с социетальными сферами общества, подверженными воздействию и требующими защиты;
- по степени соответствия ряду ключевых приоритетов сохранения национальной безопасности, отраженных в Стратегии национальной безопасности РФ от 02.07.2021 г. N 400 [3];
- в связи с основными СМИ средами, в которых осуществляется распространение и информационное воздействие;
- с возникновением новой сферы информационного воздействия и дезинформации через распространение фейковых новостей.

Первая группа защитных практик (мер) отвечает за сохранение социетальной сферы жизнедеятельности российского общества. Важность рассмотрения данного аспекта обусловлена тем, что сам феномен информатизации носит социетальный характер, опосредованный совокупностью экономических, политических, социокультурных факторов жизни социума, и относится к многосторонним, но целостным явлениям. Иными словами, происходит информационное воздействие на социум в рамках социально-экономического, политико-правового и социокультурного направлений, что взаимосвязаны между собой как единое явление.

Данная группа мер направлена на формирование нормативной базы (разработка законодательных и профильных методических актов), осуществление финансовой политики РФ, выработку административных и научно обоснованных норм, действий в сфере управления большими и малыми системами, развитием институтов гражданского общества, создание соответствующих условий для развития учреждений культуры и т.д. Особое внимание отведено сохранению и возрождению культурного наследия, контролю и цензуре. Речь идет о следующих действиях (Рис. 1):

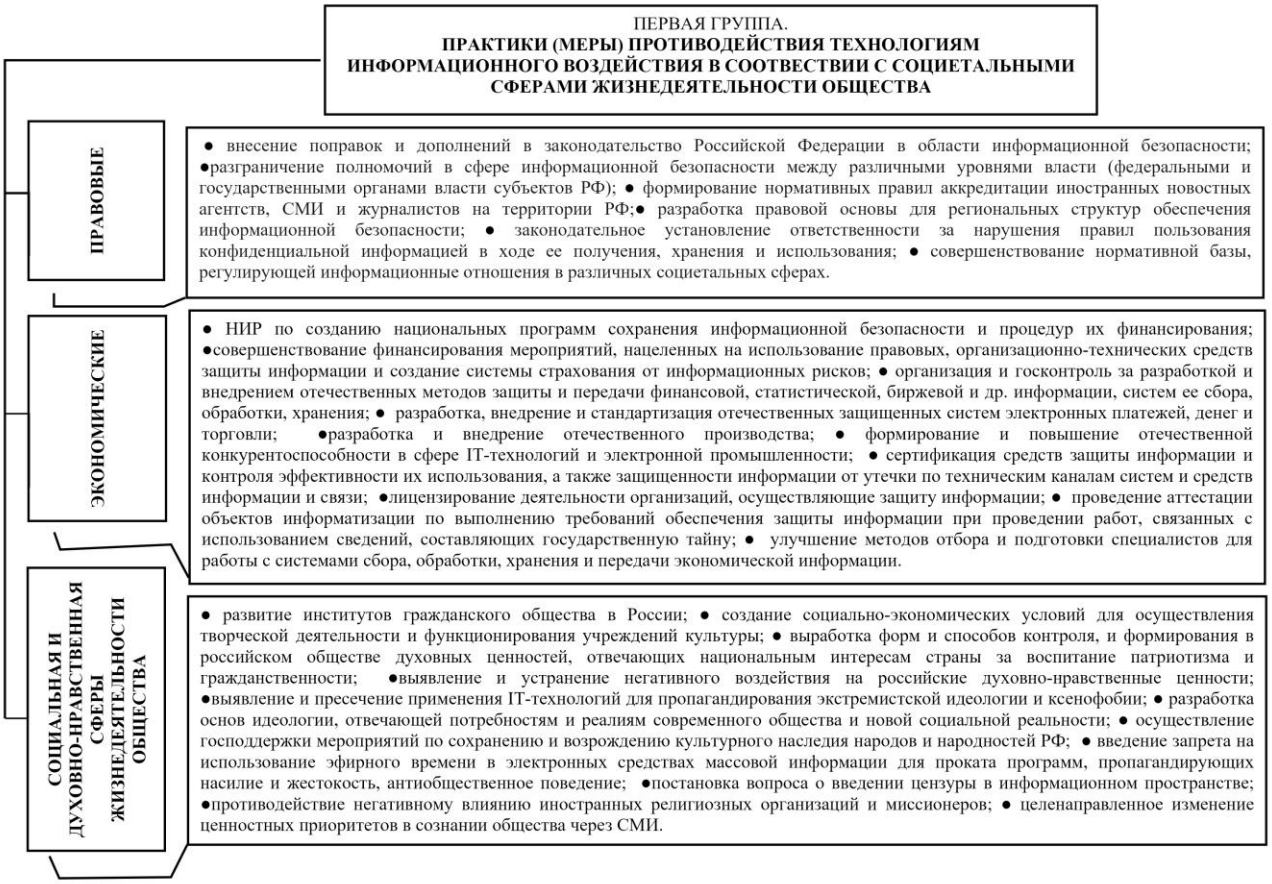

Рисунок 1 – Первая группа практик (мер) противодействия технологиям информационного воздействия .

Примечание: источник – собственная разработка по материалам [1, с. 212; 3; 4, с. 28-30].

На законодательном уровне государством также приняты меры в отношении ряда организаций, отдельных лиц, деятельность которых на территории РФ признана нежелательной. В частности, согласно данным Минюста РФ, реестр иностранных агентов с начала проведения СВО на Украине насчитывает свыше 100 организаций, общественных объединений и людей, обвинённых по статьям (Ст. 6 Закона РФ от 27.12.1991 №2124-1 «О средствах массовой информации»; Ст. 29.1 от 19.05.1995 №82-ФЗ «Об общественных объединениях»; Ст. 32 от 12.01.1996 №7-ФЗ «О некоммерческих организациях; Ст. 2.1. От 28.12.2012 №272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан РФ»; Ст. 9 от 14.07.2022 №255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием»).

По данным того же Минюста РФ, за период 2022 по 2024 гг. было выявлено около 60 иностранных и международных неправительственных организаций, деятельность которых на территории РФ нежелательна (Russian America for Democracy in Russia – «Русская Америка за демократию в России», США; Russian antiwar committee «Антивоенный комитет России»); Center for Civil Liberties – «Общественная организация «Центр Гражданских Свобод», Украина и др.).

С 2022 по 2024 гг. было принято в судебном порядке (Федеральный закон от 25.07.2002 №14-ФЗ «О противодействии экстремистской деятельности») решение и о ликвидации или запрете на территории РФ около 20 общественных объединений и религиозных организаций (Американская транснациональная холдинговая компания Meta Platforms Inc. по реализации продуктов – социальных сетей Facebook и Instagram; Общественное объединение «Этническое национальное объединение»; Международное общественное движение ЛГБТ и его структурные подразделения и др.).

В реестр террористических организаций, по данным Совета Безопасности РФ за период 2022 по 2023 гг., попало около 14 организаций, в том числе иностранных и международных, признанных таковыми (Террористическое сообщество – «московская ячейка» МТО «ИГ»; Международное молодежное движение «Колумбайн» (другое наименование «Скулшутинг»); Украинское военизированное объединение легион «Свобода России» (другое используемое наименование «Легион Свобода России»); Международное движение «Маньяки Культ Убийц» (другие используемые наименования «Маньяки Культ Убийств», «Молодёжь Которая Улыбается», М.К.У.) и др.).

Вторая группа защитных практик (мер) нацелена на поддержание ряда ключевых приоритетов сохранения национальной безопасности, с которыми феномен информационной безопасности взаимоувязан и которые он детерминирует (защита конституционного строя, суверенитета, независимости, государственной и территориальной целостности РФ, укрепление обороны страны; развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия; укрепление традиционных российских духовно-нравственных ценностей, сохранение культурного и исторического наследия народа России; поддержание стратегической стабильности, укрепление мира и безопасности, правовых основ международных отношений и т.д.), отраженных в Стратегии национальной безопасности РФ от 02.07.2021 г. N 400 [3]. Эта группа представлена следующими направлениями противодействия (Рис. 2):

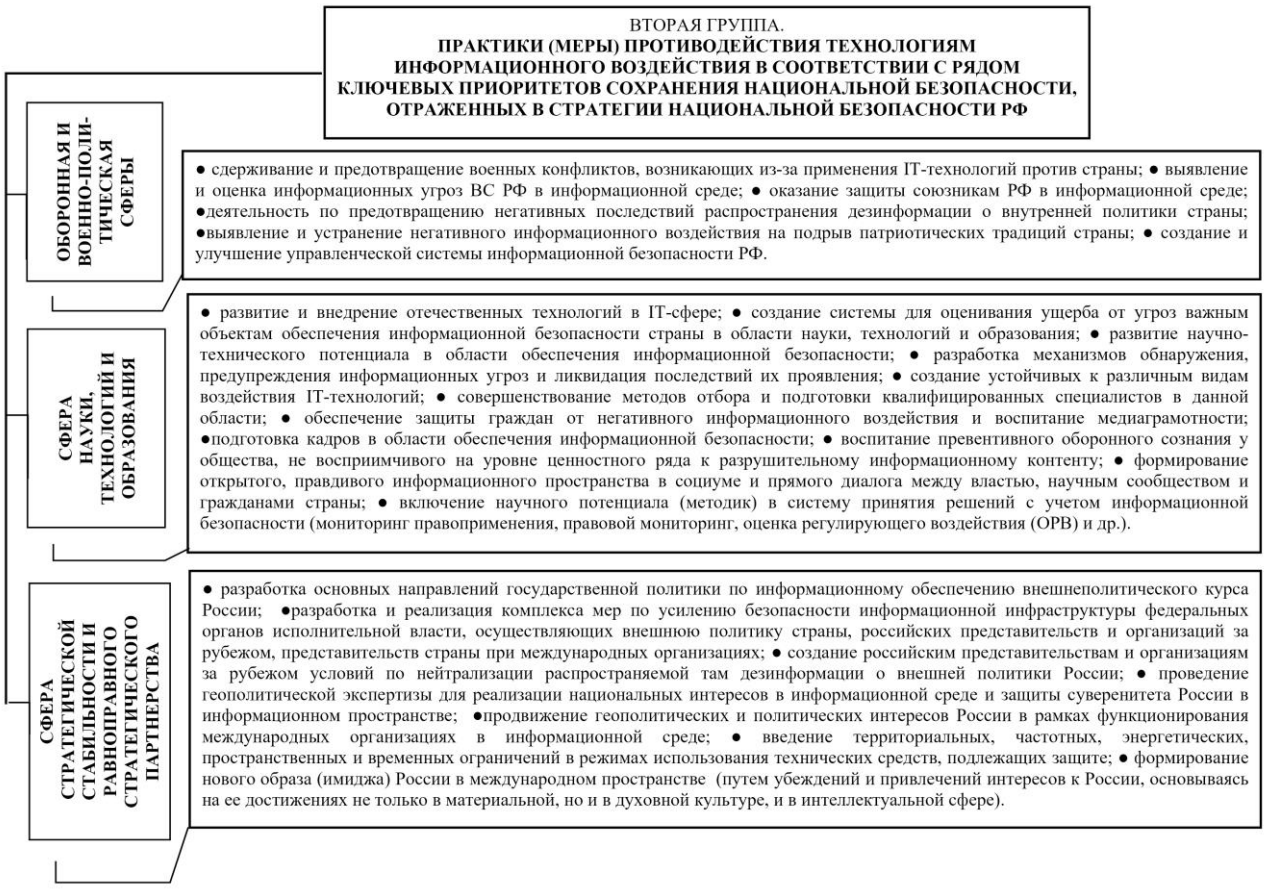

Рисунок 2 – Вторая группа практик (мер) противодействия технологиям информационного воздействия.

Примечание: источник – собственная разработка по материалам [2, с. 213-215; 3; 4, с. 28-31; 5, с. 11].

Третья группа представлена мерами противодействия информационному воздействию в соответствии с основными информационными средами (печатные СМИ, онлайн-СМИ, социальные сети и блогерство), которыми оно детерминировано и в которых оно осуществляется. Именно

среды во многом определяют успешность или не успешность данного воздействия. К основным мерам этого направления следует отнести (Рис. 3):

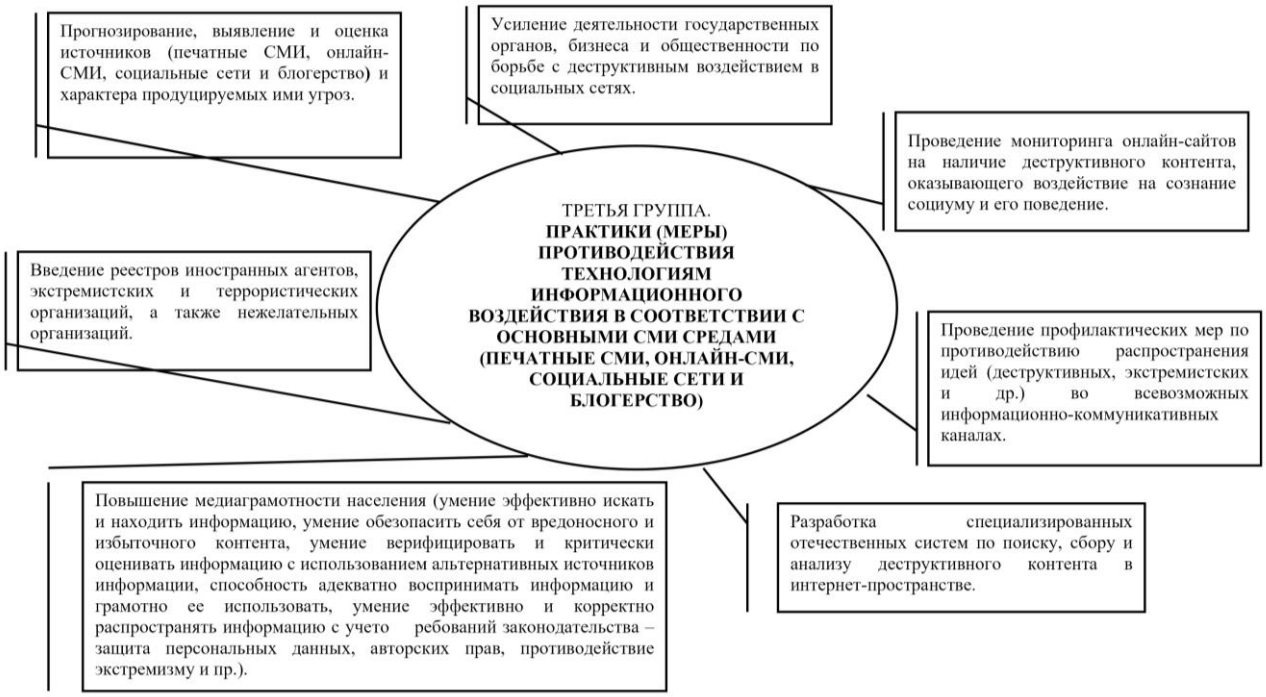

Рисунок 3 – Третья группа практик (мер) противодействия технологиям информационного воздействия.

Примечание: источник – собственная разработка по материалам [6, с. 110-111; 7, с. 125].

По данным совместного опроса, проведенного в 2023 году Motive agency & production и Институтом общественного мнения «Анкетолог», блогеров смотрят ежедневно более трети россиян (36%), несколько раз в неделю – 45% наших соотечественников, один раз в неделю – 11% интересующихся, нерегулярно – всего 9%. Основными каналами для просмотра блогеров среди россиян являются YouTube – 68%, Telegram – 63%, ВКонтакте – 55%, Дзен – 43%, ТикТок – около трети россиян 30%, Instagram (соцсеть признана экстремистской и запрещена в России) – 24%, «Одноклассники» – 23%.

Особую роль в этом информационном контенте играют, так называемые, инфлюенсеры. По популярности рейтинг инфлюенсеров на период 2023 года среди россиян выглядел следующим образом: Анастасия Ивлеева – 15% (является, в настоящее время, подследственным лицом), Юрий Дудь (признан в России иноагентом по решению Минюст РФ) – 13%, Дмитрий Куплинов – 10%, Илья Варламов (признан в России иноагентом по решению Минюст РФ) – 10%, Ольга Бузова – 8%, Ксения Бородина, Ксения Собчак и Михаил Литвин – по 7% соответственно [2, с. 153].

Четвертая группа защитных практик (мер) направлена на противодействие распространению в информационном пространстве достаточно нового феномена и эффективного инструмента управления сознанием и поведением социума. Речь идет о фейковых новостях и процессах дезинформации, на которых, как требующих предотвращения, следует остановится более подробно. В настоявшее время данное направление представлено следующими практиками (Рис. 4):

Рисунок 4 – Четвертая группа практик (мер) противодействия технологиям информационного воздействия.

Примечание: источник – собственная разработка по материалам [4, с. 28; 8, с. 82].

Примером противодействия на законодательном уровне распространению фейковой информации в сети Интернет и в период проведения СВО на Украине является блокировка Instagram, Facebook, Twitter и др. социальных сетей, через которые распространялась недостоверная информация о Вооруженных Силах России и руководстве страны.

Также, на законодательном уровне закреплены штрафы за распространение фейковой информации (от 30 до 500 тысяч рублей в зависимости от тяжести содеянного), введено уголовное наказание (не только в отношении СМИ, но физических лиц) за распространение недостоверной информации об Вооруженных Силах РФ, призывы к санкциям против России (до 15 лет лишения свободы).

Примером применения специализированных систем по поиску и анализу разного рода деструктивного контента и фейков может служить:

Во-первых – автоматизированная система «Георгий Победоносец», разработанная в 2018 году Пермской компанией ООО «СЕУСЛАБ». Ее основная цель – выявление контента, несущего пагубные идеи для сознания социума, а также контента, который используется информационными экстремистскими источниками для вербовки населения в запрещенные организации и объединения.

Во-вторых – «Крибрум» – система многофакторного мониторинга, сбора и анализа социальных медиа в режиме реального времени, разработанная исследовательской и технологической компанией АО «Крибрум» в 2010 году [9, с. 98] и имеющая свою научно-практическую и образовательную платформу на базе ВШССН МГУ им. М.В. Ломоносова под руководством академика Г.В. Осипова. Это может служить примером симбиоза социологического знания и научно-практического бизнес-контента.

Ярким примером подготовки специалистов в области противодействия распространению фейковой информации можно считать, разработанную группой ученых А.В. Манойло и В.И. Теличко в сентябре 2020 года, авторскую методику обучения специалистов способам и технологиям отражения фейков. Эта методика была опробована в октябре 2020 года на образовательной

площадке Федерального форума «Дигория» в рамках политико-коммуникационного трека, направленного на обучение участников форума методикам распознания, разоблачения и отражения фейковых новостей. Методика продемонстрировала свою эффективность и может быть применена для подготовки специалистов для различных управлений Администрации Президента РФ.

Обучение основывается на операционной последовательности таких действий, как:

- выявление и распознание фейка;
- первичный перехват информационной повестки у фейка (разоблачение); создание «вирусного антифейка», способного перехватить у фейка повестку, и вброс его в информационное пространство;
- «запуск встречной информационной волны», способной «сбить фейк на взлете»;
- вброс, поддерживающих «волну» антифейков и иного вирусного контента; оперативная социология [10, с. 82].

Также, отдельного внимания, в рамках изучения практик (мер) противодействия информационному воздействию, требует широко обсуждаемый и противоречивый вопрос о введении цензуры как решающего превентивного метода.

Согласно данным ВЦИОМ за 2021 год, о необходимости введения цензуры в интернете, «…большинство россиян (60%) считают, что необходимость в ней определяется конкретным типом информации, 11 % россиян – за свободное распространение информации в интернете, 26 % считают, что информация в сети-Интернет нуждается в цензурировании.

О необходимости ограничения информации в интернете, связанной с оружием, взрывчатыми веществами и их производством из подручных материалов заявляют большинство россиян (91%).

Столько же россиян (91%) ратуют за ограничение информации, содержащей призывы к вступлению в радикальные, экстремистские группировки.

По мнению большинства россиян, необходимо также ограничить призывы к вступлению в религиозные секты (89%), информацию о самоубийствах (88%), подвергнуть цензуре порнографические материалы (84%), сцены насилия, агрессии в видео, компьютерных играх (82%)» [11].

Также, по мнению респондентов, следует ограничить доступ к материалам, «…содержащим нецензурную лексику и информацию о финансовых компаниях по типу «МММ» (73-74%). 78 % россиян согласны с тем, что необходимо предпринимать меры борьбы с подобной информацией в интернете» [11].

Заключение.

Таким образом, с нашей точки зрения, основные направления противодействия технологиям информационного воздействия в отечественной практике представлены на всех социетальных уровнях государственной политики, обозначенными выше содержательными блоками. Безусловно, приведенный в авторской типологии перечень отечественных практик (мер) противодействия технологиям информационного воздействия далеко не исчерпывающий. Он содержательно требует дальнейшего расширения и углубления в контексте трансформаций социальной реальности, общей геополитической ситуации в стране и социального запроса от общества. Целесообразно задуматься и о выработке новых превентивных практик, нацеленных на безопасное информационное обеспечение жизнедеятельности человека, государства и общества. Актуальность научно-практического направления изучения данного феномена будет только возрастать.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Литература:

1. Карепова С.Г., Некрасов С.В., Пинчук А.Н. Информационная безопасность: специфика феномена, методы и способы ее обеспечения // Вестник Московского университета. Серия 18. Социология и политология. – 2023. – Т.29. – №4. – С. 200-220. DOI: 10.24290/1029-3736-2023-29-4-200-220.

2. Карепова С.Г., Некрасов С.В. Технологии информационного воздействия на общественное сознание в условиях современных социокультурных трансформаций России // Социально-гуманитарные знания. – 2024. – № 3. – С. 150-156. DOI: 10.34823/SGZ.2024.03.52050.

3. Указ Президента РФ от 02.07.2021 г. N 400 «О стратегии национальной безопасности Российской Федерации» / КосультантПлюс [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 10.05.2024).

4. Фалеев М.И., Черных Г.С. Угрозы национальной безопасности государства в информационной сфере и задачи МЧС России в этой области деятельности // Стратегия гражданской защиты: проблемы и исследования. – 2014. – Том 4. – №1(6). – С. 21-34.

5. Путин В.В. Россия в меняющемся мире: преемственность приоритетов и новые возможности // Вестник МГИМО-Университета. – 2012 – №4(25). – С. 8-11. DOI: 10.24833/2071-8160-2012-4-25-8-11.

6. Казаков А.В. Противодействие негативному информационному воздействию на сознание российской молодежи // Власть. – 2015. – №9. – С. 107-112.

7. Задорин И.В., Мальцева Д.В., Шубина Л.В. Уровень медиаграмотности населения в регионах России: сравнительный анализ // Коммуникация. Медиа. Дизайн. – 2017. – Том 2. – №4. – С. 123-141.

8. Зырянова М.О. Способы противодействия распространению фейковой информации // Общество: социология, психология, педагогика. – 2020. – №6. – С. 80-83.

9. Еськов А.В., Цымбал В.Н. Противодействие распространению идеологии экстремизма в сети Интернет как условие общественной безопасности // Вестник Краснодарского Университета МВД России. – 2023. – №1(59). – С. 96-100.

10. Манойло А., Теличко В., Попадюк А. Методика противодействия фейковым новостям // Международная жизнь. – 2021. – №7. – С. 78-93.

11. Интернет: возможности или угроза? / ВЦИОМ [Электронный ресурс]. – Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-vozmozhnosti-ili-ugrozy (дата обращения: 10.05.2024).

References:

1. Karepova S.G., Nekrasov S.V., Pinchuk A.N. Information security: key features of the phenomenon, its methods and means // Moscow State University Bulletin. Series 18. Sociology and Political Science. – 2023. – Vol.29. – No.4. – PP. 200-220. DOI: 10.24290/1029-3736-2023-29-4-200-220.

2. Karepova S.G., Nekrasov S.V. Technologies of information impact on public consciousness in the conditions of modern sociocultural transformations in Russia // Social and Humanitarian Knowledge. – 2024. – No.3. – PP. 150-156. DOI: 10.34823/SGZ.2024.03.52050.

3. RF Presidential Decree of 02.07.2021 N 400 «On the strategy for the national security of the Russian Federation" / ConsultantPlus [Electronic source]. – Available at https://www.consultant.ru/document/cons_doc_LAW_389271/ (accessed on 10.05.2024).

4. Faleev M.I., Chernykh G.S. Threats to the state's national security in the information sphere and the tasks of MchS of Russia // Civil Protection Strategy: problems and research. – 2014. – Vol.4. – No.1(6). – PP. 21-34.

5. Putin V.V. Russia in a changing world: the continuity of the priorities and new opportunities // MGIMO Review of International Relations. – 2012. – No.4(25). – PP. 8-11. DOI: 10.24833/2071-8160-2012-4-25-8-11.

6. Kazakov A.V. Counteracting a negative information influence on Russian youth's consciousness // Vlast'. – 2015. – No.9. – PP. 107-112.

7. Zadorin I.V., Maltseva D.V., Shubin L.V. Evaluating medialitecy of citizens of Russian regions: comparative analysis // Communication. Media. Design. – 2017. – Vol. 2. – No.4. – PP. 123-141.

8. Zyryanova M.O. Ways to combat the spread of "fake information" // Society: sociology, psychology, pedagogy. – 2020. – No.6. – PP. 80-83.

9. Eskov A.V., Tsymbal V.N. Countering the spread of ideology of extremism on the Internet as a condition for social security // Krasnodar University of the Ministry of Internal Affairs of Russia Bulletin. – 2023. – No.1(59). – PP. 96-100.

10. Manoilo A., Telichenko V., Popadyuk A. The method of counteracting fake news // The International Affairs. – 2021. – No.7. – PP. 78-93.

11. Internet: opportunities or threat? / VCIOM [Electronic source]. – Available at https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-vozmozhnosti-ili-ugrozy (accessed on 10.05.2024).

Информация об авторах:

Карепова Светлана Геннадьевна, кандидат социологических наук, ведущий научный сотрудник, Институт социологии ФНИСЦ РАН, Москва, E-mail: svetlran@mail.ru.

Некрасов Сергей Владимирович, научный сотрудник, Институт социологии ФНИСЦ РАН, Москва, E-mail: sv_79@inbox.ru.

Svetlana G. Karepova, PhD in Sociology, leading researcher, Institute of Sociology of FCTAS RAS, Moscow.

Sergey V. Nekrasov, researcher, Institute of Sociology of FCTAS RAS, Moscow.