Научная статья
https://doi.org/10.24412/2220-2404-2025-6-16
УДК 355.01

ТЕХНОЛОГИИ ПРОТИВОДЕЙСТВИЯ ВЛИЯНИЮ СЕТЕВЫХ АКТОРОВ НА СОЗНАНИЕ МОЛОДЕЖИ В ХОДЕ ИНФОРМАЦИОННОЙ ВОЙНЫ

Лушников Д.А.[1], Долгополов К.А.[2], Кузнецова О.Н.[3]
Северо-Кавказский федеральный университет[1,2,3],
https://orcid.org/0000-0003-0352-4662[1], https://orcid.org/0000-0003-4496-1789[2],
https://orcid.org/0009-0007-6949-8491[3],

Аннотация. *Рассматриваются основные технологии, методы и практики противодействия влиянию сетевых акторов на сознание молодежи в ходе информационной войны. Делаются выводы о необходимости: 1) координации деятельности различных ведомств и органов в вопросе информационного противодействия; 2) определенных ограничениях и запретах на распространение информационных данных; 3) проработки на законодательном уровне правовых норм, позволяющих региональным прокурорам в случае экстренной необходимости блокировать интернет-ресурсы, задействованные в информационных атаках; 4) использования больших языковых моделей (LLM) и машинного обучения искусственного интеллекта (machine learning, ML) в отслеживании распространения контента по различным цифровым каналам коммуникации, социальным сетям и новым медиа; 5) ограничения для доступа в киберпространство страны для сервисов и сайтов, признанных нежелательными и экстремистскими должны сочетаться с процессом создания их российских аналогов и/или популяризации уже имеющихся отечественных программ, сервисов и информационных ресурсов; 6) повышения медиаграмотности населения.*

Ключевые слова: *информационная война, информационное противоборство, информационное противодействие, молодежь, сетевые акторы, дезинформация, пропаганда, скрытая пропаганда, контрпропаганда.*

Финансирование: *Исследование выполнено в рамках государственного задания Министерства науки и высшего образования Российской Федерации № 1023112800142-3-5.4.1. «Технологии противодействия информационным войнам в молодежной среде» (FSRN-2024-0009).*

TECHNOLOGIES FOR COUNTERING THE INFLUENCE OF NETWORK ACTORS ON THE CONSCIOUSNESS OF YOUNG PEOPLE DURING THE INFORMATION WAR

Dmitry A. Lushnikov, **Kirill A. Dolgopolov**, **Oksana N. Kuznetsova**
North Caucasus Federal University

Abstract. *The main technologies, methods and practices of countering the influence of network actors on the consciousness of young people during the information war are considered. Conclusions are drawn about the necessity of: 1) coordination of the activities of various departments and bodies in the issue of information counteraction; 2) certain restrictions and prohibitions on the dissemination of information data; 3) elaboration at the legislative level of legal norms that allow regional prosecutors, in case of emergency, to block Internet resources involved in information attacks.; 4) the use of large language models (LLM) and machine learning of artificial intelligence (ML) in tracking the distribution of content through various digital communication channels, social networks and new media; 5) restrictions on access to the cyberspace of the country for services and sites deemed undesirable and extremist should be combined with the process of creating their Russian analogues and/or popularization of existing domestic programs, services and information resources; 6) increase the media literacy of the population.*

Keywords: *information war, information confrontation, information counteraction, youth, network actors, disinformation, propaganda, hidden propaganda, counter-propaganda.*

Funding: *The research was carried out within the framework of the state assignment of the Ministry of Science and Higher Education of the Russian Federation No. 1023112800142-3-5.4.1. «Technologies for countering information warfare among young people» (FSRN-2024-0009).*

Введение.

Информационная война является одним из признаков и неотъемлемым атрибутом современной эпохи окончания глобализации, фрагментации «мирового сообщества», макрорегионализации, разворачивающегося ресурсного кризиса и, как следствие, обострения имеющихся противоречий и роста конфликтогенности внутри «мир-системы».

Данное явление выступает в двух основных функциональных ипостасях: милитарной и гражданской.

В первом случае, информационная война (IW) является как частью, так и определенным этапом современной сетецентрической войны. Информационная война выступает в качестве первого важнейшего этапа войны, предваряет военные действия и потом на всем протяжении сопровождает их. Д. Гленн интерпретирует (IW) как «…использование информационно-коммуникационных технологий в ситуации вооруженного конфликта для получения преимущества над противником посредством воздействия на его военное и политическое руководство, армию и гражданское население» [1, с. 17].

Осуществляется она специализированными центрами информационно-психологических операций и т.п., входящими в структуру современных армий. На оперативном уровне информационная война ведется как единая комплексная информационно-пропагандистская компания, состоящая из отдельных «информационно-психологических» или «психологических операций» (PSYOP), в 2010 году в Вооруженных силах США переименованных в «операции по информационной поддержке военных действий» (Military Information Support Operations (MISO).

Конечными целями информационно-психологического пропагандистского воздействия «операций по информационной поддержке военных действий» является, в первую очередь, высшее военное и политическое руководство страны-противника, далее командный и рядовой состав армии и уже после – общественное сознание. Однако механистически данная иерархия целей может достигаться и инверсивно, от обратного; то есть, сначала добиваясь первоначального воздействия на общественное сознание, а уже потом на сознание и поведение институциональных агентов, отвечающих за безопасность и ведение военных действий.

Методология и методы.Информационная война имеет и сугубо «гражданское» применение и сначала отделяется от своей милитарной онтологии, а потом начинает существовать самостоятельно, без привязки к функции сопровождения военных действий. В конечном итоге, конвенциональной становится точка зрения, демонстрируемая У. Черчем, разделяющего это явление на два вида: «Информационная война, не сопровождающаяся применением физической силы» и «информационная война, сопровождающаяся применением физической силы» [2, с. 46].

Авторская интерпретация определяет информационную войну как планируемую и целенаправленную кампанию по негативному информационно-пропагандистскому и информационно-психологическому воздействию. Данное воздействие может осуществляться, имея в качестве объекта, как все общественное сознание конкретного общества, так и сознание отдельных социальных общностей и групп.

Проблема воздействия на общественное сознание со стороны враждебных акторов в киберпространстве решается в рамках, так называемого, «информационного противоборства» или «информационного противодействия».

Термин «информационное противоборство» более характерен для специалистов в области военно-информационных технологий, поскольку предполагает их ответное участие в информационной войне и, как следствие, ведение не только оборонительных, но и атакующих действий в киберпространстве.

Использование же термина «информационное противодействие», в большей степени, характерно для невоенных специалистов, ученых и представителей профессионального и экспертного сообщества в области IT-технологий. Это разделение прослеживается как в научных трудах, так и документах, регламентирующих данный вид деятельности у военных специалистов.

Информационное противоборство разделяется на два основных направления: информационно-техническое и информационно-психологическое. А. В. Шевырёв и А. Ю. Замятин выделяют следующие направления информационного противоборства:

- оперативное получение информации о существующих и перспективных методах и средствах противника, вовлечённых в информационное противодействие (в том числе – информационные системы, средства связи противника и алгоритмы их применения);

- комплексное совершенствование собственных систем и сетей связи, а также алгоритмов применения (повышение помехозащищённости, скрытности и т.п.); эффективности, гибкости,
- развитие собственных информационных систем, средств формирования и предоставления информационных ресурсов;

- развитие собственных средств информационного противодействия (включая средства радиоэлектронной борьбы, «кибератак» и подобных средств ведения информационной войны);

- совершенствование защиты от средств информационного противодействия противника [3, с. 1131].

В случае информационно-технического противоборства, основными объектами атаки и защиты являются информационно-технические системы: системы и центры обработки данных, системы передачи и хранения данных, системы защиты информации и управления.

Информационно-психологическое противоборство предполагает в качестве объектов атаки и защиты представителей военно-политического руководства и правящей элиты, то есть субъектов системы принятия решений, субъектов системы формирования общественного мнения и сознания, психику населения.

В структуре и последовательности мер информационного противоборства как гуманитарные, так и военные специалисты выделяют схожую стадиальность, которую можно обобщить следующим образом:

- перманентный мониторинг информационного потока, сбор информации, оценка текущей ситуации;
- на основании анализа текущей ситуации и возможному ее развитию принимаются решения по реализации мер информационного противодействия и/или ответного информационного воздействия;
- реализация мер информационного противодействия;
- анализ и оценка достигнутых результатов проведённых мероприятий;
- принятие решений по совершенствованию методов и инструментов информационного противодействия;
- пополнение базы данных и знаний.

Обсуждение. Результаты.

К.С. Стригунов в рамках проблематики контрмер в «неклассических войнах» указывает на то, что противодействие агрессору носит в них комплексный характер и должно осуществляться в следующих сферах:

1) информационно-психологической сфере (в т.ч. идейно-ценностной, т.е. ментальной, когнитивной и т.п.);
2) экономической сфере;
3) в научно-технологической сфере [4, с. 206].

Антироссийская компания, начатая в странах Запада в 2022 году в начале СВО, обнаруживает все признаки информационной войны, поскольку носит целенаправленный и скоординированный характер. Более того, некоторый создаваемый контент носил характер «информационных закладок», то есть создавался заранее и вбрасывался системно по различным каналам коммуникации. Ее основные цели — это международная и информационная изоляция РФ, дегуманизация («расчеловечивание») как всех россиян, так и непосредственно представителей русского этноса. Были использованы методы постправды, фейковой волны, морального мандата, остракизма и дегуманизации через «cancel culture» («культуру отмены»).

Данная антироссийская компания имела две основных аудитории: собственно, россиян и широкую международную аудиторию, представленную не только странами Запада.

Относительно россиян, упор делался на информационно-психологическом подавлении и деморализции, дезориентации относительно происходящих действий сторон, подавлении воли к сопротивлению, демобилизации общественного сознания. Особую роль играл пропагандистский и шокирующий материал, создаваемый под молодежный сегмент российской аудитории, поскольку представители молодежи более мобильны в использовании различных каналов коммуникации и обмене контентом.

Противодействие массированным информационным атакам со стороны российских ведомств запаздывало и носило несистемный и нескоординированный характер. Постепенно выстраивались механизмы противодействия негативному контенту, фейкам и дезинформации в связке российских спецслужб, ведомств, СМИ и представителей гражданского общества – волонтеров, блогеров и т.п.

Постепенно, российский контент стал активно вытеснять вражеский и их противодействие стало носить характер затяжной информационной войны «на истощение». Пророссийские нарративы стали рассматриваться общественным сознанием как более убедительные, но это получилось значительно позже, и первая фаза информационной войны была тяжела для морально-психологического и психосоматического состояния российского общества.

В американской концепции «сетецентрической войны» информационная война рассматривается как первый этап собственно вооруженных действий. Она должна предварять и сопровождать военные действия и на первом этапе вестись как «молниеносная война» («блицкриг»), противник и его общественное сознание должны быть полностью дезориентированы, деморализованы и подавлены.

Украинские центры информационно-психологических операций организовывались, в свое

время, под руководством британских и американских специалистов по PSYOP; отсюда следует и схожая стратегия, и тактические решения в информационной войне на первом этапе начавшейся СВО. Поэтому одной их характерных черт первого этапа информационно-психологической войны против России стало массовое использование «треш-контента», как наиболее эмоционально дестабилизирующего психику населения.

Постепенно формировалась и российская тактика информационной войны, включающая следующие основные направления:

1) информационный новостной контент;

2) аналитику, интерпретации происходящего и ведущихся боевых действий;

3) борьбу с фейками и дезинформацией в самом широком смысле;

4) пропаганду;

5) контрпропаганду.

Методы противодействия в информационной войне можно разделить на профилактические и оперативные, а также реактивные и проактивные. Исследователи выделяют четыре основные группы мер по превентивному противодействию негативному информационному влиянию со стороны сетевых акторов на сознание, как всего общества, так и непосредственно молодежи:

1) нормативно-правовые;

2) административные;

3) информационные;

4) экономические [5, с. 97].

В современной социально-гуманитарном знании проблематика определения, детализации и анализа эффективности технологий и практик противодействия влиянию сетевых акторов на сознание собственно молодежи в ходе информационной войны является относительно новой. Поэтому мы их рассмотрим в общей рамке мер и способов противостояния противнику в информационной войне.

Сначала коснемся информационно-технического аспекта противодействия и противоборства. Следует отметить важную роль, отводимую в информационным войнам методам и инструментам так называемого «информационно-технического воздействия», к которым относят:

1. Удаленные сетевые атаки.

2. Компьютерные вирусы («классические» вирусы, черви, троянские программы).

3. Программные закладки.

4. Аппаратные закладки.

К примеру, стоит учитывать тот факт, что производители программного обеспечения и программно-аппаратных средств встраивают в него функциональность ботов (автономного программного обеспечения, функционирующего без ведома владельца хоста). Наибольшей угрозой для молодежи является встраивание вредоносного кода в игровое программное обеспечение, наиболее популярное и распространенное у этой категории населения. Поэтому в условиях информационной войны резервирование критически важных систем и сервисов является необходимым условием информационной безопасности

Значительный интерес и возможности являют современные методы обнаружения пропаганды и информационных операций, к которым относится применение больших языковых моделей (LLM), которые позволяют анализировать огромные объемы информации.

Механизмы выявления в информационном потоке скрытой пропаганды строятся на комплексе процедур анализа данных:

1) лингвистический анализ структуры текста, частоты употребления определенных слов и фраз, риторических приемов и тональности.

2) когнитивное профилирование: выявление тактики и направлений влияния на аудиторию, манипулятивных приемов и постправды, эмоционально-насыщенного контента.

3) сетевой анализ: отслеживание распространения контента по различным цифровым каналам коммуникации, социальным сетям и новым медиа.

4) машинное обучение искусственного интеллекта: использование алгоритмов, способных обучаться на огромных объемах, данных и обнаруживать вредоносный контент.

Большие языковые модели (LLM), такие как GPT-4, используются для выявления агитационно-пропагандистских материалов, враждебных нарративов и сетевых атак в ситуации информационной войны и отличаются:

1) высокой точностью распознавания стилистики скрытой пропаганды и дезинформации;

2) возможностями сравнения текстов с обнаруженными примерами пропаганды, манипуляции и дезинформации;

3) определением идеологического подтекста и эмоционального фона сообщений;

4) анализом сетевого взаимодействия, позволяющего фиксировать скоординированные и целенаправленные психологические операции, и информационные компании.

Использование LLM позволило существенным образом сократить время обнаружения информационно-психологических атак, выявлять скрытую пропаганду и дезинформацию, маскирующиеся под нейтральный новостной фон. Растет точность и быстрота выявления дезинформации и пропаганды в огромном информационном потоке, что имеет огромное значения для информационной безопасности российского общества и противодействия негативному влиянию на молодежь. Быстрота и точность определения скрытой пропаганды и иностранного вмешательства позволяет убыстрить и методы контр-дезинформационной тактики информационного противодействия.

Однако обнаружить еще не означает успешно противодействовать, поэтому основным методом информационно-технического противоборства негативному влиянию сетевых акторов является запрет выявленных информационных ресурсов – распространителей враждебных нарративов, негативного и дезинформирующего контента. Надо констатировать тот факт, что это относительно эффективный способ противоборства, поскольку изначально по своему характеру является реактивным, а не проактивным, поскольку предполагает реакцию на воздействие, которое уже было оказано де-факто.

Социально-гуманитарные технологии, методы и практики противодействию влиянию сетевых акторов на сознание молодежи в ходе информационной войны, носят как методологический характер; то есть, предполагают, как разработку общесистемных мер, так и конкретно-методических и выступают в качестве неких гуманитарных технологий информационного противодействия. К примеру, А.В. Манойло и Е.Г. Пономарева выделяют следующие комплексные и системные по характеру меры информационного противодействия PSYOP:

1) «создание концепции идеологической политики государства», фиксация политических и социально-экономических приоритетов и обозначение «красные линии» информационного фронта;

2) инновационное развитие информационного обеспечения государственной политики России, которое позволит быстро и эффективно доводить позицию нашей страны до мировой общественности;

3) развитие научно-аналитического потенциала страны;

4) разработать соответствующую защиту отечественных информресурсов от информационных вбросов, обеспечить надлежащую подготовку кадров, способных отличать фейковые новости от достоверной информации;

5) анти-изоляционизм, поддерживать коммуникацию, проводить более взвешенную политику и дипломатию, использовать любое событие как информационный повод, позволяющий не только зафиксировать свою позицию, но и показать промахи, слабости и истинные цели противника [6, с. 15-17].

А.В. Манойло выделяет ряд авторских «контр-операций», которые являются следствием его практической и консалтинговой деятельности в сфере противостояния информационным операциям:

1) перехват информационной повестки;

2) перехват оперативной инициативы;

3) отвлечение на негодный объект;

4) информационная прививка;

6) «бумеранг» [7, с. 229].

Д.В. Шибаев выделяет следующие технологии информационного противоборства в ситуации идущей информационной войны, носящие обобщенный и методологический характер:

1. Информационную асимметрию — осуществление контр-дезинформации или пропаганды.

2. Информационное доминирование — наличие в информационной сфере государства-противника ему неподконтрольных масс-медиа, общественных объединений, политических сил.

3. Информационно-правовое доминирование — присутствие и наличие голоса в максимально большом количестве международных организаций для возможности быстрого реагирования на информационные вызовы и разъяснения международной общественности собственной точки зрения.

4. Латентность процессов информационной борьбы, т.е. скрытность и анонимность оперирования информационно-психологическими воздействиями, возможность проведения их «под чужим флагом» и с любой точки инфосферы.

5. Использование отсутствия четких юридически закрепленных в международных и национальных правовых нормах определений информационно-психологической агрессии и информа-

ционно-психологической войны в целях развязывания вооруженной агрессии и нанесения ущерба национальным интересам противников в мирных условиях.

6. Принцип возможности сочетания информационно-психологической борьбы, ведущейся участником борьбы в составе коалиции, с информационно-психологической борьбой, ведущейся этим же членом коалиции против других ее членов.

7. Создание в информационном пространстве системы органов государственной власти и управления государства-противника атмосферы недоверия, настороженности и враждебности по отношению ко всем остальным направлениям, предложениям и вариантам решения данного вопроса.

8. Информационную зависимость государства-противника от непрерывного поступления внешних или альтернативных информационных ресурсов.

9. Дестабилизацию ситуации внутри государства (геополитического субъекта) с целью навязывания внешнего антикризисного управления.

10. Информационно-психологическую экспансию.

11. Возрастное зомбирование посредством масс-медиа [8, с. 66-67].

Затрагиваемый Д.В. Шибаевым правовой аспект противодействия информационной войне - один из самых проблематичных, поскольку отсутствуют международные общепринятые четкие юридические критерии, нормы и правила по определению и оценке негативных информационно-пропагандистских и информационно-психологических воздействий на общественное сознание и, в частности, на сознание молодежи. Отсутствие подобной международной нормативно-правовой базы затрудняет организацию необходимых защитных мер, которые носили бы общепризнанный на международном уровне, легитимный и легальный характер и статус.

В отдельной особой международной институции нуждается система мер, нацеленных на информационное противодействие влиянию сетевых акторов на сознание детей и молодежи, как наиболее информационно и когнитивно слабозащищенных и уязвимых категорий населения, поскольку в современных информационных компаниях и войнах дети и молодежь рассматриваются как приоритетные объекты для сетевых атак. Однако отсутствует даже дискуссия о необходимости подобных решений на уровне ООН и других международных организаций. Поэтому инициирование подобной дискуссии видится нам одной из назревших актуальных проблем, в решении которой Российская Федерация может проявить инициативу и активность. Вербовка украинскими спецслужбами российских подростков и молодежи для осуществления диверсионно-разведывательной и террористической деятельности стало одной из серьезных проблем в обеспечении безопасности. И следует указать на то, что данная проблема будет интернализироваться и в последующем представлять угрозу не только для российского общества и государства.

В процессе контроля за киберпространством, важно избегать крайностей и излишних запретов, наиболее жесткая система фильтрации трафика действует с 2003 года в КНР. Однако рефлексия и исследование китайского опыта внедрения программы «Золотой щит», системы фильтрации содержимого интернета, представляется актуальной. И сам «Великий китайский файрвол», и законы, поддерживающие его эффективное функционирование, существенным образом ограничивают возможности компаний и свободы пользователей. Но эти меры могут носить для нас эвристический и дискуссионный характер и в более приемлемых формах, не связанных с явными ограничениями прав и свобод граждан, являться основой для российской информационной политики.

Укажем на некоторые меры, которые были связаны с повышением эффективности функционирования «Золотого щита» и предполагали «деанонимизацию» пользователей, как следствие того, что ограничения достаточно легко обходились пользователями при помощи сервисов VPN:

- запрет на анонимное общение;
- обязательную регистрацию в государственном реестре для информационных ресурсов;
- закрытие большого числа интернет-кафе;
- создание специализированного ведомства полиции для контроля над Интернетом;
- в конечном итоге, использование сервисов VPN было объявлено незаконным;
- антитеррористический закон, который давал разрешение на дешифровку интернет-трафика и изъятие информации у иностранных компаний, если она несла угрожающее содержание;
- закон о кибербезопасности ввел срок хранения в полгода для всего контента, публикуемого в китайском сегменте Интернета.

Заключение.

В заключении резюмируем некоторые меры и позволим себе выдвинуть ряд предложений и рекомендаций.

1. Встает вопрос о координации деятельности различных ведомств и органов в вопросе информационного противодействия влиянию сетевых акторов на сознание молодежи в ходе информационной войны. Одним из механизмов решение проблемы, о котором говорят ученые, является создание многофункциональной компьютерной сетевой среды управления, единой цифровой системы, которая бы охватывала правоохранительные органы, гражданские ведомства, оборонно-промышленный комплекс и все важные и критически значимые институты, занимающиеся жизнеобеспечением РФ.

2. Цензурирование, ограничения и запреты на распространение информационных данных в Интернете и СМИ — это неизбежные меры информационной безопасности. И хотя понятие «цензура» имеет плохую коннотацию в постсоветском обществе, тем не менее, большинство исследователей акцентируют внимание на её необходимости не на уровне возвращения к забытой лексике, а в качестве конкретной системы мер, оценивающих и фильтрующих информационный поток.

3. С целью ускорения реакции на информационные атаки П.Н. Кобец предлагает провести исследование и детально проработать на законодательном уровне правовые нормы, позволяющие региональным прокурорам в случае экстренной необходимости блокировать интернет-ресурсы, задействованные в информационных атаках [9, с. 26].

4. Использование больших языковых моделей (LLM) в отслеживании распространения контента по различным цифровым каналам коммуникации, социальным сетям и новым медиа. Использование машинного обучения искусственного интеллекта (machine learning, ML), алгоритмов, способных обучаться на огромных объемах, данных и обнаруживать вредоносный контент.

5. Ограничения для доступа в киберпространство страны для сервисов и сайтов, признанных нежелательными и экстремистскими должны сочетаться с процессом создания их российских аналогов и/или популяризации уже имеющихся отечественных программ, сервисов и информационных ресурсов.

6. Повышение медиаграмотности населения является одним из важных косвенных механизмов информационной безопасности ипротиводействия влиянию сетевых акторов на сознание молодежи в ходе информационной войны.

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.

Список источников:

1. *Glenn. J. C. Global Challenge 10, State of the Future 19.1. The Millennium Project. Washington. DC, 2018. – 208 p.*
2. *Church W. Information war // International Review of the Red Cross. 2000. №. 837. P. 45–56.*
3. *Шевырёв А. В., Замятин А. Ю. Концептуальные аспекты информационного противоборства // Радиолокация, навигация, связь. – 2017. С 1128-1138.*
4. *Стригунов К.С. Особенности современной неклассической войны: формы, методы, технологии. Диссертация на соискание научной степени кандидата политических наук. М. 2023. – 285 С.*
5. *Кузютин И. И. Возможные меры противодействия «цветным революциям» // Достижения науки и образования. 2016. № 7 (8). С. 96-99.*
6. *Манойло А. В., Пономарева Е. Г. Современные информационно-психологические операции: технологии и методы противодействия // Научно-аналитический журнал Обозреватель - Observer, no. 2 (349), 2019, pp. 5-17.*
7. *Манойло, А.В. Информационные войны и психологические операции. Руководство к действию. – М.: Горячая линия – Телеком, 2018. – 496 с.*
8. *Шибаев Д.В. Методы противодействия информационной войне // Российский журнал правовых исследований. - 2016. - Т. 3. - №4. С. 64-67.*
9. *Кобец П. Н. Противодействие терроризму в информационной сфере: опыт и проблемы // Научный портал МВД России, №. 3 (55), 2021, С. 18-26.*

References:

1. *Glenn. J. C. Global Challenge 10, State of the Future 19.1. The Millennium Project. Washington. DC, 2018. – 208 p.*
2. *Church W. Information war // International Review of the Red Cross. 2000. №. 837. P. 45–56.*

3. Shevyrev A.V., Zamyatin A. Y. Conceptual aspects of information warfare // Radar, navigation, communications. – 2017. From 1128-1138.

4. Strigunov K.S. Features of modern non-classical warfare: forms, methods, technologies. Dissertation for the degree of Candidate of Political Sciences. M. 2023. – 285 p.

5. Kuzyutin I. I. Possible measures to counteract the "color revolutions" // Achievements of science and education. 2016. No. 7 (8). pp. 96-99.

6. Manoilo A.V., Ponomareva E. G. Modern information and psychological operations: technologies and methods of counteraction // Scientific and Analytical journal Obozrevatel - Observer, No. 2 (349), 2019, pp. 5-17.

7. Manoilo, A.V. Information wars and psychological operations. A guide to action. Moscow: Hotline – Telecom, 2018. 496 p

8. Shibaev D.V. Methods of countering information warfare // Russian Journal of Legal Research. - 2016. - Vol. 3. - No. 4. pp. 64-67.

9. Kobets P. N. Countering terrorism in the information sphere: experience and problems // Scientific Portal of the Ministry of Internal Affairs of Russia, №. 3 (55), 2021, Pp. 18-26.

Информация об авторах:
Лушников Дмитрий Александрович, доктор социологических наук, профессор, заведующий кафедрой социологии и социальных инноваций, Северо-Кавказский федеральный университет, keremet2000@mail.ru, *https://orcid.org/*0000-0003-0352-4662
Долгополов Кирилл Андреевич, кандидат юридических наук, доцент, заведующий кафедрой кафедры уголовного права и процесса. Северо-Кавказский федеральный университет, *https://orcid.org/*0000-0003-4496-1789,
Кузнецова Оксана Николаевна, доцент кафедры государственного, муниципального управления и экономики труда, Северо-Кавказский федеральный университет, okuznetcova@ncfu.ru, *https://orcid.org/*0009-0007-6949-8491
Dmitry A. Lushnikov, Doctor of Sociology, Professor, Head of the Department of Sociology and Social Innovation, North Caucasus Federal University.
Kirill A. Dolgopolov, PhD in Law, Associate Professor, Head of the Department of Criminal Law and Procedure, North Caucasus Federal University.
Oksana N. Kuznetsova, Associate Professor of the Department of State, Municipal Management and Labor Economics, North Caucasus Federal University.

Вклад авторов:
все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors:
All authors contributed equally to this article.

Статья поступила в редакцию / The article was submitted 22.05.2025;
Одобрена после рецензирования / Approved after reviewing 18.06.2025;
Принята к публикации / Accepted for publication 20.06.2025.
Авторами окончательный вариант рукописи одобрен.