УДК 343.359
JEL F42, Z18

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГЛОБАЛЬНОМ ПОЛИТИКО-ЭКОНОМИЧЕСКОМ ПРОСТРАНСТВЕ: МЕХАНИЗМЫ МАНИПУЛЯТИВНОГО ВОЗДЕЙСТВИЯ И СИСТЕМЫ КОГНИТИВНОЙ ЗАЩИТЫ

С. А. Кристиневич
sk.bseu@gmail.com
кандидат экономических наук, доцент,
доцент кафедры экономической теории,
Белорусский государственный экономический университет,
г. Минск, Республика Беларусь

Технологии реализации силового неравенства активно используются правительствами стран, позиционирующих себя гарантами мирового порядка, международными клубами и организациями, в рамках интеграционных объединений. В силу этого практической стороной вопроса выступает необходимость выработки «ответных реакций» и механизмов защиты, встроенных в систему национальной безопасности. В статье рассмотрены существующие техники информационно-психологического воздействия и обоснована тактика делегитимации информационной интервенции.

***Ключевые слова**: информационная безопасность, информационное воздействие, интервент, медиапространство, когнитивная защита.*

Цитирование: Кристиневич, С. А. Информационная безопасность в глобальном политико-экономическом пространстве: механизмы манипулятивного воздействия и системы когнитивной защиты / С. А. Кристиневич // Экономическая наука сегодня : сб. науч. ст. / БНТУ. – Минск, 2020. – Вып. 12. – С. 46–56.

Введение. Современные технологии воздействия на массовое сознание, возможности использования медиапространства, гуманитарные техники формирования нужных образов обостряют информационную конкуренцию, особенно на глобальном уровне. В результате актуализируется проблема информационного противостояния в глобальном политико-экономическом пространстве. Такое противостояние предполагает разработку *техник информационно-психологического воздействия* со стороны интервента и, соответственно, конструирование *систем информационной безопасности* со стороны остальных акторов.

Победа в информационной конкуренции дает возможность быстро формировать нужное общественное мнение по тому или иному вопросу. Общественное мнение обеспечивает необходимой легитимностью действия глобального интервента, наделяя его правом влиять не только на конфигурацию мирового порядка, но и на направление процесса глобализации. Последствием глобализации является стирание национальных идентичностей, своего рода унификация сфер жизнедеятельности. Возникает потребность в образце такой унификации. За право им быть постоянно идет борьба, поскольку субъект, выступающий в качестве паттерна, претендует на формирование стандартов практически по всем направлениям жизнедеятельности. Определение трендов потребительских предпочтений, настойчивость в выборе инструментов экономической политики для других стран, ограничение разнообразия форм политического устройства, монополия на идентификацию демократичности государств, установление норм и атрибутов «настоящей» культуры − неполный перечень сфер влияния потенциального лидера глобализации.

В конкуренции за право быть таким образцом побеждает актор, способный не только предложить конкурентоспособную идеологию, но и эффективную технологию ее продвижения. Идеология представляет собой ментальную модель, разделяемую большинством. Ментальная модель – это совокупность правил (институтов), регламентирующих способы понимания (процесс познания) реальности и стимулирующих человека к действию. Чем большее индивидов соблюдает правила, входящие в ментальную модель, тем они легитимнее, тем меньше издержек несет интервент.

Результаты и их обсуждение. ***Техники информационного воздействия***. Возрастание роли информационной политики наблюдается с 90-х годов XX века. Родоначальником и лидером использования ее инструментов являются США. Довольно радикальный настрой заметен в официальных документах Министерства обороны этой страны. Именно в них (см. директиву Министерства обороны США № 3600, 21 декабря 1992 г.) началось употребление словосочетания «информационная война» [1, с. 27]. Впоследствии, разработка стратегии информационного воздействия была поручена корпорации РЭНД. Аналитический центр РЭНД – американская некоммерческая организация, основанная в 1948 году и работающая по заказам правительства США. Уже к концу 90-х годов были сформулированы основные принципы и подходы к ведению информационных войн (см. отчеты корпорации MR-661-SD «Strategic Information Warfare. A new face of War» (1996 г.), MR- 963-SD «The Day After … in the American Strategic Infrastructure» (1998 г.) и MR-964-SD «Strategic Information Warfare Rising» (1998 г.) [1, с. 27]. Если на начальном этапе разработка инструментов информационного воздействия шла в оборонительных целях, то с 1998 года Вооруженными силами США в «Доктрине проведения информационных операций» декларируется наступательная стратегия не только в военное, но и мирное время [2]. Современная концепция американского превосходства в информационной сфере отражена в документе Комитета начальников штабов Министерства обороны США «Единые перспективы 2020».

Другим значимым центром силы, использующим информацию как стратегический ресурс в своей деятельности, является НАТО. Ключевым документом, регламентирующим позицию Североатлантического альянса в сфере информационного воздействия, выступает директива «О принципах планирования и ведения психологических операций» [3]. Документ легитимирует проведение психологических операций со стороны альянса с целью оказания влияния на объект в любое время (военное, кризисное, мирное). Масштабы воздействия носят глобальный характер.

Интересна позиция еще одного крупного игрока в глобальном информационном пространстве − Китая. Информационная политика этой страны носит преимущественно оборонительный характер. Причем активно развиваются два основных направления: техническое обеспечение кибербезопасности и госрегулирование в области ограничения деструктивного информационно-психологического воздействия на массовое сознание. Однако в силу усиления в последние десятилетия геополитического противостояния и трансформации способов информационного воздействия, Китай допускает использование наступательной информационной стратегии, которая основана на одновременном ведении психологический, медийной и правовой войны [4, с. 282]. Существование директив, стратегий и иных документов, определяющих информационную политику как приоритетную на государственном уровне во многих странах, позволяет сделать вывод о возрастающей роли информации как инструмента достижения собственных целей в глобальном политико-экономическом пространстве.

В нашем случае контекст проблемы в меньшей степени предполагает исследование технических аспектов информационного воздействия. Целесообразным выглядит поиск способов создания новых смыслов в процессе информационно-психологического воздействия, выявление и обоснование общей схемы трансформации восприятия экономической реальности и ценностных установок. По-

нимание логики и нахождение такого *общего механизма манипулятивного воздействия* позволит обосновать тактику делегитимации интервента.

Общий механизм манипулятивного воздействия. Применение технологий воздействия на массовое сознание обусловлено широким спектром целей. Результативность воздействия, как правило, оценивается сопоставлением планируемого изменения поведения объектом с фактически полученным. Сложной задачей является моделирование восприятия реальности в краткосрочном периоде. Для такой цели обычно используется такая форма рефлексивного управления как поведенческое оружие, под которым принято понимать комплекс действий, нацеленный на эксплуатацию поведенческих стереотипов. Облегчает задачу накопление в интернете данных о человеческом поведении (Больших Данных, англ. Big Data). Технология позволяет с помощью программных инструментов структурировать огромные массивы информации и на их основе анализировать привычки, поведение и ценностные установки больших социальных групп.

Обобщение некоторого опыта когнитивного управления в различных сферах общественной жизни [5–14] позволяет предположить, что существует определенный общий механизм манипулятивного воздействия (табл. 1).

Таблица 1 – Общий механизм манипулятивного воздействия

Наименование этапа	Характеристика этапа
1. «Неприятие»	Происходит фокусировка на конкретном информационном контексте, актуализуется «проблема», которая сопровождается широким публичным обсуждением, фиксируется противоречие существующим ценностным установкам социальной группы.
2. «Странность»	Широкое обсуждение приводит к тому, что, несмотря на негативное восприятие «проблемы» большинством, следует признать ее существование.
3. «Допустимость»	Происходит встраивание «проблемы» в систему ценностных установок социальной группы, при этом оговаривается ее особое положение.
4. «Норма»	Происходит симбиоз и «опривычивание». «Проблема» претерпевает трансформацию от девиации к норме.

Источник: разработка автора.

Деструктивное информационное воздействие приводит к мировоззренческим и ценностным искажениям на персональном и общественном уровне. Это, в свою очередь, в долгосрочном периоде ведет к деформации (снижению устойчивости) существующих неформальных институтов и появлению новых, не всегда адекватных, практик восприятия реальности через смысловые шаблоны и искусственно сконструированные паттерны. Конечной целью такого манипулятивного воздействия на объект, как правило, является снижение общего конкурентного потенциала и адаптивности к изменениям. Сдерживание или, по крайней мере, фильтрация информационного контента, становится актуальной проблемой в процессе выработки стратегий межсубъектного взаимодействия на глобальном уровне. Реакцией на этот вызов и распространенной практикой является разработка национальных систем информационной безопасности.

Системы информационной (когнитивной) безопасности. На национальном уровне бремя по разработке систем информационной безопасности, как правило, лежит на государстве. Видение и описание механизмов ее обеспечения чаще всего можно встретить в концепциях национальной безопасности или самостоятельных нормативных актах, регламентирующих отношения в области информационной политики.

В последнее время разработка такого общего документа, который бы содержал систему официальных взглядов на цели, принципы и основные направления обеспечения информационной безопасности стала нормой. Учитывая, что санкционная политика сопровождается агрессивным информационным воздействием в медиапространстве с целью легитимации действий субъекта односторонних мер принуждения, возникает необходимость в существовании тактики делегитимации интервента. Для обоснования такой тактики целесообразным видится:

во-первых, использование достижений в области междисциплинарных гуманитарных технологий информационного воздействия;

во-вторых, учет описанного выше общего механизма манипулятивного воздействия как методологической основы;

в-третьих, оценка возможной гармонизации тактики с ключевым документом, регламентирующим сферу информационной безопасности.

Для иллюстрации третьего пункта рассмотрим видение проблемы информационной безопасности в базовых документах некоторых ближайших стран-соседей.

Одной из стран, испытывающей на себе давление санкционной политики, (в особенности с 2014 года) является Российская Федерация. Для защиты национальных интересов в целях обеспечения информационной безопасности Президентом утверждена Доктрина информационной безопасности Российской Федерации 5 декабря 2016 года (далее – Доктрина). Под информационной безопасностью понимается «состояние защищенности национальных интересов России в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»[1]. В документе можно выделить следующие логические блоки: определение целей и направлений обеспечения информационной безопасности, оценка состояния и анализ возможных угроз информационной безопасности, описание организационных основ обеспечения информационной безопасности.

В Доктрине отмечен рост информационно-технической активности со стороны некоторых зарубежных стран, что создает угрозу информационной инфраструктуре и тем самым актуализирует проблему технического аспекта информационной безопасности. Показана тенденция увеличения роста объема информационных материалов иностранных СМИ, где содержатся предвзятые оценки государственной политики, проводимой РФ. Отмечается, что информационное воздействие становится основным инструментом в деятельности террористических и экстремистских организаций. Среди основных направлений обеспечения информационной безопасности уделено особое внимание нейтрализации информационного (когнитивного) воздействия. Согласно п. 23 Доктрины, базовыми ориентирами являются[2]:

– «противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации»;

– «повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации»;

– «нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей».

[1] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).

[2] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).

Среди направлений обеспечения информационной безопасности в экономической сфере можно встретить[1]:

– «инновационное развитие отрасли информационных технологий и электронной промышленности, увеличение доли продукции этой отрасли в валовом внутреннем продукте, в структуре экспорта страны»;

– «повышение конкурентоспособности российских компаний».

Еще одним примером концептуального взгляда на проблему является Доктрина информационной безопасности Украины от 29 декабря 2016 года (утверждена Указом Президента Украины 25 февраля 2017 г. № 47). Структура Доктрины состоит из следующих элементов: основные положения, цель и принципы, национальные интересы Украины в информационной сфере, актуальные угрозы национальным интересам в сфере информационной безопасности, механизм реализации Доктрины, заключительные положения[2]. Структура выглядит традиционно, при этом выделяется два аспекта информационной безопасности: технический и когнитивный. Содержательно документ иллюстрирует четкую антироссийскую позицию, что может подтвердить даже поверхностный контент-анализ. Возможно, четкое представление угроз позволило конкретизировать новизну используемых в Доктрине понятий, особенно в части описания когнитивного воздействия. Наряду со стандартным для таких документов категориальным аппаратом встречаются оригинальные концепты. Так, например, вводится понятие «стратегический нарратив − специально подготовленный текст, предназначенный для вербального изложения в процессе стратегических коммуникаций с целью информационного воздействия на целевую аудиторию»[3]. Подробное изучение раздела 6 «Механизмы реализации Доктрины» дает основание сделать вывод, что аспект информационно-психологического воздействия преобладает над технической стороной проблемы. Это подтверждают следующие направления и мероприятия[4]:

– «мониторинг средств массовой информации и общедоступных ресурсов отечественного сегмента сети Интернет с целью выявления информации, распространение которой запрещено в Украине»;

– «мониторинг угроз национальным интересам и национальной безопасности в информационной сфере»;

– «содействие Министерству иностранных дел Украины по донесению официальной позиции Украины в иностранных средствах массовой информации»;

– «формирование текущих приоритетов государственной информационной политики, контроля их реализации»;

– «координация деятельности центральных и местных органов исполнительной власти в сфере обеспечения информационного суверенитета Украины»;

– «разработка стратегического нарратива и его имплементации»;

– «разработка и внедрение единых стандартов подготовки специалистов в сфере правительственных коммуникаций для нужд государственных органов».

Для Республики Беларусь проблема информационной безопасности также актуализируется в связи усилением геополитической активности игроков с разными ментальными моделями. Основным документом, в котором представлена официальная точка зрения на проблему информационной безопасности была Концепция нацио-

[1] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).

[2] Доктрина информационной безопасности Украины (утв. Указом Президента Украины 25 февраля 2017 г. № 47)

[3] Доктрина информационной безопасности Украины (утв. Указом Президента Украины 25 февраля 2017 г. № 47)

[4] Доктрина информационной безопасности Украины (утв. Указом Президента Украины 25 февраля 2017 г. № 47)

нальной безопасности Республики Беларусь[1]. Однако появление новых угроз, постоянное углубление информатизации, непрерывное усовершенствование техник когнитивного воздействия потребовало детальной проработки механизмов информационной защиты и конкретизации направлений нейтрализации рисков. В результате возникла объективная необходимость в создании самостоятельного документа, который бы обосновывал структуру и содержание концепции информационной безопасности Республики Беларусь. По мнению разработчиков, такой документ должен отвечать следующим требованиям [15, с. 16]:

– «учитывать направления устойчивого развития информационных отношений в стране»;

– «формировать систему барьеров для реализации угроз национальным интересам»;

– «стимулировать способность базовых систем экономических, политических, социальных и иных отношений Республики Беларусь противостоять информационным угрозам».

В результате изучения различных методологических подходов, сопоставления опыта создания подобных документов в странах дальнего и ближнего зарубежья была разработана и утверждена 18 марта 2019 г. Концепция информационной безопасности Республики Беларусь. Структура документа состоит из семи разделов[2]:

– общие положения;

– состояние и развитие информационной сферы в Республике Беларусь;

– государственная политика обеспечения информационной безопасности;

– безопасность информационного пространства как одно из важнейших условий развития суверенного, демократического социального государства;

– обеспечение безопасности информационной инфраструктуры;

– обеспечение безопасности информационных ресурсов;

– механизмы реализации концепции.

В содержании Концепции обращает на себя внимание весомость когнитивного аспекта информационной безопасности. Среди понятийного аппарата встречаются термины «воздействие на информацию», «деструктивное информационное воздействие», «информационный суверенитет», «информационное пространство» и другие. Последовательный анализ содержания Концепции по всем разделам позволяет обозначить некоторые особенности:

1. Кроме традиционного выделения в аналогичных зарубежных документах технического и информационно-психологического аспектов безопасности в концепции заявлена позиция «информационного нейтралитета» (глава 8), которая предполагает отсутствие вмешательства в информационную сферу других стран (п. 31) при постепенном наращивании присутствия Беларуси в мировом информационном пространстве (п. 32).

2. Обосновывается идея «информационного суверенитета», исключающего агрессивные методы информационного воздействия со стороны Беларуси. При этом заявляется принципиальная позиция по отношению проявления неуважения к традиционным белорусским ценностям, нетерпимость к дезинформации и информационным манипуляциям (п. 27).

3. В п. 16, 28 и 35 четко определяются функции государства по локализации и минимизации деструктивного информационного воздействия. Информационная поли-

[1] Концепция национальной безопасности Республики Беларусь (утв. Указом Президента Республики Беларусь 09 ноября 2010 г. № 575)

[2] Концепция информационной безопасности Республики Беларусь (утв. Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1)

тика предполагает разработку и реализацию стратегических и тактических мер по нейтрализации информационных рисков, угроз и вызовов.

4. Целый раздел (IV) посвящен угрозам, связанным с размыванием ментальных моделей, манипуляцией массовым сознанием и созданием фейковых контекстов, подрывающих конституционный строй и политическую стабильность. Из чего можно заключить о полном понимании разработчиками способов и методов воздействия, применяемых в глобальном политико-экономическом пространстве.

5. Для повышения эффективности решения задач, связанных с обеспечением информационной безопасности, предлагается использовать механизм государственно-частного партнерства (глава 26). Выделяется два направления сотрудничества: подготовка кадров в области обеспечения информационной безопасности и стимулирование участия отечественных IT компаний в решении проблемы выявления угроз информационной безопасности.

Рассмотренные системы информационной безопасности (Доктрины, Концепции) позволяют еще раз подтвердить тезис об информационном воздействии как ключевом инструменте легитимации межсубъектных отношений в модели «интервент-жертва».

В этих условиях ответом может стать тактика делегитимации информационной интервенции. Опираясь на концепцию конструирования социальной реальности, элементы проектирования управляемых конфликтов, технологии модификации ментальных моделей, концепции информационных и поведенческих войн, методики рефлексивного управления, тактика делегитимации может состоять из следующих этапов (таблица 2):

Таблица 2 – Тактика делегитимации интервента

Наименование этапа	**Содержание этапа**
1. Актуализация конфликта в глобальном политико-экономическом пространстве	Позволяет зафиксировать публичную реакцию акторов политико-экономического пространства на конфликт, идентифицировать «своих» и «чужих», приступить к формированию информационной коалиции
2. Модификация восприятия образа жертвы в медиапространстве	Предполагает проведение информационных атак, снижающих воздействие астротурфинга[1] со стороны интервента и формирующих положительный имидж потерпевшей стороны.
3. Имплементация нового образа жертвы в массовое сознание	Сопровождается публичной оценкой величины нанесенного ущерба, экономических и гуманитарных потерь, отсутствием оправдания недружественных действий и пересмотром поведенческих стратегий в условиях информационного давления.
4. Институционализация образа жертвы	Характеризуется рационализацией и формированием устойчивого восприятия объекта как жертвы, сопровождается упоминанием в нормативных актах и закреплением образа в общественном сознании.
5. Легитимация образа жертвы	Позволяет оправдать применение контрмер по отношению к интервенту, обеспечивает признание целесообразности симметричной реакции.

Источник. Авторская разработка.

Таким образом, концептуальная схема может выглядеть как представлено на рисунке 1.

[1] Астротурфинг – «технология искусственного создания общественного мнения путем размещения многочисленных заказных публикаций, оформленных как совершенно независимые мнения частных лиц». Довольно эффективной формой является создание «платных организованных групп воздействия». Наиболее известные в мире группы: США – проект «Честный голос», Китай – «Умаодан», Великобритания – «Cambridge Analytica», Израиль – «Хасбара».

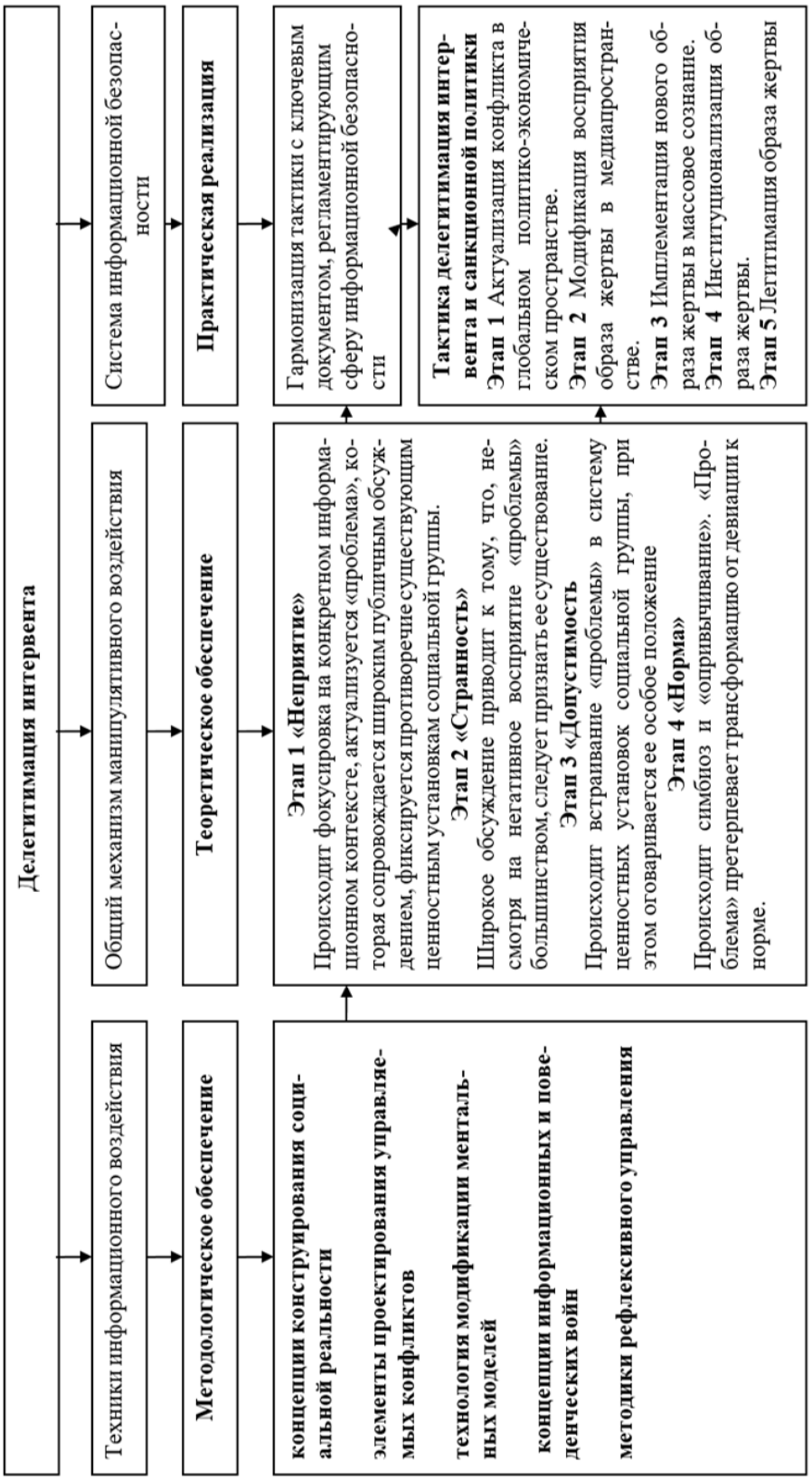

Рисунок 1 – Концептуальная схема делегитимации интервента

Источник: авторская разработка

Выводы. Диапазон целей интервентов глобального уровня достаточно широк: от тактических − конструирования правил, улучшающих условия ведения бизнеса для национальных компаний, до стратегических − экспорта идеологий. Преимущества в переговорной силе и ресурсном потенциале позволяют интервенту, опираясь на современные гуманитарные технологии, выигрывать в информационной конкуренции. Результативность делегитимации информационной стратегии интервента зависит не только от техники информационного воздействия, но и от возможностей жертвы аккумулировать и перераспределять ресурсы.

Список использованных источников

1. Антонович, П. Ключевые аспекты информационной войны / П. Антонович // Армейский вестник. – 2014. – № 1. – С. 26–29.

2. Степанова, Н. Информационное противоборство на современном этапе / Н. Степанова // Молодой ученый. – 2009. – № 2. – С. 252–256.

3. Бодров, М. Психологическое воздействие на личность / М. Бодров. – Litres, 2018. – 125 с.

4. Кошурникова, Н. Особенности информационной политики современного Китая / Н. Кошурникова // Китай: история и современность: материалы IX междунар. науч.-практ. конф. Екатеринбург, 21–23 октября 2015 г. – Екатеринбург: Издательство Уральского университета, 2016. – С. 279–284.

5. Калдор, М. Новые и старые войны: организованное насилие в глобальную эпоху. / М. Калдор. – М. : Изд-во Института Гайдара, 2015. – 416 с.

6. Невоенные рычаги внешней политики России: региональные и глобальные механизмы / под общ. ред. В. М. Братерского. – М. : Изд. дом Высшей школы экономики, 2012. – 282 с.

7. Подберёзкин, А. И. Военные угрозы России: аналитический доклад. МГИМО(У) МИД России, Центр военно-политических исследований. – М. : МГИМО-Университет, 2014. –186 с.

8. Попов, И. М. Война будущего: Концептуальные основы и практические выводы. Очерки стратегической мысли / И. М. Попов, М. М. Хамзатов. – М. : Кучково поле, 2016. – 832 с.

9. Информационные операции в сети Интернет / под общ. ред. А. Б. Михайловского. – М. : АНО ЦСОиП, 2014. – 128 с.

10. Кристиневич, С. А. Институциональные интервенции как рациональный выбор: микроэкономические основания недобровольного обмена / С. А. Кристиневич // Вестник Московского университета. Серия 6. Экономика. – 2018. – № 6. – С. 24–39.

11. Кристиневич, С. А. Санкции как силовой инструмент в глобальном политико-экономическом пространстве / С. А. Кристиневич // Белорусский экономический журнал. – 2019. – № 1. – С. 30–42.

12. Кристиневич, С. А. Институциональные интервенции: концепция и механизмы реализации в национальной и мировой экономике / С. А. Кристиневич. – Минск : ИВЦ Минфина, 2020. – 234 с.

13. Scott, D. The Behavioral Origins of War / D. Scott, C. Stam. – Univ. of Michigan Press, 2003. – 302 p.

14. Sitaraman, G. Zionts, D., Behavioral War Powers / G. Sitaraman, D. Zionts // New York University Law Review. – 2015. – Vol. 90, № 2. – P. 1–76.

15. Арчаков, В. Теоретическое обоснование Концепции информационной безопасности Республики Беларусь / В. Арчаков, О. Макаров // Наука и инновации. – 2018. – № 10. – С. 14–20.

Статья поступила в редакцию 27 августа 2020 года

INFORMATION SECURITY IN THE GLOBAL POLITICAL AND ECONOMIC SPACE: MECHANISMS OF MANIPULATIVE INFLUENCE AND SYSTEMS OF COGNITIVE PROTECTION

S. A. Kristinevich
PhD in Economics, Associate Professor,
Associate Professor of the Department of Economic theory
Belarusian State Economic University
Minsk, Republic of Belarus

The implementation technologies of power inequalities are actively used by governments of countries that position themselves as guarantors of world order, international clubs and organizations, within the framework of integration associations. Because of this, the practical side of the question is the need to develop "response reactions" and protection mechanisms built into the national security system. The article deals with the existing technology information and psychological impact and justified tactic to delegitimize information influence.

***Keywords**: information security, information influence, interventionist, media space, cognitive protection.*

References

1. Antonovich, P. (2014) Klyuchevye aspekty informatsionnoi voiny [Key aspects of information war]. *Armejskij vestnik*. (1), 26–29. (In Russian).

2. Stepanova, N. (2009) Informatsionnoe protivoborstvo na sovremennom etape [Information confrontation at the present stage]. *Molodoi uchenyi*. (2), 252–256. (In Russian).

3. Bodrov, M. (2018) *Psihologicheskoe vozdejstvie na lichnost'*. [Psychological impact on personality], Litres. (In Russian).

4. Koshurnikova, N. (2016) "Specific features of modern China informational policy". *materialy IX mezhdunar. nauch.-prakt. konf* [thesises of IX international scientific conference]. *Kitai: istoriya i sovremennost'* [China: history and contemporarity]., 21–23 oktober 2015, Ekaterinburg, Russia. Ekaterinburg, Izdatel'stvo Ural'skogo universiteta, pp. 279–284. (In Russian).

5. Kaldor, M. (2015) *Novye i starye voiny: organizovannoe nasilie v global'nuyu epokhu* [New and old wars: organized violence during the global era]. – Moscow, Institut Gajdara publ. (In Russian).

6. Braterskii, V. S. (ed.) (2012) *Nevoennye rychagi vneshnei politiki Rossii: regional'nye i global'nye mekhanizmy* [Non-military instruments of Russian foreign policy: local and global mechanisms]. Moscow, Vysshej shkoly jekonomiki publ. (In Russian).

7. Podberezkin, A. I. (2014) *Voennye ugrozy Rossii* [Military threats to Russia]: analiticheskii doklad. MGIMO(U) MID Rossii, Tsentr voenno-politicheskikh issledovanii. – Moscow.: MGIMO-Universitet. (In Russian).

8. Popov, I. M., Hamzatov, M. M. (2016) *Voina budushchego: Kontseptual'nye osnovy i prakticheskie vyvody. Ocherki strategicheskoi mysli* [The war of future: conceptional basics and practical conclusions. Essays of strategic thought]. Moscow, Kuchkovo pole publ.(In Russian).

9. Mihailovsky, A. B., Rastorguev, S., Litvinenko, M. (2014) Informatsionnye operatsii v seti Internet [Information operations in the Internet]. Moscow, ANO CSOiP publ., (In Russian).

10. Kristinevich, S. A. (2018) Institutsional'nye interventsii kak ratsional'nyi vybor: mikroekonomicheskie osnovaniya nedobrovol'nogo obmena [Institutional interventions as rational choice: microeconomical basics of involuntary exchange]. *Vestnik Moskovskogo universiteta. Serija 6. Ekonomika*. (6), 24–39. (In Russian).

11. Kristinevich, S. (2019) Sanktsii kak silovoi instrument v global'nom politiko-ekonomicheskom prostranstve [Sanctions as a tool of power politics in global political and economic space]. *Belorusskij ekonomicheskii zhurnal*.(1), 30–42. (In Russian).

12. Kristinevich, S. A. (2020) *Institucional'nye interventsii: kontseptsiya i mekhanizmy realizatsii v natsional'noi i mirovoi ekonomike* [Institutional interventions: concept and mechanisms of realization in national and global economy] Minsk, IVTS Minfina publ., 2020. – 234 s. (1), 26–29. (In Russian).

13. Scott, D., Stam, C. (2003) The Behavioral Origins of War. – Univ. of Michigan Press. (1), 26–29.

14. Sitaraman, G. Zionts, D., (2015) Behavioral War Powers. New York University Law Review. – 90 (2), 1–76. (In Russian).

15. Artshakov, V., Makarov, O. (2018) Teoreticheskoe obosnovanie Kontseptsii informatsionnoii bezopasnosti Respubliki Belarus'[Theoretical justification of Concept of Belarussian informational safety]. *Nauka i innovatsii*. (10), 14–20. (In Russian).